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
_____ Т.Р. Змызгова
_____ 2023 г.

Рабочая программа учебной дисциплины
ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

образовательной программы высшего образования - программы специалитета 10.05.03
Информационная безопасность автоматизированных систем

Специализация №5
Безопасность открытых информационных систем

Форма обучения: очная

Курган 2023

Рабочая программа дисциплины «Защита информации от утечки по техническим каналам» составлена в соответствии с учебным планом программы специалитета: «Информационная безопасность автоматизированных систем» (безопасность открытых информационных систем), утвержденным для очной формы обучения «30» июня 2023 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» 31 августа 2023 года, протокол № 1.

Рабочую программу составил:
канд. техн. наук, доцент Д.И. Дик

Согласовано:

Заведующий кафедрой «БИАС»
канд. техн. наук, доцент Д.И. Дик

Начальник Управления
образовательной деятельности И.В. Григоренко

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

1. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины - 10 зачетных единиц (360 акад. часов)

Очная форма обучения

Вид учебной работы	На всю дисциплину	семестр 8	семестр 9
Аудиторные занятия (контактная работа с преподавателем), всего часов, в том числе:	**186**	**96**	**90**
Лекции	62	32	30
Лабораторные работы	62	32	30
Практические занятия	62	32	30
Самостоятельная работа, всего часов в том числе:	**174**	**84**	**90**
Подготовка к зачету с оценкой	18	18	-
Подготовка к экзамену	27	-	27
Другие виды самостоятельной работы (подготовка к практическим работам и рубежному контролю)	129	66	63
Вид промежуточной аттестации	**экзамен, зачет с оценкой**	**зачет с оценкой**	**экзамен**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**360**	**180**	**180**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Защита информации от утечки по техническим каналам» является обязательной дисциплиной блока Б1 модуля Информационная безопасность.

Дисциплина изучается в 8 и 9 семестре и требует от обучаемых умений, навыков и компетенций, полученных при изучении дисциплин «Основы теории защиты информации», «Основы информационной безопасности», «Организация ЭВМ и вычислительных систем», «Аппаратные средства вычислительной техники» и «Методы контроля защищенности информации в информационных системах».

Результаты обучения по дисциплине необходимы для освоения дисциплин: «Реагирование на инциденты информационной безопасности»; «Катастрофоустойчивость информационных систем»; «Организация конфиденциального документооборота», а также при подготовке выпускной квалификационной работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Целью курса «Защита информации от утечки по техническим каналам» является изучение формирование у обучающихся знаний по основам инженерно-технической защиты информации, а также навыков и умения в применении знаний для конкретных условий.

Задачи дисциплины:

– ознакомление с техническими каналами утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами;

– ознакомление с техническими каналами утечки акустической (речевой) информации;

– изучение способов и средств защиты информации, обрабатываемой техническими средствами;

– изучение способов и средств защиты выделенных (защищаемых) помещений от утечки акустической (речевой) информации;

– изучение методов и средств контроля эффективности защиты информации от утечки по техническим каналам.

Результаты обучения по дисциплине необходимы развития системного мышления, необходимого для решения задач инженерно-технической защиты информации с учетом требований системного подхода.

Компетенции, формируемые в результате освоения дисциплины:

- Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. (ОПК-6).

- Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации (ОПК-9).

В результате изучения дисциплины обучающийся должен **знать**:

- основные нормативные и методические документы в области технической защиты информации. (для ОПК-6, ОПК-9);
- методы и средства контроля эффективности технической защиты информации (для ОПК-6);
- технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам (для ОПК-9).

уметь:

- определять ресурсы и объекты, подлежащие защите, а также требования к системе защиты. (для ОПК-6);
- осуществлять меры противодействия утечки информации по техническим каналам. (для ОПК-6, ОПК-9);
- обслуживать технические средства защиты информации. (для ОПК-9).

владеть:

- методами аттестации уровня защищенности объектов, помещений, технических средств и систем (для ОПК-6);
- навыками моделирования технических каналов утечки информации (для ОПК-9);
- навыками установки и настройки средств технической защиты информации (для ОПК-9).

