

Федеральное государственное бюджетное образовательное учреждение высшего образования «Тамбовский государственный университет имени Г.Р. Державина»  
Институт математики, физики и информационных технологий  
Кафедра математического моделирования и информационных технологий

УТВЕРЖДАЮ:  
Директор института



Н. Л. Королева  
«04» июля 2022 г.

## **РАБОЧАЯ ПРОГРАММА**

по дисциплине Б1.О.20 Защита информации от утечки по техническим каналам

Направление подготовки/специальность: 10.03.01 - Информационная безопасность

Профиль/направленность/специализация: Безопасность компьютерных систем

Уровень высшего образования: бакалавриат

Квалификация: Бакалавр

год набора: 2022

**Автор программы:**

Кандидат технических наук, доцент Зауголков Игорь Алексеевич

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.03.01 - Информационная безопасность (уровень бакалавриата) (приказ Министерства образования и науки РФ от «17» ноября 2020 г. № 1427).

Рабочая программа принята на заседании Кафедры математического моделирования и информационных технологий «29» июня 2022 г. Протокол № 12

Рассмотрена и одобрена на заседании Ученого совета Института математики, физики и информационных технологий, Протокол от «04» июля 2022 г. № 6.

## СОДЕРЖАНИЕ

1. Цели и задачи дисциплины.....	4
2. Место дисциплины в структуре ОП бакалавра.....	4
3. Объем и содержание дисциплины.....	4
4. Контроль знаний обучающихся и типовые оценочные средства.....	10
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	25
6. Учебно-методическое и информационное обеспечение дисциплины.....	27
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	27

## 1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

ПК-4 Способен организовывать технологический процесс защиты информации в компьютерных системах

1.2 Типы задач профессиональной деятельности, к которым готовятся обучающиеся в рамках освоения дисциплины:

- эксплуатационный

1.3 Дисциплина ориентирована на подготовку обучающихся к профессиональной деятельности в сфере: 06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере)

1.4 В результате освоения дисциплины у обучающихся должны быть сформированы:

Обобщенные трудовые функции / трудовые функции / трудовые или профессиональные действия (при наличии профстандарта)	Код и наименование компетенции ФГОС ВО, необходимой для формирования трудового или профессионального действия	Индикаторы достижения компетенций
	ПК-4 Способен организовывать технологический процесс защиты информации в компьютерных системах	Организует технологический процесс защиты информации в компьютерных системах от утечки по техническим каналам

1.5 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ПК-4 Способен организовывать технологический процесс защиты информации в компьютерных системах

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения			
		Очная (семестр)			
		3	5	7	8
1	Компьютерная экспертиза		+		
2	Преддипломная практика				+
3	Расследование компьютерных инцидентов			+	
4	Электроника и схемотехника	+			

## 2. Место дисциплины в структуре ОП бакалавриата:

Дисциплина «Защита информации от утечки по техническим каналам» относится к обязательной части учебного плана ОП по направлению подготовки 10.03.01 - Информационная безопасность.

Дисциплина «Защита информации от утечки по техническим каналам» изучается в 4, 5 семестрах.

## 3. Объем и содержание дисциплины

3.1. Объем дисциплины: 9 з.е.

Очная: 9 з.е.

Вид учебной работы	Очная (всего часов)
<b>Общая трудоёмкость дисциплины</b>	<b>324</b>
Контактная работа	208
Лекции (Лекции)	96
Лабораторные (Лаб. раб.)	112
Самостоятельная работа (СР)	80
Экзамен	36
Зачет	-

### 3.2.Содержание курса:

№ темы	Название раздела/темы	Вид учебной работы, час.			Формы текущего контроля
		Лек ции	Лаб · раб.	СР	
		О	О	О	
4 семестр					
1	Введение	14	10	10	Собеседование; Тестирование
2	Объекты информационной безопасности.	14	27	10	Собеседование
3	Угрозы безопасности информации.	20	27	12	Защита лабораторных работ; Тестирование
5 семестр					
4	Методы, способы и средства технической защиты информации.	16	15	16	Защита лабораторных работ; Тестирование; Реферат
5	Организация инженерно-технич еской защиты информации	16	15	16	Защита лабораторных работ
6	Основы методического обеспечения инженерно-технич еской защиты информации	16	18	16	Защита лабораторных работ; Тестирование

### Тема 1. Введение (ПК-4)

#### Лекция.

Предмет, цели, задачи и содержание курса технической защиты информации (ТЗИ). Роль и место курса в подготовке специалистов по организации защиты информации в государственных и коммерческих структурах. Базовые знания, необходимые для изучения курса. Рекомендуемые учебные пособия.

### **Лабораторные работы.**

Подготовить доклад на тему Роль и место курса в подготовке специалистов по организации защиты информации в государственных и коммерческих структурах

### **Задания для самостоятельной работы.**

1. Проработка конспектов лекций и вопросов, вынесенных на самостоятельное изучение основной и дополнительной литературы.
2. Подготовка к тестированию.

## **Тема 2. Объекты информационной безопасности. (ПК-4)**

### **Лекция.**

Основные свойства информации как предмета технической защиты.

Виды информации, защищаемой техническими средствами. Свойства информации, влияющие на возможности ее защиты. Понятие о демаскирующих признаках объектов защиты. Характеристики и особенности семантической (смысловой) информации и информации о демаскирующих признаках объекта.

Демаскирующие признаки объектов защиты.

Классификация демаскирующих признаков. Опознавательные признаки и признаки деятельности объектов. Видовые, сигнальные и вещественные демаскирующие признаки. Информативность признаков. Понятие о признаковых структурах. Основные видовые демаскирующие признаки объектов наблюдения. Особенности видовых признаков в оптическом и радиодиапазонах. Источники и носители конфиденциальной информации.

Понятие об источниках, носителях и получателях информации. Классификация источников информации. Источники технической и экономической информации при научных исследованиях, разработке, производстве и эксплуатации продукции, на различных этапах и видах коммерческой деятельности. Виды носителей информации (люди, физические поля, электрические сигналы и материальные тела). Источники опасных сигналов.

Понятие об опасном сигнале и их источниках. Основные и вспомогательные технические средства и системы. Побочные электромагнитные излучения и наводки. Акустоэлектрические преобразователи, их виды и принципы работы. Принципы высокочастотного навязывания. Высокочастотные и низкочастотные побочные излучения технических средств и систем (ТСС). Паразитная генерация усилителей. Виды паразитных связей между цепями ТСС. Паразитные наводки в цепях электропитания, заземления, в токопроводящих конструкциях помещений и зданий.

### **Лабораторные работы.**

Мониторинг радиоэлектронной обстановки в защищаемом помещении с помощью скоростного поискового приемника радиосигналов «СКОРПИОН»

Определение частоты работающей радиозакладки с использованием скоростного поискового приемника радиосигналов «СКОРПИОН».

### **Задания для самостоятельной работы.**

1. проработка конспектов лекций и вопросов, вынесенных на самостоятельное изучение основной и дополнительной литературы
2. подготовка к тестированию

## **Тема 3. Угрозы безопасности информации. (ПК-4)**

### **Лекция.**

Виды угроз безопасности информации.

Виды потенциальных угроз безопасности информации. Преднамеренные и случайные воздействия на источники информации. Утечка информации и ее особенности. Подходы к оценке уровня угрозы. Факторы, влияющие на возможность реализации угроз.

