Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Курганский государственный университет»
(КГУ)

Кафедра «Безопасность информационных и автоматизированных систем»

УТВЕРЖДАЮ:
Первый Проректор
_____ / С.Н. Щербич /
«30» сентября 2019 г.

Рабочая программа учебной дисциплины

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

образовательной программы высшего образования –
программы специалитета
10.05.03 Информационная безопасность автоматизированных систем
Направленность: (специализация №7) обеспечение информационной безопасности распределенных информационных систем
Форма обучения: очная

Курган 2019

Рабочая программа дисциплины «Техническая защита информации» составлена в соответствии с учебным планом по программе специалитета «Информационная безопасность автоматизированных систем» (Обеспечение информационной безопасности распределенных информационных систем), утвержденным для очной формы обучения « 29 » августа 2019 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» 27 сентября 2019 года, протокол № 2.

Рабочую программу составил:
ст. преподаватель В.В. Москвин

Согласовано:

Заведующий кафедрой «БИАС»
канд. пед. наук, доцент Е.Н. Полякова

Начальник Управления
образовательной деятельности С.Н. Синицын

Специалист по учебно-методической
работе Учебно-методического
отдела Г.В. Казанкова

1. ОБЪЕМ ДИСЦИПЛИНЫ

Всего: 9 зачетных единицы трудоемкости (324 академических часа)

Очная форма обучения

Вид учебной работы	На всю дисциплину	Семестр	
		8	9
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**192**	**96**	**96**
Лекции	64	32	32
Лабораторные работы	64	32	32
Практические занятия	64	32	32
Самостоятельная работа, всего часов в том числе:	**132**	**84**	**48**
Подготовка к зачету	18	18	-
Подготовка к экзамену	27	-	27
Другие виды самостоятельной работы (подготовка к лабораторным работам, практическим занятиям и рубежному контролю)	87	66	21
Вид промежуточной аттестации	**зачет с оценкой, экзамен**	**зачет с оценкой**	**экзамен**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**324**	**180**	**144**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Техническая защита информации» относится к базовой части Блока 1.

Изучение дисциплины базируется на результатах обучения, сформированных при изучении следующих дисциплин:

- Основы информационной безопасности.
- Программно-аппаратные средства защиты информации.
- Моделирование физических процессов в профессиональной деятельности
- Теоретические основы компьютерной безопасности.
- Безопасность сетей ЭВМ.
- Безопасность операционных систем.

Результаты обучения по дисциплине необходимы для выполнения разделов курсовых проектов по дисциплине «Разработка и эксплуатация защищенных автоматизированных систем» и «Управление информационной безопасностью», а также выпускной квалификационной работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Целью изучения дисциплины является: формирование у студентов знаний по основам инженерно-технической защиты информации, а также навыков и умений применения знаний для конкретных условий, развитие системного мышления, необходимого для решения задач инженерно-технической защиты информации с учетом требований системного подхода.

Задачи дисциплины:

- изучение основных понятий, методов и средств, используемых в технической защите информации;
- изучение способов образования технических каналов утечки информации;
- изучение методов эффективного противодействия утечки информации.

Компетенции, формируемые в результате освоения дисциплины:

- способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5);
- способность к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8);
- способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6);
- способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14);

- способность участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (ПК-15);

- способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-16);

- способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17);

- способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23);

- способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24);

- способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27).

В результате изучения дисциплины обучающийся должен:

знать:

- технические каналы утечки информации (для ОК-5, ПК-6, ПК-17, ПК-23, ПК-24);

- основы физической защиты объектов информатизации (для ОПК-8, ПК-16, ПК-23).

уметь:

- анализировать и оценивать угрозы информационной безопасности объекта (для ОПК-8, ПК-14, ПК-27).

владеть:

- методами и средствами технической защиты информации (для ОК-5, ОПК-8, ПК-6, ПК-17, ПК-24);

- методами расчета и инструментального контроля показателей технической защиты информации (для ПК-6, ПК-15, ПК-23, ПК-27).

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-тематический план. Очная форма обучения

Рубеж	Номер темы	Наименование темы	Количество часов контактной работы с преподавателем		
			Лекции	Лаборат. работы	Практич. занятия
8 семестр					
Рубеж 1	1	***Введение. Концепция инженерно-технической защиты информации.***	**8**	-	-
		Цели и задачи курса. Содержание дисциплины.	1	-	-
		Системный подход к защите информации	3	-	-
		Основные концептуальные положения инженерно-технической защиты информации.	4	-	-