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Учебно-тематический план

Очная форма обучения

8 семестр

Рубеж	Номер темы	Наименование темы	Количество часов контактной работы с преподавателем		
			Лекции	Практ. занятия	Лаб. работы
Рубеж 1	1	Основные концептуальные положения инженерно-технической защиты информации	2	-	-
	2	Организационно-правовые основы технической защиты информации	4	-	4
	3	Виды информации, защищаемой техническими средствами	2	-	-
	4	Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.	4	8	6
	5	Демаскирующие признаки объектов защиты	4	-	-

		Рубежный контроль 1	-	2	-
Рубеж 2	*6*	Источники и носители информации, защищаемой техническими средствами, принципы записи и съема информации с носителей	4	-	-
	7	Технические каналы утечки акустической (речевой) информации	2	-	6
	8	Способы и средства защиты информации от утечки по техническим каналам	2	10	4
	9	Методы и средства контроля эффективности технической защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами	4	-	6
	10	Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам	4	10	6
		Рубежный контроль 2	-	2	-
		Всего:	**32**	**32**	**32**

9 семестр

Рубеж	Номер темы	Наименование темы	Количество часов контактной работы с преподавателем		
			Лекции	Практ. занятия	Лаб. работы
Рубеж 3	11	Принципы добывания и обработки информации техническими средствами	5	-	-
	12	Классификация и структура технических каналов утечки информации	5	-	-
	13	Средства предотвращения утечки информации по техническим каналам	5	-	-
	14	Методы и средства выявления электронных устройств негласного получения информации	5	8	10
		Рубежный контроль 3	-	2	-
Рубеж 4	15	Основы физической защиты объектов информатизации	5	8	10
	16	Организация технической защиты информации на объектах информатизации	5	10	10
		Рубежный контроль 4	-	2	-
		Всего:	**30**	**30**	**30**

4.2. Содержание лекционных занятий

8 семестр

Тема 1. Основные концептуальные положения инженерно-технической защиты информации. Цели и задачи защиты информации. Ресурсы, выделяемые на защиту информации. Принципы защиты информации техническими средствами. Принципы проектирования систем технической защиты.

Тема 2. Организационно-правовые основы технической защиты информации. Определение подразделений и лиц, ответственных за организацию защиты информации; Нормативно-правовые, руководящие и методические материалы (документы) по защите информации; Меры ответственности за нарушение правил защиты Порядок разрешения спорных и конфликтных ситуаций по вопросам защиты информации.

Тема 3. Виды информации, защищаемой техническими средствами. Свойства информации, влияющие на возможности ее защиты.

Тема 4. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. Общая характеристика технических каналов утечки информации, обрабатываемой средствами вычислительной техники. Электрические каналы утечки информации. Электромагнитные каналы утечки информации, обрабатываемой средствами вычислительной техники. Специально создаваемые технические каналы утечки информации

Тема 5. Демаскирующие признаки объектов защиты. Классификация демаскирующих признаков. Опознавательные признаки и признаки деятельности. Видовые сигнальные вещественные.

Тема 6. Источники и носители информации, защищаемой техническими средствами, принципы записи и съема информации с носителей. Определение. Классификация источников и носителей информации. Запись и съем информации. Источники сигналов.

Тема 7. Технические каналы утечки акустической (речевой) информации. Характеристики технических каналов утечки информации. Структура акустических каналов.

Тема 8. Способы и средства защиты информации от утечки по техническим каналам. Средства защиты информации по каналам ПЭМИН. Средства защиты акустической речевой информации. Средства защиты от несанкционированного применения сотовых телефонов, диктофонов и радиопередатчиков.

Тема 9. Методы и средства контроля эффективности технической защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами, организационный контроль эффективности ТЗИ. Технический контроль эффективности ТЗИ. Документирование результатов контроля.

Тема 10. Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам. Понятие контролируемой зоны. Требования у техническим и программным средствам, устанавливаемых в выделенных помещениях.

9 семестр

Тема 11. Принципы добывания и обработки информации техническими средствами. Основные принципы разведки. Классификация технической разведки. Технологии добычи информации.

Тема 12. Классификация и структура технических каналов утечки информации. Утечка и Утечка (информации) по техническому каналу.