Органы разведки.

Роль разведки в деятельности государств и коммерческих структур. Структура органов разведки. Виды зарубежной разведки и разведки коммерческих структур. Классификация технической разведки по физической природе носителя. Носители технических средств разведки. Принципы ведения разведки.

Технология разведки. Основные принципы и этапы добывания информации. Структура органов управления, добывания и информационной работы. Видовая и комплексная обработка данных и сведений.

Способы несанкционированного доступа к источникам информации.

Понятие о разведывательном контакте и его условиях. Виды доступа к источникам информации (физический контакт и дистанционный доступ). Принципы доступа к источникам информации без физического проникновения к контролируемой зоне. Классификация и характеристики наземных средств дистанционного съема информации с носителей. Принципы доступа к источникам информации без нарушения государственной границы. Возможности зарубежной космической, воздушной и морской разведки в мирное время.

Способы и средства добывания информации техническими средствами. Способы и средства наблюдения. Факторы, влияющие на эффективность обнаружения и распознавания объектов наблюдения. Структура и основные характеристики средств наблюдения. Параметры зрительной системы человека. Классификация и основные характеристики объективов. Виды и технические характеристики визуально-оптических приборов.

Способы и средства перехвата сигналов. Задачи, решаемые при перехвате сигналов. Структура средств перехвата и их функции. Классификация и характеристики антенн. Структура радиоприемника и его характеристики. Особенности и основные характеристики сканирующих радиоприемников. Принципы определения координат источников радиоизлучений и анализа сигналов.

Способы и средства подслушивания акустических сигналов. Параметры слуховой системы человека. Структура и характеристики технических средств подслушивания. Классификация и характеристики микрофонов. Виды и принципы работы остронаправленных микрофонов. Стетоскопы. Принципы работы и характеристики диктофонов для скрытной записи. Классификация и характеристики закладных устройств. Варианты камуфлирования закладных устройств. Способы и средства лазерного подслушивания и ВЧ-навязывания. Способы и средства добывания информации о демаскирующих признаках веществ. Способы и возможности определения демаскирующих признаков веществ.

Технические каналы утечки информации. Характеристики каналов утечки информации. Структура технических каналов утечки информации. Отличия технического канала утечки информации от канала связи. Виды технических каналов утечки информации. Типовая структура технического канала утечки информации. Основные характеристики технических каналов утечки информации. Способы комплексного использования злоумышленниками технических каналов утечки информации.

Оптические каналы утечки информации. Структура оптического канала утечки информации. Условия освещенности объектов наблюдения в видимом и ИК-диапазонах в различные периоды времени. Характеристики среды распространения оптических лучей. Основные показатели оптоэлектронных линий связи и способы снятия с них информации. Варианты оптических каналов утечки информации для типовых контролируемых зон организации.

Радиоэлектронные каналы утечки информации. Особенности радиоэлектронных каналов утечки информации. Виды и структура радиоэлектронных каналов утечки информации. Акустические каналы утечки информации.

Структура акустического канала утечки информации. Отражение и поглощение акустических волн в среде распространения. Понятие о реверберации и влияние времени реверберации на разборчивость речи. Способы увеличения протяженности акустического канала утечки информации. Материально-вещественные каналы утечки информации. Структура материально-вещественного канала утечки информации и характеристики ее элементов.

### **Лабораторные работы.**

Лабораторная работа.

Определение частоты работающей радиозакладки с использованием скоростного поискового приемника радиосигналов "СКОРПИОН"

Лабораторная работа.

Определение мощности работающей радиозакладки с использованием портативного измерителя частоты и мощности MFP – 8000

Лабораторная работа.

Определение электромагнитных излучений работающей радиозакладки с использованием генератора шума ЛГШ-503.

#### **Задания для самостоятельной работы.**

1. проработка конспектов лекций и вопросов, вынесенных на самостоятельное изучение основной и дополнительной литературы
2. подготовка к тестированию, контрольной работе

### **Тема 4. Методы, способы и средства технической защиты информации. (ПК-4)**

#### **Лекция.**

Концепция технической защиты информации. Цели и задачи технической защиты информации. Принципы технической защиты информации. Уровни безопасности информации. Методы защиты информации. Сущность инженерной защиты и технической охраны источников информации. Понятие об информационном портрете объекта защиты. Способы изменения информационного портрета при маскировке и дезинформировании. Зависимость качества информации от отношения мощностей носителя информации и помехи. Сущность энергетического скрытия. Показатели эффективности технической защиты информации

Способы и средства инженерной защиты и технической охраны. Концепция охраны объектов. Категорирование объектов охраны. Демаскирующие признаки злоумышленника и стихийных сил (пожара, воды). Модели злоумышленников. Уровни физической безопасности объектов охраны. Типовая структура системы охраны. Системы автономной и централизованной охраны. Основные показатели системы охраны. Показатели эффективности технической охраны объектов.

Способы и средства инженерной защиты объектов. Типовые инженерные конструкции. Естественные и искусственные преграды. Двери и ворота. Виды замков. Способы и средства защиты окон. Виды стекол, используемых для укрепления окон. Контрольно-пропускные пункты пропуска людей и автотранспорта. Способы и средства идентификации людей. Металлические шкафы, сейфы и хранилища. Показатели стойкости сейфов и хранилищ.

Способы и средства обнаружения злоумышленников и пожара. Структура комплекса технических средств охраны. Классификация извещателей. Принципы работы и основные характеристики контактных извещателей. Акустические извещатели. Оптико-электронные извещатели. Микроволновые (радиоволновые) извещатели. Вибрационные извещатели. Емкостные извещатели. Тепловые и ионизационные извещатели. Комбинированные извещатели. Помехи работе извещателей. Рекомендации по установке извещателей. Приемно-контрольные приборы, их назначение, классификация и основные характеристики. Пульты централизованного наблюдения.

Способы и средства видеоконтроля. Структура системы видеоконтроля. Способы и средства нейтрализации угроз. Виды способов и средств нейтрализации угроз. Подразделение охраны. Средства тревожной сигнализации. Средства управления системой охраны. Способы и средства передачи извещений. Автоматизированные интегральные системы охраны объектов, их структура и тенденция развития.

Способы и средства защиты информации от наблюдения. Способы и средства противодействия наблюдению в оптическом диапазоне волн.

Виды маскировки и их сущность. Особенности маскировки в видимом и ИК-диапазонах света. Виды и принципы применения искусственных масок, аэрозолей и воздушной пены. Способы и средства противодействия радиолокационному и гидроакустическому наблюдению. Способы информационного скрытия объектов от радиолокационного наблюдения. Средства дезинформирования и пассивного зашумления изображения на экране радиолокатора. Способы уменьшения эффективной площади рассеяния объекта наблюдения. Виды радиопоглощающих покрытий. Способы активного подавления сигналов радиолокаторов.



Способы и средства защиты информации от подслушивания. Способы и средства информационного скрывания акустических сигналов и речевой информации. Способы и средства информационного скрывания информации от подслушивания. Виды информационного скрывания речевой информации. Классификация способов технического закрытия. Сущность способов технического закрытия, их сравнительный анализ. Типы и параметры скремблеров.

Способы и средства энергетического скрывания акустических сигналов.