	2	***Теоретические основы инженерно-технической защиты информации.***	**24**	***8***	***32***
		Информация как предмет защиты	2	-	-
Рубеж 2		Источники опасных сигналов	2	2	-
		Характеристика технической разведки	4	-	4
		Технические каналы утечки информации	4	2	
		Методы инженерно-технической защиты информации	4	-	4
		Методы инженерной защиты и технической охраны объектов	4	6	4
		Методы скрытия информации и ее носителей	4	-	20
	3	***Физические основы инженерно-технической защиты информации***	-	***24***	-
		Физические основы побочных электромагнитных излучений и наводок.	-	-	-
		Распространение сигналов в технических каналах утечки информации.	-	24	-
		Всего	**32**	**32**	**32**
9 семестр					
	3	***Физические основы инженерно-технической защиты информации***	**9**	**-**	***8***
Рубеж 1		Физические основы побочных электромагнитных излучений и наводок.	3	-	-
		Распространение сигналов в технических каналах утечки информации.	4	-	4
		Физические процессы подавления опасных сигналов.	2	-	4
	4	***Технические средства добывания и инженерно-технической защиты информации***	**9**	***14***	***12***
		Средства технической разведки	3		4
		Средства инженерной защиты и технической охраны	3		4
		Средства предотвращения утечки информации по техническим каналам.	3	14	4
Рубеж 2	***5***	***Организационные основы инженерно-технической защиты информации***	**6**	***18***	***12***
		Государственная система защиты информации	2	-	-
		Контроль эффективности инженерно-технической защиты информации.	4	18	4
	6	***Методическое обеспечение инженерно-технической защиты информации.***	**8**	-	-
		Моделирование инженерно-технической защиты информации	4	-	4
		Методические рекомендации по оценке эффективности защиты информации	4	-	4
		Всего:	**32**	**32**	**32**

4.2. Содержание лекционных занятий

Тема 1. Концепция инженерно-технической защиты информации.

1.1. Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература.

1.2. Системный подход к защите информации.

Характеристика инженерно-технической защиты информации как области информационной безопасности. Основные проблемы инженерно-технической защиты информации. Представление сил и средств защиты информации в виде системы. Основные параметры системы защиты информации.

1.3. Основные концептуальные положения инженерно-технической защиты информации.

Цели и задачи защиты информации. Ресурсы, выделяемые на защиту информации. Принципы защиты информации техническими средствами. Основные направления инженерно-технической защиты информации. Показатели эффективности инженерно-технической защиты информации.

Тема 2. Теоретические основы инженерно-технической защиты информации.

2.1. Информация как предмет защиты.

Особенности информации как предмета защиты. Свойства информации, влияющие на ее безопасность. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие о текущей и эталонной признаковой структуре.

2.2. Источники опасных сигналов.

Понятие об опасном сигнале. Основные и вспомогательные технические средства и системы, их классификация и характеристика. Опасные сигналы, образующиеся в результате акустоэлектрических преобразований. Виды побочных опасных электромагнитных излучений. Паразитные связи и наводки опасных сигналов. Случайные антенны. Виды опасных сигналов в помещении.

2.3. Характеристика технической разведки.

Основные задачи и органы технической разведки. Принципы технической разведки. Основные этапы и процессы добывания информации технической разведкой. Классификация технической разведки по видам носителя информации и средств разведки. Возможности видов технической разведки по добыванию разведывательной информации. Основные направления развития технической разведки. Модель иностранной технической разведки.

2.4. Технические каналы утечки информации.

Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Простые и составные технические каналы утечки информации. Характеристика и возможности оптических, акустических, радиоэлектронных и материально-вещественных каналов утечки информации.

2.5. Методы инженерно-технической защиты информации.

Классификация методов инженерно-технической защиты информации. Инженерная защита и техническая охрана объектов. Пространственное, энергетическое и структурное скрытие информации и ее носителей. Дезинформирование как метод скрытия. Комплексное применение методов защиты.

2.6. Методы инженерной защиты и технической охраны объектов.

Классификация методов инженерной защиты и технической охраны объектов защиты. Инженерные конструкции. Автономные и централизованные системы охраны. Модели злоумышленника. Подсистемы обнаружения злоумышленников и пожара, видеоконтроля, нейтрализации угроз и управления охраной. Способы повышения помехоустойчивости средств обнаружения злоумышленников и пожара. Автоматизация процессов охраны.

2.7. Методы скрытия информации и ее носителей.

Пространственное скрытие объектов наблюдения и сигналов. Структурное и энергетическое скрытие объектов наблюдения. Методы технического закрытия речевых сигналов. Звукоизоляция и звукопоглощение. Энергетическое скрытие радио и электрических сигналов. Виды и условия зашумления сигналов.

Тема 3. Физические основы инженерно-технической защиты информации.

3.1. Физические основы побочных электромагнитных излучений и наводок.

Акустоэлектрические преобразования. Сосредоточенные и распределенные источники побочных излучений. Характер электромагнитных излучений в ближней и дальней зонах. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок. Цепи Пикара. Физические явления, вызывающие утечку информации по цепям электропитания, заземления и токопроводящим конструкциям здания.

3.2. Распространение сигналов в технических каналах утечки информации.

Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях. Распространение оптических сигналов в атмосфере и в светопроводах. Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи. Основные показатели среды распространения сигналов, влияющие на дальность технических каналов утечки и качество информации на его выходе.

3.3. Физические процессы подавление опасных сигналов.

Подавление опасных сигналов акустоэлектрических преобразователей. Экранирование электрических, магнитных, и электромагнитных полей. Требования к экранам. Компенсация полей. Подавление опасных сигналов в цепях электропитания и заземления. Зашумление опасных сигналов помехами.