Классификация технических каналов утечки информации. Информационный сигнал и его характеристики

Тема 13. Средства предотвращения утечки информации по техническим каналам. Устройства для перехвата информации и признаки их установки. Методы поиска закладных устройств. Аппараты и приборы для поиска шпионских устройств

Тема 14. Методы и средства выявления электронных устройств негласного получения информации. Классификация, характеристики, возможности, наиболее вероятные способы применения.

Тема 15. Основы физической защиты объектов информатизации. Сущность, цель и задачи. Анализ структуры физической защиты. Принципы и методы физической защиты объектов информатизации. Анализ объектов физической защиты. Физические средства подсистемы задержки

Тема 16. Организация технической защиты информации на объектах информатизации. Схема анализа защищаемого объекта информатизации. Категорирование защищаемой информации. Категорирование объектов защиты по уровню важности. Анализ возможных источников угроз безопасности.

4.3. Практические занятия
8 семестр

№ темы	Наименование темы	Наименование тем практических занятий	Норматив времени, час.
4	Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами	Изучение функциональных возможностей систем оценки защищенности выделенных помещений по акустическому и виброакустическому каналу «Спрут-мини»	8
	1-ый рубежный контроль	**Тестирование**	**2**
8	Способы и средства защиты информации от утечки по техническим каналам	Изучение функциональных возможностей измерительной аппаратуры по определению параметров сигналов побочных электромагнитных излучений на примере селективного микро вольтметра, анализатора спектра	10
10	Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам	Изучение функциональных возможностей автоматизированной системы оценки защищенности технических средств от утечки информации по каналу побочных электромагнитных излучений и наводок «Пиранья» ST-31 p	10
	2-ой рубежный контроль	**Тестирование**	**2**
		Итого	**32**

9 семестр

№ темы	Наименование темы	Наименование тем практических занятий	Норматив времени, час.
14	Методы и средства выявления электронных устройств негласного получения информации	Изучение функциональных возможностей автоматизированной системы оценки защищенности технических средств от утечки информации по каналу побочных электромагнитных излучений и наводок «Пиранья» ST-31 p	8
	3-ый рубежный контроль	**Тестирование**	**2**
15	Основы физической защиты объектов информатизации	Изучение функциональных возможностей нелинейного локатора, индикатора поля. Исследование методов и средств поиска электронных устройств перехвата информации	8
16	Организация технической защиты информации на объектах информатизации	Изучение функциональных возможностей нелинейного локатора, индикатора поля. Исследование методов и средств поиска электронных устройств перехвата информации	10
	4-ой рубежный контроль	**Тестирование**	**2**
		Итого	**30**

4.4. Лабораторные работы

8 семестр

№ темы	Наименование темы	Наименование тем лабораторных работ	Норматив времени, час.
2	Организационно-правовые основы технической защиты информации	*Лабораторная работа № 1.* Исследование способов защиты акустической информации от высокочастотного навязывания и микрофонного эффекта с использованием программного обеспечения Electronics Workbench	4
4	Технические каналы утечки информации, обрабатываемой средствами вычислитель -ной техники и автоматизированными системами	*Лабораторная работа № 2.* Исследование способов защиты акустической информации от высокочастотного навязывания и микрофонного эффекта с использованием программного обеспечения Electronics Workbench (NI Multisim) системами	6
7	Технические каналы утечки акустической (речевой) информации	*Лабораторная работа № 3.* Способы выявления и параметризации потенциальных каналов утечки информации в цепях питания с использованием программного обеспечения Electronics Workbench	6

8	Способы и средства защиты информации от утечки по техническим каналам	*Лабораторная работа № 4.* Способы выявления и параметризации потенциальных каналов утечки информации в цепях питания с использованием программного обеспечения Electronics Workbench	4
9	Методы и средства контроля эффективности технической защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами	*Лабораторная работа № 5.* Расчет основных показателей технических каналов утечки информации.	6
10	Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой ин -формации по техническим каналам	*Лабораторная работа № 6.* Способы и средства защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами	6
		Итого	**32**