Методы энергетического скрывания акустических сигналов: звукоизоляция и звукопоглощение. Классификация, сущность и параметры звукоизоляции ограждений, кабин, акустических экранов, глушителей. Способы повышения звукоизоляции окон и дверей. Основные звукопоглощающие материалы и способы их применения. Типы и способы применения генераторов акустического и вибрационного зашумления. Способы оценки энергетических и информационных показателей безопасности речевой информации.

Способы и средства предотвращения утечки информации с помощью закладных устройств. Основные демаскирующие признаки проводных и радиозакладных устройств, качественная оценка их информативности. Классификация средств обнаружения, локализации и подавления закладных устройств. Принципы работы и основные характеристики обнаружителей электромагнитного поля, их достоинства и недостатки, способы применения. Возможности бытовых приемников и селективных вольтметров. Особенности специальных радиоприемников. Типы и параметры сканирующих приемников. Состав, принципы работы, возможности и параметры автоматизированных комплексов радиоконтроля помещений. Способы контроля телефонных линий и цепей электропитания. Способы подавления сигналов закладных устройств. Типы генераторов радиопомех.

Способы и средства предотвращения утечки информации через побочные электромагнитные излучения и наводки. Требования к средствам подавления сигналов побочных электромагнитных излучений и наводок. Методы и средства пассивного подавления опасных сигналов акустоэлектрических преобразователей. Экранирование электрических, магнитных и электромагнитных полей. Экранирование проводов и кабелей. Материалы для экранирования. Требования к заземлению и конструкция заземлителей. Развязка и фильтрация цепей электропитания. Средства активного линейного и пространственного зашумления.

Способы предотвращения утечки информации по материально-вещественному каналу. Классификация способов предотвращения утечки информации по материально-вещественному каналу. Способы и средства уничтожения информации, содержащейся в отходах делового и промышленного производства. Способы и средства стирания информации магнитных носителей. Способы защиты демаскирующих веществ.

### **Лабораторные работы.**

Поиск технических средств негласного съема информации по диэлектрической проницаемости среды.

### **Задания для самостоятельной работы.**

1. проработка конспектов лекций и вопросов, вынесенных на самостоятельное изучение основной и дополнительной литературы
2. подготовка к тестированию, контрольной работе

## **Тема 5. Организация инженерно-технической защиты информации (ПК-4)**

### **Лекция.**

Общие положения по инженерно-технической защите информации в организации.

Краткая характеристика государственной системы защиты информации. Основные руководящие и нормативные документы по организации инженерно-технической защиты информации в организации, их сущность.

Организационные и технические меры по инженерно-технической защите информации в организации.

Основные направления инженерно-технической защиты информации в организации. Сущность организационных и технических мер по защите информации в организации. Задачи и виды контроля эффективности защиты информации.

### **Лабораторные работы.**

Блокирование сигналов сотовых телефонов с помощью многоканального генератора радиопомех КВАРТЕТ. Радиоэлектронное подавление технических средств негласного съема информации

### **Задания для самостоятельной работы.**

1. Проработка конспектов лекций и вопросов, вынесенных на самостоятельное изучение основной и дополнительной литературы
2. Подготовка к тестированию, контрольной работе

## **Тема 6. Основы методического обеспечения инженерно-технической защиты информации (ПК-4)**

### **Лекция.**

Системный подход к защите информации. Сущность системного подхода и системного анализа. Характеристики системы защиты информации. Сущность характеристик системы защиты информации. Частный и глобальный критерии эффективности системы защиты. Алгоритм проектирования системы.

Моделирование объекта защиты.

Сущность и методические рекомендации по структурированию защищаемой информации. Выявление и описание источников информации. Формы представления моделей объектов информационной безопасности.

Моделирование угроз информации.

Виды моделей угроз информации: путей физического проникновения злоумышленника к источнику и каналов утечки. Методические рекомендации по определению путей проникновения злоумышленника к источнику информации, формы моделей. Типовые индикаторы каналов утечки. Методические рекомендации по моделированию каналов утечки. Формы представления результатов моделирования. Рекомендации по оценке угроз безопасности информации.

Методические рекомендации по разработке мер защиты.

Основные способы и средства защиты информации от типовых вариантов угроз. Рекомендации по оценке затрат на защиту и форме их представления.

Комплексирование мер защиты. Оптимизация проекта системы (предложений) защиты информации. Требования к оформлению проекта системы (предложений) при представлении на согласование и утверждений. Тенденции развития методического обеспечения защиты информации.

### **Лабораторные работы.**

Поиск радиозакладных устройств с использованием портативного металлодетектора АКА 7202М

### **Задания для самостоятельной работы.**

1. Проработка конспектов лекций и вопросов, вынесенных на самостоятельное изучение основной и дополнительной литературы
2. Подготовка к тестированию, лабораторной работе

## **4. Контроль знаний обучающихся и типовые оценочные средства**

### **4.1. Распределение баллов:**

4 семестр

- посещаемость – 20 баллов
- текущий контроль – 60 баллов
- контрольные срезы – 2 среза по 10 баллов каждый
- премиальные баллы – 20 баллов

Распределение баллов по заданиям:

№ те мы	Название темы / вид учебной работы	Формы текущего контроля / срезы	Мах. кол-во баллов	Методика проведения занятия и оценки
1.	Введение	Собеседование	20	<p>Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.</p> <p>Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> <li>- правильность ответа по содержанию;</li> <li>- полнота и глубина ответа;</li> <li>- сознательность ответа;</li> <li>- логика изложения материала;</li> <li>- рациональность использованных приемов и способов решения поставленной учебной задачи;</li> <li>- своевременность и эффективность использования наглядных пособий и технических средств при ответе;</li> <li>- использование дополнительного материала;</li> <li>- рациональность использования времени, отведенного на задание.</li> </ul> <p>20 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>15 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>10 баллов – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается.</p>
		Тестирование(контрольный срез)	10	<p>Тест состоит из 15 вопросов.</p> <p>10 балла – студент правильно отвечает на 75-100% вопросов в тесте.</p> <p>6 баллов - студент правильно отвечает на 50-75% вопросов в тесте.</p> <p>2 балла - студент правильно отвечает на 25-50% вопросов в тесте.</p> <p>Менее 25% правильных ответов баллов не дает</p>

2.	Объекты информационн ой безопасности.	Собеседо вание	20	<p>Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.</p> <p>Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> <li>- правильность ответа по содержанию;</li> <li>- полнота и глубина ответа;</li> <li>- сознательность ответа;</li> <li>- логика изложения материала;</li> <li>- рациональность использованных приемов и способов решения поставленной учебной задачи;</li> <li>- своевременность и эффективность использования наглядных пособий и технических средств при ответе;</li> <li>- использование дополнительного материала;</li> <li>- рациональность использования времени, отведенного на задание.</li> </ul> <p>20 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>15 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>10 баллов – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается.</p>
3.	Угрозы безопасности информации.	Защита лаборатор ных работ	20	<p>Лабораторные работы выполняются по тематике практических занятий.</p> <p>20 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию</p> <p>15 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы</p> <p>10 баллов - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы</p>
		Тестиров ание(кон трольны й срез)	10	<p>Тест состоит из 15 вопросов.</p> <p>10 баллов – студент правильно отвечает на 75-100% вопросов в тесте</p> <p>6 баллов - студент правильно отвечает на 50-75% вопросов в тексте</p> <p>2 балла - студент правильно отвечает на 25-50% вопросов в тесте.</p> <p>Менее 25% правильных ответов баллов не дает</p>