Тема 4. Технические средства добывания и инженерно-технической защиты информации.

4.1. Средства технической разведки.

Визуально-оптические приборы. Фотоаппараты. Оптоэлектронные приборы наблюдения в видимом и инфракрасном диапазонах. Акустические приемники. Направленные микрофоны. Структура комплексов перехвата. Особенности сканирующих радиоприемников. Закладные устройства, средства ВЧ-навязывания и лазерного подслушивания. Автономные средства разведки.

4.2. Средства инженерной защиты и технической охраны.

Основные инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации. Средства управления доступом. Классификация и характеристика охранных, охранно-пожарных и пожарных извещателей. Средства видеоконтроля и видеоохраны. Средства нейтрализации угроз. Средства управления и передачи извещений. Автоматизированные интегральные системы охраны.

4.3. Средства предотвращения утечки информации по техническим каналам.

Средства маскировки и дезинформирования в оптическом и радиодиапазонах. Средства звукоизоляции и звукопоглощения. Средства обнаружения, локализации и подавления сигналов закладных устройств. Средства подавления сигналов акустоэлектрических преобразователей, цепей электропитания и заземления. Генераторы линейного и пространственного зашумления.

Тема 5. Организационные основы инженерно-технической защиты информации.

5.1. Государственная система защиты информации.

Основные задачи, структура и характеристика государственной системы противодействия технической разведке. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической разведке. Основные организационные и технические меры по защите информации. Аттестация объектов, лицензирование деятельности по защите информации и сертификация ее средств.

5.2. Контроль эффективности инженерно-технической защиты информации.

Виды контроля эффективности инженерно-технической защиты информации. Требования по защите информации от утечки по техническим каналам. Методы технического контроля. Особенности инструментального контроля эффективности инженерно-технической защиты информации.

Тема 6. Методическое обеспечение инженерно-технической защиты информации.

6.1. Моделирование инженерно-технической защиты информации.

Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации. Принципы моделирования объектов защиты. Моделирование угроз безопасности информации. Методические рекомендации по выбору рациональных вариантов защиты. Способы оптимизации мер инженерно-технической защиты информации.

6.2. Методические рекомендации по оценке эффективности защиты информации.

Способы оценки эффективности охраны объектов защиты. Оценка эффективности защиты видовых признаков объектов наблюдения. Способы оценки безопасности речевой информации в помещении. Способы определения уровней опасных сигналов на выходах основных и вспомогательных техниче-

ских средств. Способы оценки размеров контролируемых зон I и II. Оценка дальности перехвата опасных сигналов.

4.3 Лабораторные работы

Номер темы	Наименование темы	Наименование лабораторной работы	Норматив времени, час.
		8 семестр	
2	Теоретические основы инженерно-технической защиты информации.	*Лабораторная работа №1.* Исследование параметров и характеристик видеокамер.	2
		Лабораторная работа №2. Цифровые диктофоны	2
		Лабораторная работа №3. Генераторы радиошума и блокираторы источников радиосигналов.	4
3	Физические основы инженерно-технической защиты информации	*Лабораторная работа №4.* Обнаружение оптических сигналов передатчиков в ИК-диапазона	4
	1-ый рубежный контроль	***Тестирование***	***2***
		Лабораторная работа №5. Обнаружение и локализация закладных устройств с помощью нелинейного локатора.	4
		Лабораторная работа №6. Обнаружение сигналов линейных и сетевых закладок	4
		Лабораторная работа №7. Многофункциональные поисковые приборы, ST-031 «Пиранья».	4
		Лабораторная работа №8. Статистический анализ загрузки заданного радиодиапазона и обнаружение радиозакладных устройств в защищаемом помещении. RS-TURBO	4
	2-ой рубежный контроль	***Тестирование***	***2***
	Всего за 8 семестр		**32**
		9 семестр	
4	Технические средства добывания и инженерно-технической защиты информации	*Лабораторная работа №1.* Защита телефонных линий от прослушивания с помощью прибора «Прокруст – 2000»	4
		Лабораторная работа №2. Технические средства для поиска работающих радиозакладок.	4
		Лабораторная работа №3. Поиск радиозакладок нелинейными радиолокаторами.	4
	1-ый рубежный контроль	***Тестирование***	***2***
5	Организационные основы инженерно-технической	*Лабораторная работа №4.* Оценка эффективности активной защиты от	4

	защиты информации.	утечек по акустическому к и виброакустическому каналам с помощью комплекса «Соната АВ 1М»	
		Лабораторная работа №5. Оценка защищенности ограждающих конструкций помещения от утечки информации по акустическому каналу комплексом «Спрут-мини».	4
		Лабораторная работа №6. Оценка защищенности ограждающих конструкций помещения от утечки информации по виброакустическому каналу комплексом «Спрут-мини».	4
	2-ой рубежный контроль	***Тестирование***	***2***
		Лабораторная работа №7. Оценка защищенности ограждающих конструкций помещения от утечки информации по каналам акустоэлектрических преобразований технических средств с помощью комплекса «Спрут-мини».	4
	Всего за 9 семестр		**32**
	Итого		**64**