9 семестр

№ темы	Наименование темы	Наименование тем практических занятий	Норматив времени, час.
14	Методы и средства выявления электронных устройств негласного получения информации	*Лабораторная работа № 1.* Контроль и оценка эффективности защиты речевой информации	10
15	Основы физической защиты объектов информатизации	*Лабораторная работа № 2.* Исследование способов подавления проводных закладных подслушивающих устройств с использованием программного обеспечения Electronics Workbench	10
16	Организация технической защиты информации на объектах информатизации	*Лабораторная работа № 3.* Расчеты по оценке защищенности речевой информации от утечки по каналу низкочастотного акустоэлектрического преобразования	10
		Итого	**30**

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Лекционный курс базируется на пассивном методе обучения, реализующем традиционную объяснительно-иллюстративную образовательную технологию, в рамках которой студенты выступают в роли слушателей, воспринимающих учебный материал и участвующих в дискуссиях и экспресс – опросах.

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

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.

Конспект каждой лекции завершается перечнем контрольных вопросов, ответы на которые должны быть получены студентом в процессе самостоятельной проработки материала лекции при подготовке к очередному лекционному занятию.

Лабораторные и практические занятия проводятся на основе интерактивных методов в виде творческих заданий экспериментального характера, направленных не столько на закрепление уже изученного материала, сколько на изучение нового, и выполняемые студентами, объединяемыми в малые группы (2-3 человека). Задания не имеют однозначного решения и соответствуют целям обучения.

Залогом качественного выполнения лабораторных работ и практических заданий является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Рекомендуется подготовить вопросы по неясным моментам и обсудить их с преподавателем в начале лабораторного 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 практических и лабораторных занятиях в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает самостоятельное изучение тем дисциплины, подготовку к лабораторным и практическим занятиям, рубежным контролям, подготовку к зачету с оценкой (8 семестр) и экзамену (9 семестр).

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
8 семестр	

Самостоятельное изучение тем:	***44***
Основные концептуальные положения инженерно-технической защиты информации	4
Организационно-правовые основы технической защиты информации	4
Виды информации, защищаемой техническими средствами	4
Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами.	5
Демаскирующие признаки объектов защиты	4
Источники и носители информации, защищаемой техническими средствами, принципы записи и съема информации с носителей	5
Технические каналы утечки акустической (речевой) информации	4
Способы и средства защиты информации от утечки по техническим каналам	4
Методы и средства контроля эффективности технической защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами	5
Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам	5
Подготовка к лабораторным работам (по 2 часу)	12
Подготовка к практическим занятиям (по 2 часу)	6
Подготовка к рубежным контролям (по 2 часа)	4
Подготовка к зачет с оценкой	18
Итого за 8 семестр:	**84**
9 семестр	
Самостоятельное изучение тем:	***47***
Принципы добывания и обработки информации техническими средствами	6
Классификация и структура технических каналов утечки информации	6
Средства предотвращения утечки информации по техническим каналам	9
Методы и средства выявления электронных устройств негласного получения информации	10
Основы физической защиты объектов информатизации	6
Организация технической защиты информации на объектах информатизации	10
Подготовка к лабораторным работам (по 2 часу)	6
Подготовка к практическим занятиям (по 2 часу)	6
Подготовка к рубежным контролям (по 2 часа)	4
Подготовка к экзамену	27
Итого за 9 семестр:	**90**
Всего:	**174**

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 практическим и лабораторным работам.
3. Банк тестовых заданий к рубежным контролям № 1, № 2, № 3, № 4.
4. Вопросы к зачету с оценкой.
5. Вопросы к экзамену.