4.	Посещаемость	20	20 баллов – стопроцентное посещение занятий студентом 13-15 баллов – посещаемость студента составляет не менее 80 % занятий 9-12 баллов – посещаемость студента составляет не менее 50 % занятий 5-8 баллов – посещаемость студента составляет не менее 25 % занятий
5.	Премияльные баллы	20	Дополнительные премиальные баллы могут быть начислены: - за проект, выполненный по заказу работодателя и реализованный на практике – 20 баллов; - постоянная активность во время практических занятий – 10 баллов; - полностью подготовленная к публикации статья по тематике в рамках дисциплины – 10 баллов; - участие с докладом во всероссийской олимпиаде по тематике изучаемой дисциплины – 20 баллов; - участие в выставке по тематике изучаемой дисциплины – 20 баллов; - публикация статьи по тематике изучаемой дисциплины в сборнике студенческих работ / материалах всероссийской конференции / журнале из перечня ВАК – 10 / 15 / 20
6.	Итого за семестр	100	

#### 5 семестр

- посещаемость – 10 баллов
- текущий контроль – 52 балла
- контрольные срезы – 2 среза по 4 балла каждый
- премиальные баллы – 20 баллов
- ответ на экзамене: не более 30 баллов

#### Распределение баллов по заданиям:

№ те мы	Название темы / вид учебной работы	Формы текущего контроля / срезы	Мах. кол-во баллов	Методика проведения занятия и оценки
1.	Методы, способы и средства технической защиты информации.	Защита лабораторных работ	11	Лабораторные работы выполняются по тематике практических занятий. 11 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию 9 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы 6 баллов - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы
		Тестирование(контрольный срез)	4	Тест состоит из 15 вопросов. 4 балла – студент правильно отвечает на 50-100% вопросов в тесте 2 балла - студент правильно отвечает на 25-50% вопросов в тесте. Менее 25% правильных ответов баллов не дает

		Реферат	5	<p>5 баллов – реферат выполнен обучающимся самостоятельно, в полном объеме, с соблюдением необходимых технических параметров; стиль изложения отвечает специфике жанра научной работы; во введении логично, объективно и аргументировано характеризуется научная проблема; содержание реферата включает самостоятельное исследование, а заключение содержит выводы, логично вытекающие из содержания основной части; список литературы оформлен в соответствии с правилами ГОСТа</p> <p>3 балла – во введении четко сформулированы основные позиции реферата, а содержание соответствует теме реферата; в содержании реферата логично, связно, но недостаточно полно излагается теоретическая или практическая часть; заключение содержит выводы, логично вытекающие из содержания основной части; стиль изложения соответствует специфике жанра научной работы; в оформлении списка литературы встречаются незначительные погрешности</p> <p>1-2 балла – текст реферата представляет несамостоятельное (компиляция; плагиат) научное исследование; реферат написан с несоблюдением технических и научных требований</p>
2.	Организация инженерно-технической защиты информации	Защита лабораторных работ	20	<p>Лабораторные работы выполняются по тематике практических занятий.</p> <p>20 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию</p> <p>15 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы</p> <p>10 баллов - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы</p>
3.	Основы методического обеспечения инженерно-технической защиты информации	Защита лабораторных работ	16	<p>Лабораторные работы выполняются по тематике практических занятий.</p> <p>16 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию</p> <p>12 баллов – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы</p> <p>8 баллов - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы</p>
		Тестирование(контрольный срез)	4	<p>Тест состоит из 15 вопросов.</p> <p>4 балла – студент правильно отвечает на 50-100% вопросов в тесте</p> <p>2 балла - студент правильно отвечает на 25-50% вопросов в тесте.</p> <p>Менее 25% правильных ответов баллов не дает</p>

4.	Посещаемость	10	<p>10 баллов – стопроцентное посещение занятий студентом</p> <p>7-9 баллов – посещаемость студента составляет не менее 80 % занятий</p> <p>4-6 баллов – посещаемость студента составляет не менее 50 % занятий</p> <p>1-3 балла – посещаемость студента составляет не менее 25 % занятий</p>
5.	Премияльные баллы	20	<p>Дополнительные премияльные баллы могут быть начислены:</p> <ul style="list-style-type: none"> <li>- за проект, выполненный по заказу работодателя и реализованный на практике – 20 баллов;</li> <li>- постоянная активность во время практических занятий – 10 баллов;</li> <li>- полностью подготовленная к публикации статья по тематике в рамках дисциплины – 10 баллов;</li> <li>- участие с докладом во всероссийской олимпиаде по тематике изучаемой дисциплины – 20 баллов;</li> <li>- участие в выставке по тематике изучаемой дисциплины – 20 баллов;</li> <li>- публикация статьи по тематике изучаемой дисциплины в сборнике студенческих работ / материалах всероссийской конференции / журнале из перечня ВАК – 10 / 15 / 20</li> </ul>
6.	Ответ на экзамене	30	<p>Оценка «удовлетворительно»- студент имеет достаточный минимальный объем знаний по дисциплине; студентом усвоена основная литература, рекомендованная учебной программой; студент умеет ориентироваться в основных теориях, концепциях и направлениях по дисциплине и давать им оценку; студент умеет делать выводы без существенных ошибок;</p> <p>Оценка «хорошо» – «достаточно полные и систематизированные знания по дисциплине;» умение ориентироваться в основном теориях, концепциях и направлениях дисциплины и давать им критическую оценку; использование научной терминологии, лингвистически и логически правильное изложение ответа на вопросы, умение делать обоснованные выводы; владение инструментарием по дисциплине, умение его использовать в постановке и решении научных и профессиональных задач; усвоение основной и дополнительной литературы, рекомендованной учебной программой по дисциплине; самостоятельная работа на практических занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий; средний уровень сформированности заявленных в рабочей программе компетенций.</p> <p>- Оценка «отлично» – систематизированные и гл и полные знания по всем разделам дисциплины, а также по основным вопросам, выходящим за пределы учебной программы; точное использование научной терминологии систематически грамотное и логически правильное изложение ответа на вопросы; безупречное владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке научных и практических задач; выраженная способность самостоятельно и творчески решать сложные проблемы и нестандартные ситуации; полное и глубокое усвоение основной и дополнительной литературы, рекомендованной учебной программой по дисциплине; умение ориентироваться в теориях, концепциях и направлениях дисциплины и давать им критическую оценку, используя научные достижения других дисциплин; творческая самостоятельная работа; активное участие в групповых обсуждениях.</p>

7.	Итого за семестр	100	
----	------------------	-----	--

Итоговая оценка по экзамену выставляется в 100-балльной шкале и в традиционной четырехбалльной шкале. Перевод 100-балльной рейтинговой оценки по дисциплине в традиционную четырехбалльную осуществляется следующим образом:

100-балльная система	Традиционная система
85 - 100 баллов	Отлично
70 - 84 баллов	Хорошо
50 - 69 баллов	Удовлетворительно
Менее 50	Неудовлетворительно

#### 4.2 Типовые оценочные средства текущего контроля

### Защита лабораторных работ

#### Тема 3. Угрозы безопасности информации.

Лабораторная работа.