4.4 Практические занятия

Номер темы	Наименование темы	Наименование тем практических занятий	Норматив времени, час.
		8 семестр	
2	Теоретические основы инженерно-технической защиты информации.	*Практическое занятие №1.* Характеристика технической разведки	4
		Практическое занятие №2. Методы инженерно-технической защиты информации	4
		Практическое занятие №3. Методы инженерной защиты и технической охраны объектов	4
		Практическое занятие №4. Пространственное скрытие объектов наблюдения и сигналов.	2
		Практическое занятие №5. Структурное и энергетическое скрытие объектов наблюдения.	2
		Практическое занятие №6. Методы технического закрытия речевых сигналов.	4
		Практическое занятие №7. Звукоизоляция и звукопоглощение.	4
		Практическое занятие №8. Энергетическое скрытие радио и электрических сигналов.	4

		Практическое занятие №9. Виды и условия зашумления сигналов.	4
	Всего за 8 семестр		**32**
		9 семестр	
3	Физические основы инженерно-технической защиты информации.	*Практическое занятие №1.* Распространение сигналов в технических каналах утечки информации.	4
		Практическое занятие №2. Физические процессы подавления опасных сигналов.	4
4	Технические средства добывания и инженерно-технической защиты информации.	*Практическое занятие №3.* Средства технической разведки	4
		Практическое занятие №4. Средства инженерной защиты и технической охраны	4
		Практическое занятие №5. Средства предотвращения утечки информации по техническим каналам.	4
5	Организационные основы инженерно-технической защиты информации.	*Практическое занятие №6.* Контроль эффективности инженерно-технической защиты информации.	4
6	Методическое обеспечение инженерно-технической защиты информации.	*Практическое занятие №7. Моделирование инженерно-технической защиты информации*	4
		Практическое занятие №8. Способы оценки эффективности охраны объектов защиты	2
		Практическое занятие №9. Оценка дальности перехвата опасных сигналов.	2
	Всего за 9 семестр		**32**
	Итого		**64**

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

При прослушивании лекций рекомендуется в конспекте отмечать все важные моменты, на которых заостряет внимание преподаватель, в частности те, которые направлены на качественное выполнение соответствующей лабораторной работы или практического занятия.

Преподавателем запланировано использование при чтении лекций технологии учебной дискуссии. Поэтому рекомендуется фиксировать для себя интересные моменты с целью их активного обсуждения на дискуссии в конце лекции.

Залогом качественного выполнения лабораторных работ и практических занятий является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Рекомендуется подготовить вопросы по неясным моментам и обсудить их с преподавателем в начале лабораторной работы или практического занятия.

Преподавателем запланировано применение на лабораторных и практических занятиях технологий развивающейся кооперации, коллективного взаимодействия, разбора конкретных ситуаций.

Для текущего контроля успеваемости по очной форме обучения преподавателем используется балльно-рейтинговая система контроля и оценки академической активности. Поэтому настоятельно рекомендуется тщательно прорабатывать материал дисциплины при самостоятельной работе, участвовать во всех формах обсуждения и взаимодействия, как на лекциях, так и на лабораторных и практических занятиях в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает самостоятельное изучение разделов дисциплины, подготовку к лабораторным и практическим занятиям, к рубежным контролям, подготовку к экзамену и зачету с оценкой.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Самостоятельное изучение тем:	**17**
- Основные концептуальные положения инженерно-технической защиты информации.	1
- Источники опасных сигналов	1
- Характеристика технической разведки	1
- Технические каналы утечки информации	1
- Методы инженерно-технической защиты информации	1
- Методы инженерной защиты и технической охраны объектов	1
- Методы скрытия информации и ее носителей	1
- Физические основы побочных электромагнитных излучений и наводок.	1
- Распространение сигналов в технических каналах утечки информации.	1
- Физические процессы подавления опасных сигналов.	1
- Средства технической разведки	1
- Средства инженерной защиты и технической охраны	1
- Средства предотвращения утечки информации по техническим каналам.	1
- Государственная система защиты информации	1
- Контроль эффективности инженерно-технической защиты информации.	1
- Моделирование инженерно-технической защиты информации	1
- Методические рекомендации по оценке эффективности защиты информации	1
Подготовка к лабораторным работам (по 1 часу на каждое занятие)	30
Подготовка к практическим занятиям (по 1 часу на каждое занятие)	32
Подготовка к рубежным контролям (по 2 часа на каждый контроль)	8
Подготовка к зачету	18
Подготовка к экзамену	27
Всего:	**132**

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Перечень оценочных средств

1. Балльно-рейтинговая система контроля и оценки академической активности студентов в КГУ.
2. Отчеты студентов по лабораторным работам
3. Отчеты студентов по практическим занятиям
4. Банк тестовых заданий к рубежным контролям № 1, № 2, №3 и №4.
5. Вопросы к зачету с оценкой
6. Вопросы к экзамену