6.2. Система балльно-рейтинговой оценки работы студентов по дисциплине

№	Наименование	Содержание

<table>
<tr><td rowspan="4">1</td><td rowspan="4">Распределение баллов за семестр по видам учебной работы, сроки сдачи учебной работы (доводятся до сведения студентов на первом учебном занятии)</td><td colspan="7">Распределение баллов, 8 семестр</td></tr>
<tr><td>Вид учебной работы:</td><td>Посещение лекций</td><td>Выполнение практической работы</td><td>Выполнение лабораторных работ</td><td>Рубежный контроль №1</td><td>Рубежный контроль №2</td><td>Зачет с оценкой</td></tr>
<tr><td>Балльная оценка:</td><td>1б х 16 = 16б</td><td>8б х 3= 24б</td><td>3б х 6 = 18б</td><td>6</td><td>6</td><td>30</td></tr>
<tr><td colspan="7">Распределение баллов, 9 семестр</td></tr>
<tr><td></td><td>Вид учебной работы:</td><td>Посещение лекций</td><td>Выполнение практической работы</td><td>Выполнение лабораторных работ</td><td>Рубежный контроль №3</td><td>Рубежный контроль №4</td><td>Экзамен</td></tr>
<tr><td></td><td>Балльная оценка:</td><td>1 б х 15 = 15б</td><td>8б х 3= 24б</td><td>5б х 3 = 15б</td><td>8</td><td>8</td><td>30</td></tr>
<tr><td>2</td><td>Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и на экзамене</td><td colspan="7">60 и менее баллов – неудовлетворительно; незачет;
61…73 – удовлетворительно; зачет;
74… 90 – хорошо;
91…100 – отлично</td></tr>
<tr><td>3</td><td>Критерии допуска к промежуточной аттестации, возможности получения автоматически экзаменационной оценки «удовлетворительно» по дисциплине, возможность получения бонусных баллов</td><td colspan="7">Для допуска к промежуточной аттестации по дисциплине за семестр обучающийся должен набрать по итогам текущего и рубежного контроля не менее 51 баллов. В случае если обучающийся набрал менее 51 балла, то к аттестационным испытаниям он не допускается.
Для получения зачета с оценкой (в 8 семестре) / экзамена (9 семестре) без проведения процедуры промежуточной аттестации обучающемуся необходимо набрать в ходе текущего и рубежных контролей не менее 61 балла. В этом случае итог балльной оценки, получаемой обучающимся, определяется по количеству баллов, набранных им в ходе текущего и рубежного контролей. При этом, на усмотрение преподавателя, бальная оценка обучающегося может быть повышена за счет получения дополнительных баллов за академическую активность.
Обучающийся, имеющий право на получение оценки без проведения процедуры промежуточной аттестации, может повысить ее путем сдачи аттестационного испытания. В случае получения обучающимся на аттестационном испытании 0 баллов итог бальной оценки по дисциплине не снижается.
За академическую активность в ходе освоения дисциплины, участие в учебной, научно-исследовательской, спортивной, культурно-творческой и общественной деятельности обучающемуся могут быть начислены дополнительные баллы. Максимальное количество дополнительных баллов за академическую активность составляет 30.
Основанием для получения дополнительных баллов являются:
- выполнение дополнительных заданий по дисциплине; дополнительные баллы начисляются преподавателем;
- участие в течение семестра в учебной, научно-исследовательской, спортивной, культурно-творческой и общественной деятельности КГУ.</td></tr>
</table>

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 (зачету с оценкой / экзамену) набрана сумма менее 51 баллов, обучающемуся необходимо набрать недостающее количество баллов за счет выполнения дополнительных заданий, до конца последней (зачетной) недели семестра. 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

Рубежный контроль в 8 и 9 семестре осуществляется в форме тестирования на лабораторных занятиях.

Тестирование проводится в письменной форме, при этом каждый такой тест содержит 12 и 16 (в 8 и 9 семестре соответственно) несложных вопросов/заданий по соответствующей теме. Каждый вопрос оценивается в 0.5 балла.

Оценивается количество правильных ответов на задания теста: студент, ответивший правильно менее, чем на 50% заданий теста, считается не прошедшим тестирование и обязан повторно пройти этот тест во время консультации по дисциплине, а также во время проведения консультаций по дисциплине в форме собеседования.

На каждое тестирование при рубежном контроле студенту отводится 2 академических часа.

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

Примерные тестовые задания приведены ниже. Каждый вопрос оценивается в один балл.

Зачет с оценкой (8 семестр) проводится в виде тестирования: студент выполняет задания, состоящие из вопросов, рассматриваемых на рубежный контролях.

Преподаватель оценивает в баллах результаты тестирования каждого студента по количеству правильных ответов. На зачет студенту отводится 1 астрономический час.