Определение частоты работающей радиозакладки с использованием скоростного поискового приемника радиосигналов "СКОРПИОН"

Лабораторная работа.

Определение мощности работающей радиозакладки с использованием портативного измерителя частоты и мощности MFP – 8000

Лабораторная работа.

Определение электромагнитных излучений работающей радиозакладки с использованием генератора шума ЛГШ-503.

#### Тема 4. Методы, способы и средства технической защиты информации.

Лабораторная работа №1

Поиск технических средств негласного съема информации по диэлектрической проницаемости среды.

Лабораторная работа №2

Поиск пассивных средств защиты помещений и аппаратуры.

Лабораторная работа №3

Поиск специальных технических средств распознавания пользователей ПК.

#### Тема 5. Организация инженерно-технической защиты информации

Лабораторная работа №1

Блокирование сигналов сотовых телефонов с помощью многоканального генератора радиопомех КВАРТЕТ. Радиоэлектронное подавление технических средств негласного съема информации

Лабораторная работа №2

Защита от утечки речевой информации при проведении конфиденциальных переговоров от ее перехвата с помощью Устройства защиты конфиденциальных переговоров TF-012N.

Предоставить результат виде отчета.

#### Тема 6. Основы методического обеспечения инженерно-технической защиты информации

Лабораторная работа №1

Поиск радиозакладных устройств с использованием портативного металлодетектора АКА 7202М

Лабораторная работа №2

Поиск подслушивающих устройств и измерение частоты радиосигналов с помощью Cub.



## Реферат

Тема 4. Методы, способы и средства технической защиты информации.

1. Законодательство о персональных данных.
3. Защита авторских прав.
4. Назначение, функции и типы систем видеозащиты.
5. Как подписывать с помощью ЭЦП электронные документы различных форматов.
6. Обзор угроз и технологий защиты Wi-Fi-сетей.
7. Проблемы внедрения дискового шифрования.
8. Борьба со спамом: основные подходы, классификация, примеры, прогнозы на будущее.
9. Особенности процессов аутентификации в корпоративной среде.
10. Квантовая криптография.
11. Утечки информации: как избежать. Безопасность смартфонов.
12. Безопасность применения пластиковых карт - законодательство и практика.
13. Защита CD- и DVD-дисков от копирования.
14. Современные угрозы и защита электронной почты.
15. Программные средства анализа локальных сетей на предмет уязвимостей.
16. Безопасность применения платежных систем - законодательство и практика.
17. Аудит программного кода по требованиям безопасности.
18. Антишпионское ПО (antispware).
19. Обеспечение безопасности Web-сервисов.
20. Защита от внутренних угроз.
21. Технологии RFID.
22. Уничтожение информации на магнитных носителях.
23. Ботнеты - плацдарм современных кибератак.
24. Цифровые водяные знаки в изображениях.
25. Электронный документооборот. Модели нарушителя.
26. Идентификация по голосу. Скрытые возможности.
27. Безопасность океанских портов.
28. Безопасность связи.
29. Безопасность розничной торговли.
30. Банковская безопасность.
31. Информатизация управления транспортной безопасностью.
32. Биопаспорт.
33. Обзор современных платформ архивации данных.
34. Что такое консалтинг в области ИБ.
35. Бухгалтерская отчетность как источник рассекречивания информации.
36. Управление рисками: обзор потребительских подходов.
37. Категорирование информации и информационных систем. Обеспечение базового уровня информационной безопасности.
38. Распределенные атаки на распределенные системы.
39. Оценка безопасности автоматизированных систем.
40. Windows и Linux: что безопаснее?
41. Функциональная безопасность программных средств.
42. Технологические процессы и стандарты обеспечения функциональной безопасности в жизненном цикле программных средств.

### 43. Информационная безопасность: экономические аспекты.

#### Собеседование

##### Тема 1. Введение

1. Основные направления, методы и средства технического противодействия закладным устройствам.
2. Оптико-электронный канал утечки речевой информации. Лазерные микрофоны интерферометрического и дифференциально-интерферометрического принципов действия.
3. Понятие о демаскирующих признаках объекта. Демаскирующие признаки сигналов.
4. Механизм (методика, принцип) обнаружения и классификации опасных сигналов.
5. Методы локализации закладных устройств. Метод энергетического зондирования. Метод акустической и радиолокационной триангуляции.
6. Атрибуты и признаки потенциально опасного сигнала закладных устройств.
7. Государственная система (иерархия) в области технических средств защиты информации. Основные руководящие, нормативные и методические документы.
8. Технический контроль эффективности мер по защите информации. Общая методика проведения технического контроля (ПЭМИН, акустических и виброакустических каналов утечки).

##### Тема 2. Объекты информационной безопасности.

1. Основные свойства информации как предмета защиты.
2. Виды защищаемой информации.
3. Демаскирующие признаки объектов защиты (видовые признаки, демаскирующие признаки сигналов, демаскирующие признаки веществ).
4. Виды источников и носителей информации.
5. Принципы записи и съема информации с носителя.
6. Источники сигналов.
7. Побочные электромагнитные излучения.
8. Опасные сигналы и поля.
9. Паразитные связи и наводки.

#### Тестирование

##### Тема 1. Введение

К техническим средствам приема, обработки, хранения и передачи информации (ТСПИ) относятся:

- а) (!) средства и системы информатизации;
- б) средства открытой телефонной связи;
- в) системы пожарной и охранной сигнализации;
2. К вспомогательным техническим средствам и системам (ВТСС) относятся:
  - а) средства и системы информатизации;
  - б) (!) средства открытой телефонной связи;
  - в) программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение).
3. Опасной зоной 2 называется:
  - а) (!) зона, в пределах которой отношение “информационный сигнал/помеха” превышает допустимое нормированное значение
  - б) пространство вокруг ТСПИ, в пределах которого на случайных антеннах наводится информационный сигнал выше допустимого (нормированного) уровня

4. Опасной зоной 2 называется:

- а) зона, в пределах которой отношение “информационный сигнал/помеха” превышает допустимое нормированное значение;
- б) (!) пространство вокруг ТСПИ, в пределах которого на случайных антеннах наводится информационный сигнал выше допустимого (нормированного) уровня.

5. Сосредоточенная случайная антенна это:

- а) (!)компактное техническое средство;
- б) кабели, провода, металлические трубы.

### Тема 3. Угрозы безопасности информации.

1. Распределенным случайным антеннам:

- а) (?) компактное техническое средство;
- б) (!) кабели, провода, металлические трубы.

2. Носителем речевой акустической информации являются:

- а) (!) механические колебания частиц упругой среды;
- б) (?) электрический ток;
- с) (?) электромагнитные волны.

3. Сигнал – это:

- а) (!)отображение процесса изменения данных во времени при их обработке;
- б) (?) физическая величина, изменяющаяся во времени.

4. Информационный сигнал – это:

- а) (!) сигнал однозначно отображающий информацию;
- б) (?) информация, зафиксированная на материальном носителе.

### Тема 4. Методы, способы и средства технической защиты информации.

1. Видовые демаскирующие признаки видимом свете это:

- а) (!) фотометрические и геометрические характеристики объекта;
- б) (?) температура поверхности;
- с) (!) тени, дым, пыль, следы на грунте, снеге, воде;
- д) (!) Взаимное расположение элементов объекта;
- е) (!)Расположение объекта по отношению к другим объектам.