6.2. Система балльно-рейтинговой оценки работы студентов по дисциплине

№	Наименование	Содержание						
1	Распределение баллов за семестры по видам учебной работы, сроки сдачи учебной работы *(доводятся до сведения студентов на первом учебном занятии)*	Распределение баллов						
		8 семестр						
		Вид ученой работы:	Посещение лекций	Выполнение и защита лабораторных работ	Выполнение практических заданий	Рубежный контроль №1	Рубежный контроль №2	Зачет с оценкой
		Балльная оценка:	$1_б$ x16=$16_б$	$3_б$ x 8=$24_б$	$2_б$ x 9=$18_б$	6	6	30
		9 семестр						
		Вид учебной работы:	Посещение лекций	Выполнение и защита отчетов по лабораторным работам	Выполнение практических заданий	Рубежный контроль №1	Рубежный контроль №2	Экзамен
		Балльная оценка:	$1_б$ x 16=$16_б$	$3_б$ x 7=$21_б$	2б x 9=18б	7	8	30
2	Критерий пересчета баллов в традиционную оценку по итогам работы в семестре, на зачете и экзамене.	60 и менее баллов – неудовлетворительно; 61…73 – удовлетворительно; 74… 90 – хорошо; 91…100 – отлично						

3	Критерии допуска к промежуточной аттестации, возможности получения автоматического зачета (экзаменационной оценки) по дисциплине, возможность получения бонусных баллов	Для допуска к промежуточной аттестации (экзамену, зачету с оценкой) студент должен набрать по итогам текущего и рубежного контроля не менее 50 баллов и должен выполнить все лабораторные и практические работы. Для получения экзаменационной оценки «автоматически» студенту необходимо набрать следующее минимальное количество баллов: - 68 для получения «автоматически» оценки удовлетворительно». По согласованию с преподавателем студенту, набравшему минимум 68 баллов, могут быть добавлены дополнительные (бонусные) баллы за активность на лабораторных занятиях, активное участие в научной и методической работе, оригинальность принятых решений в ходе выполнения лабораторных работ, за участие в значимых учебных и внеучебных мероприятиях кафедры и выставлена за экзамен, зачет с оценкой «автоматически» оценка «хорошо» или «отлично».
4	Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) студентов для получения недостающих баллов в конце семестра	В случае если к промежуточной аттестации (экзамену или зачету с оценкой) набрана сумма менее 50 баллов, студенту необходимо набрать недостающее количество баллов за счет выполнения дополнительных заданий, до конца последней (зачетной) недели семестра. При этом необходимо проработать материал всех пропущенных лабораторных и практических работ. Формы дополнительных заданий (назначаются преподавателем): - выполнение и защита пропущенной лабораторной или практической работы (при невозможности дополнительного проведения работы преподаватель устанавливает форму дополнительного задания по тематике пропущенной работы самостоятельно) – до 4 баллов. Ликвидация академических задолженностей, возникших из-за разности в учебных планах при переводе или восстановлении, проводится путем выполнения дополнительных заданий, форма и объем которых определяется преподавателем.

6.3. Процедура оценивания результатов освоения дисциплины

Рубежные контроли проводятся в форме письменного тестирования.

Перед проведением каждого рубежного контроля преподаватель прорабатывает со студентами основной материал соответствующих разделов дисциплины в форме краткой лекции-дискуссии. Варианты тестовых заданий для рубежных контролей состоят из 20 вопросов. На каждое тестирование при рубежном контроле студенту отводится 2 академических часа.

Баллы студенту выставляются в зависимости от числа правильно выбранных ответов. Итоговая оценка по тесту формируется путем суммирования набранных баллов и отнесения их к общему количеству вопросов в задании. Помножив полученное значение на 100%, можно привести итоговую оценку к традиционной следующим образом:

«неудовлетворительно» – менее 50%
«удовлетворительно» – 50% - 70%
«хорошо» – 70% - 90%
«отлично» – 90% - 100% .

Преподаватель оценивает в баллах результаты тестирования каждого студента по количеству правильных ответов и заносит в ведомость учета текущей успеваемости.

Зачет с оценкой и экзамен проводятся в форме ответов на вопросы. На экзамене билет состоит из 2-х вопросов и 1 практического задания. Практическое задание состоит в поиске закладного устройства в аудитории с помощью выданного технического средства. На зачете преподаватель выбирает любых 2 вопроса из перечня вопросов, которые ранее были выданы преподавателем. Вопросы к зачету и экзамену доводятся до студентов на последней лекции в семестре. Время, отводимое студенту на подготовку вопросов, составляет 1 академический час.

Результаты текущего контроля успеваемости, зачета и экзамена заносятся преподавателем в зачетную или экзаменационную ведомость, которая сдается в организационный отдел института в день зачета или экзамена, а также выставляются в зачетную книжку студента.

6.4. Примеры оценочных средств для рубежных контролей, зачета и экзамена

8 СЕМЕСТР

1-ый рубежный контроль

1. Для чего используется прибор Бархан-1?