Результаты зачета с оценкой заносятся преподавателем в зачетную ведомость, которая сдается в организационный отдел института в день зачета с оценкой, а также выставляются в зачетную книжку студента.

Экзамен (9 семестр) проводится в традиционной (устной) форме: студент выполняет задания билета, включающего один теоретический вопрос и одно практическое задание, и отвечает преподавателю. Оцениваются полнота и правильность ответов студента на теоретические вопросы билета, его эрудиция в смежных вопросах, а также правильность решения задачи.

Вопросы к экзамену доводятся до студентов на последней лекции в семестре. Каждый вопрос оценивается в 15 баллов. На подготовку ответа студенту отводится 1 астрономический час.

Результаты зачета с оценкой и экзамена заносятся преподавателем в зачетную и экзаменационную ведомость, соответственно, которая сдается в организационный отдел института в день зачета с оценкой, экзамена, а также выставляются в зачетную книжку студента.

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

Примеры тестовых заданий для рубежного контроля №1

1. Выберите ВСЕ основные цели защиты информации из списка.

а. Сохранение государственной и коммерческой тайны.

б. Обеспечение прав при использовании средств съема информации.

в. Предотвращение угроз безопасности личности, общества, государства.

2. Выберите ВСЕ основные задачи защиты информации из списка.

а. Защита прав граждан

б. Предотвращение НСД

в. Сохранение государственной и коммерческой тайны.

г. Предотвращение утечки, хищения, искажения и подделки информации

3. Выберите ВСЕ способы защиты информации методом «Сокрытия».

а. пассивное скрытие;

б. специальная защита;

в. легендирование;

г. техническая дезинформация;

д. активное скрытие;

е. имитация.

Примеры тестовых заданий для рубежного контроля №2

1. Укажите правильное определение. Организационный контроль эффективности ТЗИ - это ...

а. проверка исполнения и контроля мероприятий по ТЗИ требованиям руководящих и нормативно-методических документов в области ТЗИ;

б. проверка соответствия полноты и обоснованности мероприятий по ТЗИ требованиям руководящих и нормативно-методических документов в области ТЗИ;

в. контроль эффективности ТЗИ, проводимый с использованием программных средств контроля.

г. контроль эффективности ТЗИ, проводимый с использованием технических средств контроля.

2. Выберите ВСЕ РАЗДЕЛЫ акта проверки состояния ТЗИ из списка.

а. Общие сведения об объекте контроля;

б. Общие сведения о субъекте, обеспечивающий контроль;

в. Общие вопросы организации ТЗИ на объекте;

г. Список лиц, ответственных за обеспечение ТЗИ в организации;

д. Организация и состояние защиты объектов информатизации;

е. Полнота и качество проведения лицензиатами ФСТЭК России работ по защите и аттестации объектов информатизации;

ж. Полнота и качество проведения проверочных мероприятий ФСБ России на объекте защиты;

з. Выводы и рекомендации.

Примерный перечень вопросов для зачета с оценкой

1. Укажите, как классифицируются демаскирующие признаки по характеристикам объекта:

а. сигнальные;

б. прямые;

в. объемные;

г. видовые;

д. вещественные;

е. излучающие.

2. Вберите ТОЛЬКО носители информации из списка.

а. люди;

б. продукция;

в. измерительные датчики;

г. поля;

д. интеллектуальные средства обработки информации;

е. элементарные частицы;

Примеры тестовых заданий для рубежного контроля №3

1. На какие классы подразделяют уязвимости?

а. объектные и субъектные;

б. объектные, субъектные и комплексные;

в. одиночные и комплексные;

г. обязательные и случайные;

д. объектные, субъектные, случайные и комплексные;

е. объектные, субъектные, обязательные и комплексные;

ж. случайные, объектные и комплексные;

з. случайные, обязательные и комплексные;

и. случайные, объектные и субъектные;

к. нет правильного варианта.

2. Выберите ВСЕ верные варианты классификации технической разведки по физической природе:

а. морская;

б. оптическая;

в. физическая;

г. сейсмическая;

д. воздушная;

е. комплексная;

ж. химическая.