2. Видовые демаскирующие признаки ИК-диапазоне:

- а) (?) фотометрические характеристики объекта;
- б) (!) геометрические характеристики объекта;
- с) (!)температура поверхности.

3. Видовые демаскирующие признаки в радиодиапазоне:

- а) (!) излучение;
- б) (!)Отражение;
- с) (?) фотометрические характеристики объекта;
- д) (?) геометрические характеристики объекта.

4. Сигналы по форме классифицируются:

- а) (!) аналоговые;
- б) (!)дискретные;
- с) (?) акустические;
- д) (?) электромагнитные;
- е) (?) корпускулярные.

5. Сигналы по физической природе классифицируются:

- а) (?) аналоговые;
- б) (?) дискретные;

- с) (!) акустические;
  - д) (!) электромагнитные;
  - е) (!) корпускулярные;
  - ф) (!) электрические;
  - г) (!) магнитные;
  - h) (!) материально-вещественные.
6. Сигналы по виду информации классифицируются:
- а) (?) аналоговые;
  - б) (?) дискретные;
  - с) (?) акустические;
  - д) (!) Речевые;
  - е) (!) Телеграфные;
  - ф) (!) Телекодовые;
  - г) (!) Факсимильные;
  - h) (!) Телевизионные;
  - и) (!) Условные.

#### Тема 6. Основы методического обеспечения инженерно-технической защиты информации

1. Демаскирующие признаки веществ по строению делятся на:
  - а) (!) Макроскопическое, микроскопическое, субмикроскопическое;
  - б) (?) Физическое, химическое, изотопное, ионное.
2. Демаскирующие признаки веществ по составу делятся на:
  - а) (?) Макроскопический, микроскопический, субмикроскопический;
  - б) (!) Физический, химический, изотопный, ионный.
3. Демаскирующие признаки веществ по свойствам делятся на:
  - а) (!) механические, химические, акустические, тепловые, лучистые,
  - б) электрические, магнитные, ядерные;
  - с) (?) Макроскопический, микроскопический, субмикроскопический.
4. Носитель информации это:
  - а) (!) материальные объекты и субъекты, обеспечивающие запись, хранение и передачу информации в пространстве и времени;
  - б) (?) информационный сигнал, отображающий сообщение.
5. Запись информации это:
  - а) (!) изменение параметров носителя информации;
  - б) (?) модуляция параметров сигнала.
6. Съём информации это:
  - а) (!) регистрация (воспроизведение) изменений параметров носителя информации, возникших в процессе записи информации;
  - б) (?) детектирование и демодуляция сигнала.
7. Запись информации на материальные тела происходит путем:
  - а) (!) изменения физической структуры и химического состава;
  - б) (?) изменения параметров поля (токов);
  - с) (?) изменения параметров сигналов.
8. Запись информации на носители в виде полей (токов) происходит путем:
  - а) (?) изменения физической структуры и химического состава;
  - б) (!) изменения параметров поля (токов) – изменение параметров сигналов.

9. Модуляция это:

- a) (!) Непрерывное изменение параметров сигналов;
- b) (?) Дискретное изменение параметров сигналов.

10. Манипуляция это:

- a) (?) Непрерывное изменение параметров сигналов;
- b) (!) Дискретное изменение параметров сигналов.

11. Источник сигнала это:

- a) (!) объект, излучающий или переизлучающий (отражающий) сигнал;
- b) (?) радио и электротехнические элементы и устройства.

12. Функциональные источники сигналов это:

- a) (!) устройства, созданные для обеспечения связи между санкционированными абонентами;
- b) (?) случайно возникающие в результате побочных излучений и наводок.

13. Источники опасных сигналов это:

- a) (?) устройства, созданные для обеспечения связи между санкционированными абонентами;
- b) (!) случайно возникающие в результате побочных излучений и наводок.

14. Основные источники сигналов:

- a) (!) обеспечивают обработку, хранение и передачу защищаемой информации;
- b) (?) обеспечивают обработку, хранение и передачу открытой информации.

4.3 Промежуточная аттестация по дисциплине проводится в форме зачета, экзамена

#### **Типовые вопросы зачета (ПК-4)**

1. Представление сил и средств защиты информации в виде системы.
2. Классификация угроз информационной безопасности по природе возникновения.
3. Классификация угроз информационной безопасности по степени преднамеренности проявления.
4. Классификация угроз информационной безопасности по непосредственному источнику угроз.
5. Классификация угроз информационной безопасности по степени воздействия на АС.
6. Основные виды угроз для АС.
7. Структура, классификация и основные характеристики технических каналов утечки информации. Простые и составные технические каналы утечки информации.
8. Подсистемы обнаружения злоумышленников и пожара, видеоконтроля, нейтрализации угроз и управления.
9. Основные направления инженерно-технической защиты информации. Свойства информации, влияющие на ее безопасность.
10. Пространственное, энергетическое и структурное скрывание информации и ее носителей.

#### **Типовые задания для зачета (ПК-4)**

1. В каком техническом канале утечки информации в качестве носителей выступают электрические, электромагнитные и магнитные поля?
  - (1) оптический
  - (2) радиоэлектронный
  - (3) акустический
  - (4) материально-вещественный
2. В каком техническом канале утечки информации в качестве носителей используются упругие акустические волны?
  - (1) оптический
  - (2) радиоэлектронный

- (3) акустический
- (4) материально-вещественный

3. Информативность канала оценивается по:

- (1) количеству информации, которую может передать канал
- (2) ценности информации, которая передается каналом
- (3) величине помех в канале
- (4) величине затухания сигнала в канале

4. Каналы, в которых утечка информации носит достаточно регулярный характер, называются:

- (1) постоянные
- (2) периодические
- (3) эпизодические
- (4) неконтролируемые

5. Как называется процесс изменения параметров сигнала в зависимости от передаваемой информации?

- (1) демодуляция
- (2) модуляция
- (3) фрагментация
- (4) интерпретация

#### **Типовые вопросы экзамена (ПК-4)**

1. Основные свойства информации как предмета защиты.
2. Виды защищаемой информации.
3. Демаскирующие признаки объектов защиты (видовые признаки, демаскирующие признаки сигналов, демаскирующие признаки веществ).
4. Виды источников и носителей информации.
5. Принципы записи и съема информации с носителя.
6. Источники сигналов.
7. Побочные электромагнитные излучения.
8. Опасные сигналы и поля.
9. Паразитные связи и наводки.
10. Виды угроз информации.
11. Способы несанкционированного доступа к конфиденциальной информации.
12. Добывание информации без проникновения в контролируемую зону.
13. Показатели эффективности добывания информации.
14. Способы и средства добывания информации в оптическом диапазоне.
15. Технические средства наблюдения (объективы, визуально-оптические приборы, фото- и киноаппараты, средства TV наблюдения).
16. Технические средства наблюдения в инфракрасном диапазоне (приборы ночного видения, тепловизоры).
17. Способы и средства наблюдения в радиодиапазоне.
18. Способы и средства перехвата сигналов (антенны, приемники).
19. Технические средства измерения признаков сигналов.
20. Способы и средства подслушивания.
21. Технические средства подслушивания (микрофоны, аудиоманитофоны, приемники опасных сигналов).
22. Технические средства подслушивания (закладные устройства).