1) Для обнаружения и локализации радиоизлучающих технических средств
2) Для технического ограничения использования мобильных телефонов на контролируемых территориях.
3) Для защиты от утечки информации за счет побочных электромагнитных излучений и наводок средств офисной техники
4) Для проверки эффективности работы устройств и комплексов радиомониторинга, используемых для обследования и защиты выделенных помещений.

2. До какой частоты максимальной частоты можно сканировать диапазон комплексом RS turbo с дополнительным конвертером?

1) До 2,2 ГГц 2) До 5 ГГц 3) До 9 ГГц

4) До 12 ГГц 5) Другой вариант: _____

2-ой рубежный контроль

1. Максимальная дальность блокирования прибором Бархан-1 составляет?

1) 10м 2) 15м 3) 20м 4) 25м

2. Средство СРМ-700 выполняет функции:

1) универсального зонд-монитора;
2) радиоприемника;
3) сканера частот;
4) нелинейного локатора.

9 СЕМЕСТР

1-ый рубежный контроль

1. Какие из перечисленных устройств относятся к блокираторам сотовой связи?

1) Мозаика 2) Шиповник-2 3) Гном-3 4) Бриз 5) Поиск-2У
6) Питон 7) Квартет-4 8) АКА-7202 9) Скорпион 10) ЛГШ-701

2. Для чего используется программно-аппаратный комплекс RS-TURBO?

1) Для обнаружения подслушивающих устройств и других источников несанкционированных излучений, передающих сигналы по радиоканалу, сети электропитания, проводным линиям и в оптическом ИК-диапазоне.

2) Для определения местоположения (локализации) подслушивающих устройств и других источников несанкционированных излучений, передающих сигналы по радиоканалу, сети электропитания, проводным линиям и в оптическом ИК-диапазоне.

3) Для нейтрализации подслушивающих устройств и других источников несанкционированных излучений, передающих сигналы по радиоканалу, сети электропитания, проводным линиям и в оптическом ИК-диапазоне.

4) Для обнаружения, идентификации, определения местоположения (локализации) и нейтрализации подслушивающих устройств и других источников несанкционированных излучений, передающих сигналы по радиоканалу, сети электропитания, проводным линиям и в оптическом ИК-диапазоне.

2-ой рубежный контроль

1. Какие стандарты GSM блокирует прибор Бархан-1?

1) GSM-850МГц
2) GSM-900МГц
3) GSM-1800МГц
4) GSM-1900МГц

2. Прибор «Унискан-7215М» предназначен:

1) для физической защиты периметра
2) для выполнения визуального досмотра труднодоступных, слабоосвещенных мест в помещениях, транспортных средствах и грузах.
3) для обнаружения и локализации РСТС негласного получения информации
4) для поиска металлических предметов в диэлектрических и слабопроводящих средах

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. Характеристика инженерно-технической защиты информации как области информационной безопасности.
2. Основные проблемы инженерно-технической защиты информации. Основные параметры системы защиты информации.
3. Цели и задачи защиты информации. Ресурсы, выделяемые на защиту информации.
4. Принципы защиты информации техническими средствами.
5. Основные направления инженерно-технической защиты информации. Показатели эффективности инженерно-технической защиты информации.
6. Свойства информации, влияющие на ее безопасность.
7. Виды, источники и носители защищаемой информации.
8. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие о текущей и эталонной признаковой структуре.
9. Понятие об опасном сигнале. Основные и вспомогательные технические средства и системы, их классификация и характеристика.
10. Опасные сигналы, образующиеся в результате акустоэлектрических преобразований.
11. Виды побочных опасных электромагнитных излучений.
12. Паразитные связи и наводки опасных сигналов.
13. Случайные антенны. Виды опасных сигналов в помещении.
14. Основные задачи и органы технической разведки.
15. Принципы технической разведки.
16. Основные этапы и процессы добывания информации технической разведкой.
17. Классификация технической разведки по видам носителя информации и средств разведки.
18. Возможности видов технической разведки по добыванию разведывательной информации.
19. Основные направления развития технической разведки.
20. Модель иностранной технической разведки.
21. Понятие и особенности утечки информации.
22. Структура, классификация и основные характеристики технических каналов утечки информации.
23. Простые и составные технические каналы утечки информации.
24. Характеристика и возможности оптических, акустических каналов утечки информации.
25. Характеристика и возможности радиоэлектронных и материально-вещественных каналов утечки информации.
26. Классификация методов инженерно-технической защиты информации. Инженерная защита и техническая охрана объектов.
27. Пространственное, энергетическое и структурное скрытие информации и ее носителей.
28. Дезинформирование как метод скрытия.
29. Комплексное применение методов защиты.