23. Технические средства подслушивания (средства лазерного подслушивания, средства высокочастотного навязывания).
24. Способы и средства добывания информации о радиоактивных веществах.
25. Технические каналы утечки информации (особенности, характеристики, классификация).
26. Оптические каналы утечки информации.
27. Радиоэлектронные каналы утечки информации (структура, источники).
28. Радиоэлектронные каналы утечки информации (среда распространения).
29. Классификация помех в каналах утечки.
30. Акустические каналы утечки информации.
31. Комплексное использование каналов утечки.
32. Принципы инженерно-технической защиты информации.
33. Основные методы защиты информации техническими средствами.
34. Способы и средства инженерной защиты и технической охраны.
35. Подсистема инженерной защиты.
36. Способы и средства обнаружения злоумышленников и пожара.
37. Подсистема наблюдения.
38. Средства нейтрализации угроз.
39. Методы и средства противодействия в оптическом диапазоне.
40. Способы и средства противодействия радиолокационному и гидроакустическому наблюдению.
41. Способы и средства противодействия подслушиванию.
42. Способы и средства информационного скрытия речевой информации от подслушивания.
43. Способы и средства энергетического скрытия акустического сигнала (звукоизоляция).
44. Способы и средства энергетического скрытия акустического сигнала (звукопоглощение).
45. Способы и средства энергетического скрытия акустического сигнала (зашумление).
46. Способы и средства предотвращения записи речевой информации на диктофон.
47. Способы и средства предотвращения утечки информации с помощью закладных устройств.
48. Технические средства подавления сигналов закладных устройств.
49. Способы и средства предотвращения утечки информации через побочные излучения и наводки.
50. Организация инженерно-технической защиты информации.
51. Методическое обеспечение инженерно-технической защиты информации.
52. Меры инженерно-технической защиты информации.

#### **Типовые задания для экзамена (ПК-4)**

1. К техническим средствам приема, обработки, хранения и передачи информации (ТСПИ) относятся:
  - а) (!)средства и системы информатизации;
  - б) средства открытой телефонной связи;
  - в) системы пожарной и охранной сигнализации;
2. К вспомогательным техническим средствам и системам (ВТСС) относятся:
  - а) средства и системы информатизации;
  - б) (!)средства открытой телефонной связи;
  - в) программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение).
3. Опасной зоной 2 называется:
  - а) (!) зона, в пределах которой отношение “информационный сигнал/помеха” превышает допустимое нормированное значение
  - б) пространство вокруг ТСПИ, в пределах которого на случайных антеннах наводится информационный сигнал выше допустимого (нормированного) уровня
4. Опасной зоной 2 называется:

- а) зона, в пределах которой отношение “информационный сигнал/помеха” превышает допустимое нормированное значение;
- б) (!) пространство вокруг ТСПИ, в пределах которого на случайных антеннах наводится информационный сигнал выше допустимого (нормированного) уровня.

5. Сосредоточенная случайная антенна это:

- а) (!)компактное техническое средство;
- б) кабели, провода, металлические трубы.

#### 4.4. Шкала оценивания промежуточной аттестации

##### Зачет

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
«зачтено» (50 - 100 баллов)	ПК-4	Имеет высокий уровень знаний и обладает навыками и умениями решения задач с использованием методов и теоретических представлений компьютерной экспертизы. Умеет находить цифровые следы в компьютерных системах и сетях. Способен организовывать работы по компьютерной экспертизе как часть технологического процесса защиты информации в компьютерных системах.
«не зачтено» (0 - 49 баллов)	ПК-4	Не имеет знаний и не обладает навыками и умениями решения задач с использованием методов и теоретических представлений компьютерной экспертизы. Не умеет находить цифровые следы в компьютерных системах и сетях. Не способен организовывать работы по компьютерной экспертизе как часть технологического процесса защиты информации в компьютерных системах.

##### Экзамен

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
«отлично» (85 - 100 баллов)	ПК-4	Демонстрирует высокий теоретический уровень знаний в области защиты информации от утечки по техническим каналам. Свободно применяет методики определения требований к защите информации. Понимает принципы обеспечения защиты информации и источников угроз ИБ. Способен организовывать технологический процесс защиты информации от утечки по техническим каналам в компьютерных системах.
«хорошо» (70 - 84 баллов)	ПК-4	Демонстрирует хороший теоретический уровень знаний в области защиты информации от утечки по техническим каналам. Может применять методики определения требований к защите информации. Понимает принципы обеспечения защиты информации и источников угроз ИБ. Способен организовывать технологический процесс защиты информации от утечки по техническим каналам в компьютерных системах.



«удовлетворительно» (50 - 69 баллов)	ПК-4	Демонстрирует достаточный теоретический уровень знаний в области защиты информации от утечки по техническим каналам. Затрудняется применять методики определения требований к защите информации. Не до конца понимает принципы обеспечения защиты информации и источников угроз ИБ. Показывает низкую способность организовывать технологический процесс защиты информации от утечки по техническим каналам в компьютерных системах.
«неудовлетворительно» (менее 50 баллов)	ПК-4	Не демонстрирует высокий теоретический уровень знаний в области защиты информации от утечки по техническим каналам. Не может применять методики определения требований к защите информации. Не понимает принципы обеспечения защиты информации и источников угроз ИБ. Не способен организовывать технологический процесс защиты информации от утечки по техническим каналам в компьютерных системах.

## 5. Методические указания для обучающихся по освоению дисциплины (модуля)

### 5.1 Методические указания по организации самостоятельной работы обучающихся:

Приступая к изучению дисциплины, в первую очередь обучающимся необходимо ознакомиться содержанием рабочей программы дисциплины (РПД), которая определяет содержание, объем, а также порядок изучения и преподавания учебной дисциплины, ее раздела, части.

Для самостоятельной работы важное значение имеют разделы «Объем и содержание дисциплины», «Учебно-методическое и информационное обеспечение дисциплины» и «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы».

В разделе «Объем и содержание дисциплины» указываются все разделы и темы изучаемой дисциплины, а также виды занятий и планируемый объем в академических часах.

В разделе «Учебно-методическое и информационное обеспечение дисциплины» указана рекомендуемая основная и дополнительная литература.

В разделе «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы» содержится перечень профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины.

### 5.2 Рекомендации обучающимся по работе с теоретическими материалами по дисциплине

При изучении и проработке теоретического материала необходимо:

- просмотреть еще раз презентацию лекции в системе MOODLe, повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной дополнительной литературы;
- при самостоятельном изучении теоретической темы сделать конспект, используя рекомендованные в РПД источники, профессиональные базы данных и информационные справочные системы;
- ответить на вопросы для самостоятельной работы, по теме представленные в пункте 3.2 РПД.
- при подготовке к текущему контролю использовать материалы фонда оценочных средств (ФОС).

### 5.3 Рекомендации по работе с научной и учебной литературой

Работа с основной и дополнительной литературой является главной формой самостоятельной работы и необходима при подготовке к устному опросу на семинарских занятиях, к дебатам, тестированию, экзамену. Она включает проработку лекционного материала и рекомендованных источников и литературы по тематике лекций.

Конспект лекции должен содержать реферативную запись основных вопросов лекции, в том числе с опорой на размещенные в системе MOODLe презентации, основных источников и литературы по темам, выводы по каждому вопросу. Конспект может быть выполнен в рамках распечатки выдачи презентаций лекций или в отдельной тетради по предмету. Он должен быть аккуратным, хорошо читаемым, не содержать не относящуюся к теме информацию или рисунки.

Конспекты научной литературы при самостоятельной подготовке к занятиям должны содержать ответы на каждый поставленный в теме вопрос, иметь ссылку на источник информации с обязательным указанием автора, названия и года издания используемой научной литературы. Конспект может быть опорным (содержать лишь основные ключевые позиции), но при этом позволяющим дать полный ответ по вопросу, может быть подробным. Объем конспекта определяется самим студентом.

В процессе работы с основной и дополнительной литературой студент может:

- делать записи по ходу чтения в виде простого или развернутого плана (создавать перечень основных вопросов, рассмотренных в источнике);
- составлять тезисы (цитирование наиболее важных мест статьи или монографии, короткое изложение основных мыслей автора);
- готовить аннотации (краткое обобщение основных вопросов работы);
- создавать конспекты (развернутые тезисы).

#### 5.4. Рекомендации по подготовке к отдельным заданиям текущего контроля

Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.

Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:

- правильность ответа по содержанию;
- полнота и глубина ответа;
- сознательность ответа;
- логика изложения материала;
- рациональность использованных приемов и способов решения поставленной учебной задачи;
- своевременность и эффективность использования наглядных пособий и технических средств при ответе;
- использование дополнительного материала;
- рациональность использования времени, отведенного на задание.

Устный опрос может сопровождаться презентацией, которая подготавливается по одному из вопросов практического занятия. При выступлении с презентацией необходимо обращать внимание на такие моменты как:

- содержание презентации: актуальность темы, полнота ее раскрытия, смысловое содержание, соответствие заявленной темы содержанию, соответствие методическим требованиям (цели, ссылки на ресурсы, соответствие содержания и литературы), практическая направленность, соответствие содержания заявленной форме, адекватность использования технических средств учебным задачам, последовательность и логичность презентуемого материала;
- оформление презентации: объем (оптимальное количество), дизайн (читаемость, наличие и соответствие графики и анимации, звуковое оформление, структурирование информации, соответствие заявленным требованиям), оригинальность оформления, эстетика, использование возможности программной среды, соответствие стандартам оформления;
- личностные качества: ораторские способности, соблюдение регламента, эмоциональность, умение ответить на вопросы, систематизированные, глубокие и полные знания по всем разделам программы;

- содержание выступления: логичность изложения материала, раскрытие темы, доступность изложения, эффективность применения средств ИКТ, способы и условия достижения результативности и эффективности для выполнения задач своей профессиональной или учебной деятельности, доказательность принимаемых решений, умение аргументировать свои заключения, выводы.

## **6. Учебно-методическое и информационное обеспечение дисциплины**

### **6.1 Основная литература:**

1. Большаков, А. С., Режеб, Т. Б. К. Методические указания и контрольные задания по дисциплине Инженерно-техническая защита информации. - 2022-04-04; Методические указания и контрольные задания по дисциплине Инженерно-техническая защита и. - Москва: Московский технический университет связи и информатики, 2013. - 149 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/61734.html>
2. Тамб. гос. ун-т им. Г.Р. Державина Инженерно-техническая защита информации. Акустический канал утечки. - [Тамбов]: Изд-во ТГУ, 2008. - 1 электрон. опт. диск (CD).
3. Титов, А. А. Инженерно-техническая защита информации : учебное пособие. - Весь срок охраны авторского права; Инженерно-техническая защита информации. - Томск: Томский государственный университет систем управления и радиоэлектроники, 2010. - 197 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/13931.html>
4. Тамб. гос. ун-т им. Г.Р. Державина Производственная практика "Инженерно-техническая защита информации" : электрон. УМК. - [Тамбов]: [Изд-во ТГУ], 2008. - 1 электрон. опт. диск.

### **6.2 Дополнительная литература:**

1. Скрипник Д. А. Общие вопросы технической защиты информации. - 2-е изд., испр.. - Москва: Национальный Открытый Университет «ИНТУИТ», 2016. - 425 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=429070>
2. Креопалов, В. В. Технические средства и методы защиты информации : учебное пособие. - 2021-12-31; Технические средства и методы защиты информации. - Москва: Евразийский открытый институт, 2011. - 278 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/10871.html>
3. Аверченков В. И., Рытов М. Ю. Служба защиты информации: организация и управление : учебное пособие для вузов. - 3-е изд., стер.. - Москва: Флинта, 2016. - 186 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=93356>
4. [Тамб. гос. ун-т им. Г.Р. Державина] Инженерно-техническая защита информации. Электромагнитный канал утечки. Комплекс Навигатор ПЗГ. - [Тамбов]: Изд-во ТГУ, 2008. - 1 электрон. опт. диск (CD).

### **6.3 Иные источники:**

1. Федеральный портал «Российское образование» - <http://www.edu.ru/>
2. Портал "Гуманитарное образование" - <http://www.humanities.edu.ru/>
3. Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов» - <http://school-collection.edu.ru/>
4. Федеральная служба по надзору в сфере образования и науки - <http://obrnadzor.gov.ru>
5. Вопросы образования - <http://www.ecsocman.edu.ru/vo>

## **7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы**

Для проведения занятий по дисциплине необходимо следующее материально-техническое обеспечение: учебные аудитории для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы.

Учебные аудитории и помещения для самостоятельной работы укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы укомплектованы компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета.

Для проведения занятий лекционного типа используются наборы демонстрационного оборудования, обеспечивающие тематические иллюстрации (проектор, ноутбук, экран/ интерактивная доска).

Лицензионное и свободно распространяемое программное обеспечение:

Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition. 1500-2499 Node 1 year Educational Renewal Licence

Операционная система Microsoft Windows 10

Adobe Reader XI (11.0.08) - Russian Adobe Systems Incorporated 10.11.2014 187,00 MB 11.0.08

7-Zip 9.20

Microsoft Office Профессиональный плюс 2007

Профессиональные базы данных и информационные справочные системы:

1. Электронный каталог Фундаментальной библиотеки ТГУ. – URL: <http://biblio.tsutmb.ru/elektronnyij-katalog>
2. Университетская библиотека онлайн: электронно-библиотечная система. – URL: <https://biblioclub.ru>
3. Консультант студента. Гуманитарные науки: электронно-библиотечная система. – URL: <https://www.studentlibrary.ru>
4. Научная электронная библиотека eLIBRARY.ru. – URL: <https://elibrary.ru>
5. Научная электронная библиотека Российской академии естествознания. – URL: <https://www.monographies.ru>
6. Российская национальная библиотека. – URL: <http://nlr.ru>
7. Российская государственная библиотека. – URL: <https://www.rsl.ru>
8. Президентская библиотека имени Б.Н. Ельцина. – URL: <https://www.prilib.ru>
9. Электронная библиотека РФФИ. – URL: <https://www.rfbr.ru/rffi/ru/library>

### **Электронная информационно-образовательная среда**

[https://auth.tsutmb.ru/authorize?response\\_type=code&client\\_id=moodle&state=xyz](https://auth.tsutmb.ru/authorize?response_type=code&client_id=moodle&state=xyz)

Взаимодействие преподавателя и студента в процессе обучения осуществляется посредством мультимедийных, гипертекстовых, сетевых, телекоммуникационных технологий, используемых в электронной информационно-образовательной среде университета.