30. Классификация методов инженерной защиты и технической охраны объектов защиты.
31. Инженерные конструкции. Автономные и централизованные системы охраны.
32. Модели злоумышленника.
33. Подсистемы обнаружения злоумышленников и пожара, видеоконтроля, нейтрализации угроз и управления охраной.
34. Пространственное скрытие объектов наблюдения и сигналов. Структурное и энергетическое скрытие объектов наблюдения.
35. Методы технического закрытия речевых сигналов.
36. Звукоизоляция и звукопоглощение.
37. Энергетическое скрытие радио и электрических сигналов. Виды и условия зашумления сигналов.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. Акустоэлектрические преобразования. Сосредоточенные и распределенные источники побочных излучений.
2. Характер электромагнитных излучений в ближней и дальней зонах. Паразитная генерация радиоэлектронных средств.
3. Виды паразитных связей и наводок. Цепи Пикара.
4. Физические явления, вызывающие утечку информации по цепям электропитания, заземления и токопроводящим конструкциям здания.
5. Распространение акустических сигналов в атмосфере, воде и в твердой среде.
6. Особенности распространения акустических сигналов в помещениях.
7. Основные показатели среды распространения сигналов, влияющие на дальность технических каналов утечки и качество информации на его выходе.
8. Подавление опасных сигналов акустоэлектрических преобразователей.
9. Экранирование электрических, магнитных, и электромагнитных полей. Требования к экранам. Компенсация полей.
10. Подавление опасных сигналов в цепях электропитания и заземления. Зашумление опасных сигналов помехами.
11. Визуально-оптические приборы. Фотоаппараты.
12. Оптоэлектронные приборы наблюдения в видимом и инфракрасном диапазонах.
13. Акустические приемники. Направленные микрофоны.
14. Структура комплексов перехвата.
15. Особенности сканирующих радиоприемников.
16. Закладные устройства, средства ВЧ-навязывания и лазерного подслушивания.
17. Автономные средства разведки.
18. Основные инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.
19. Средства управления доступом.
20. Классификация и характеристика охранных, охранно-пожарных и пожарных извещателей.
21. Средства видеоконтроля и видеоохраны.

22. Средства нейтрализации угроз.
23. Средства управления и передачи извещений.
24. Автоматизированные интегральные системы охраны.
25. Средства маскировки и дезинформирования в оптическом и радиодиапазонах.
26. Средства звукоизоляции и звукопоглощения.
27. Средства обнаружения, локализации и подавления сигналов закладных устройств.
28. Средства подавления сигналов акустоэлектрических преобразователей, цепей электропитания и заземления.
29. Генераторы линейного и пространственного зашумления.
30. Основные задачи, структура и характеристика государственной системы противодействия технической защите.
31. Основные руководящие, нормативные и методические документы по защите информации и противодействия технической разведке.
32. Основные организационные и технические меры по защите информации.
33. Аттестация объектов, лицензирование деятельности по защите информации и сертификация ее средств.
34. Виды контроля эффективности инженерно-технической защиты информации.
35. Требования по защите информации от утечки по техническим каналам
36. Методы технического контроля.
37. Особенности инструментального контроля эффективности инженерно-технической защиты информации.
38. Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации.
39. Принципы моделирования объектов защиты.
40. Моделирование угроз безопасности информации.
41. Методические рекомендации по выбору рациональных вариантов защиты.
42. Способы оптимизации мер инженерно-технической защиты информации.
43. Способы оценки эффективности охраны объектов защиты.
44. Оценка эффективности защиты видовых признаков объектов наблюдения.
45. Способы оценки безопасности речевой информации в помещении.
46. Способы определения уровней опасных сигналов на выходах основных и вспомогательных технических средств.
47. Оценка дальности перехвата опасных сигналов.

6.5. Фонд оценочных средств

Полный банк заданий для текущего, рубежных контролей и промежуточной аттестации по дисциплине, показатели, критерии, шкалы оценивания компетенций, методические материалы, определяющие процедуры оценивания образовательных результатов, приведены в учебно-методическом комплексе дисциплины.

7. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

7.1. Основная учебная литература

1. Технические средства и методы защиты информации. [Электронный ресурс]: Под ред. А. П. Зайцева и А. А. Шелупанова. - 7-е изд., испр. – М.: Горячая линия - Телеком, 2012. - 442 с. - ISBN 978-5-9912-0233-6. . – Доступ ЭБС «Консультант студента».

7.2 Дополнительная литература

1. Бузов, Г. А. Защита информации ограниченного доступа от утечки по техническим каналам [Электронный ресурс]: - Москва : Горячая линия - Телеком, 2015. - 586 с. - ISBN 978-5-9912-0424-8. – Доступ ЭБС «Консультант студента»
2. Ворона, В. А. Инженерно-техническая и пожарная защита объектов / Ворона В. А. , Тихонов В. А. - Вып. 4. - Москва : Горячая линия - Телеком, 2012. - 512 с. - ISBN 978-5-9912-0179-7. – Доступ ЭБС «Консультант студента»
3. Свинарев, Н. А. Инструментальный контроль и защита информации : учеб. пособие / Свинарев Н. А. , Ланкин О. В. , Данилкин А. П, Потехецкий С. В. , Перетокин О. И. - Воронеж : ВГУИТ, 2013. - 192 с. - ISBN 978-5-00032-018-1. – Доступ ЭБС «Консультант студента»
4. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Техническая защита информации: Лабораторный практикум / Под редакцией Ю.Ф. Каторина [Электронный ресурс]: - СПб: НИУ ИТМО, 2013. - 112 с.– Режим доступа: http://window.edu.ru/resource/351/80351/files/itmo1476.pdf

8. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

1. Методические указания к выполнению лабораторной работы «Статистический анализ загрузки заданного радиодиапазона и обнаружения радиозакладных устройств в защищенном помещении» по дисциплине «Техническая защита информации» для студентов специальности 10.05.03. КГУ. 2016.
2. Методические указания к выполнению лабораторной работы «Проверка выполнения норм эффективности защиты речевой информации от утечки по акустическому каналу с помощью комплекса «Спрут-мини» по дисциплине ««Техническая защита информации» для студентов специальности 10.05.03. КГУ. 2016.
3. Методические указания к выполнению лабораторной работы «Обнаружение оптических сигналов передатчиков ИК-диапазона» по дисциплине «Техническая защита информации» для студентов специальности 10.05.03. КГУ. 2016.
4. Методические указания к выполнению лабораторной работы «Обнаружение сигналов линейных и сетевых закладок» по дисциплине «Техническая защита информации» для студентов специальности 10.05.03. КГУ. 2016.
5. Методические указания к выполнению лабораторной работы «Оценка защищенности ограждающих конструкций помещения от утечки информации по акустическому каналу комплексом «Спрут-мини» по дисциплине «Техническая защита информации» для студентов специальности 10.05.03. КГУ. 2016.

6. Методические указания к выполнению лабораторной работы «Оценка защищенности помещения от утечки информации по каналам акусто-электрических преобразований технических средств с помощью комплекса «Спрут-мини» по дисциплине «Техническая защита информации» для студентов специальности 10.05.03. КГУ. 2016.

7. Методические указания к выполнению лабораторной работы «Оценка защищенности ограждающих конструкций помещения от утечки информации по виброакустическому каналу комплексом «Спрут-мини» по дисциплине «Техническая защита информации» для студентов специальности 10.05.03. КГУ. 2016.

8. ФСТЭК. Сборник типовых лабораторных практикумов. Защита информации в локальных вычислительных сетях и помещениях от утечки по техническим каналам за счет побочных электромагнитных излучений и наводок. Методическое пособие по аттестации объектов информатизации по требованиям безопасности информации. Москва, 2011. – 293 с.

9. ФСТЭК. Сборник типовых лабораторных практикумов. Контроль защищенности локальных вычислительных сетей от несанкционированного доступа. Методическое пособие по аттестации объектов информатизации по требованиям безопасности информации. Москва, 2011. – 453 с.

10. ФСТЭК. Сборник типовых лабораторных практикумов. Защита речевой информации в помещениях. Методическое пособие по аттестации объектов информатизации по требованиям безопасности информации. Москва, 2011. – 220 с.

11. Методические указания к выполнению практических занятий по теме «Теоретические основы инженерно-технической защиты информации» по дисциплине «Техническая защита информации» для студентов очной формы обучения специальности 10.05.03. КГУ. 2017.

12. Методические указания к выполнению контрольной работы по теме «Моделирование технической разведки для объекта информатизации» по дисциплине «Техническая защита информации» для студентов очной формы обучения направления 10.05.03. КГУ. 2017.

9. РЕСУРСЫ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Официальный сайт Федеральной службы по техническом и экспортному контролю http://fstec.ru
2. ЭБС «Лань» - https://e.lanbook.com/;
3. ЭБС «Znanium» - https://znanium.com/;
4. ЭБС «Консультант студента» - https://www.studentlibrary.ru;
5. Национальный Открытый Университет «ИНТУИТ» - https://intuit.ru;
6. http://infotecs.ru;
7. http://www.itsec.ru;
8. http://www.bnti.ru/articles.asp?lvl=04.03. - Статьи по теме «Средства защиты информации»

10. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

Система KESS поддержки образовательного процесса КГУ http://dist.kgsu.ru/.

При чтении лекций используются слайдовые презентации.

Минимальные требования к операционной системе и программному обеспечению компьютера, используемого при показе слайдовых презентаций: Windows XP, Libre Office.

11. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Переносной проектор BENQ PB6110 с экраном, локальная сеть компьютеров на базе Intel Core i3-2120 - 16 шт. с выходом в Internet, коммутатор 2-го уровня D-LINK DGS-101D/E1A, средства выявления каналов утечки информации, средства проверки на соответствие требованиям защиты от утечек по техническим каналам.

ПРИЛОЖЕНИЕ 1

Аннотация к рабочей программе дисциплины

«Техническая защита информации»

образовательной программы высшего образования –
программы специалитета
10.05.03 – Информационная безопасность автоматизированных систем
Направленность: (специализация №7)
Обеспечение информационной безопасности распределенных информационных систем

Трудоемкость дисциплины: 9 з.е. (324 академических часа)
Семестр: 8, 9 (очная форма обучения)
Форма промежуточной аттестации: зачет с оценкой, экзамен
Содержание дисциплины. Основные разделы

Технические каналы утечки информации. Демаскирующие признаки объектов. Средства выявления каналов утечки информации. Защита информации от утечки по техническим каналам. Защита объектов. Технический контроль эффективности мер защиты информации. Аттестация объектов информатизации.