3. Укажите ВСЕ этапы добывания информации:

а. информационная работа;

б. планирование;

в. нормативное и оперативное управление действиями исполнителей и режимами работы технических средств;

г. организация добывания;

д. разработка замысла операции по добыванию информации;

е. добывание данных и сведений.

Примеры тестовых заданий для рубежного контроля №4

1. Установите соответствие между принципами организации комплексной системы защиты и их определениями.

Название принципа	Определение
1. Системность	**а.** предполагает, что система защиты предприятия должна включать совокупность объектов защиты, сил и средств, принимаемых мер, проводимых мероприятий и действий по обеспечению безопасности.
2. Комплексность	б. состоит в том, что механизмы защиты должны быть интуитивно понятны и просты в использовании.
3. Своевременность	**в,** при оценке эффективности мероприятий безопасности не ограничиваются рассмотрением только самой системы, но и учитывают влияния на нее внешних факторов.
4. Непрерывности	**г.** означает, что меры защиты не должны «запаздывать». Например, бесполезно выводить охранную сигнализацию на пульт дежурного, который сможет прибыть в случае тревоги на объект охраны лишь спустя полчаса.
5. Разумная достаточность	д. учитывает тот факт, что создать абсолютно непреодолимую систему защиты принципиально невозможно. При достаточном количестве времени и средств можно преодолеть любую защиту, поэтому имеет смысл вести речь только о некотором приемлемом уровне безопасности.
6. Простота применения	**е.** предполагает принятие соответствующих мер на всех этапах жизненного цикла систем предприятия.

а. 1-а, 2-б,3-в,4-г,5-д,6-е;

б. 1-е, 2-г,3-д,4-в,5-б,6-а;

в. 1-б, 2-в,3-д,4-д,5-а,6-е;

г. 1-а, 2-б,3-г,4-г,5-д,6-е;

д. 1-е, 2-а,3-г,4-е,5-д,6-б;

е. 1-в, 2-а,3-е,4-г,5-д,6-б;

ж. 1-в, 2-б,3-б,4-г,5-д,6-е;

з. 1-а, 2-в,3-а,4-д,5-е,6-б.

2. Выберите все критерии категорирования защищаемых объектов по количественному критерию оценки.

а. площадь пострадавшей территории;

б. ущерб финансово-кредитной системе;

в. по численности персонала;

г. время на восстановление;

д. ущерб природным ресурсам и экосистеме;

е. по материальным активам.

Примерный перечень вопросов для экзамена

1. Системный подход к защите информации, основные положения. Цели, задачи и ресурсы системы защиты информации.

2. Угрозы безопасности информации и меры по их предотвращению.

3. Понятие о защищаемой информации, виды защищаемой информации. Демаскирующие признаки объектов защиты, их классификация. Видовые демаскирующие признаки, демаскирующие признаки сигналов, демаскирующие признаки веществ.

4. Технические разведки и их цели. Классификация технической разведки по физической природе носителя информации, по видам носителей аппаратуры разведки.

5. Классификация методов инженерной защиты и технической охраны объектов защиты. Подсистема инженерной защиты.

6. Способы и средства обнаружения злоумышленников и пожара. Назначение, задачи.

7. Извещатели, их классификация, принципы работы.

8. Подсистема наблюдения. Подсистема нейтрализации угроз.

9. Основные задачи, структура и характеристика государственной системы защиты информации и противодействия техническим разведкам. Основные руководящие, нормативные и методические документы. Основные организационные и технические меры.

10. Аттестация объектов информатизации, лицензирование деятельности по защите информации, сертификация средств защиты информации.

11. Характеристика объекта информатизации, как объекта защиты от технических разведок. Основные (ОТСС) и вспомогательные (ВТСС) технические средства и системы, их классификация и характеристики. Граница контролируемой зоны объекта информатизации. Виды опасных сигналов на ОИ.

12. Понятие и особенности утечки информации. Определение технического канала утечки информации. Структура, классификация, основные характеристики ТКУИ.

13. Выделенные (защищаемые) помещения. Характеристики речевого сигнала (звукового поля). Общая характеристика и классификация технических каналов утечки акустической (речевой) информации.

14. Классификация способов и средств защиты выделенных помещений от утечки речевой информации по техническим каналам. Способы и средства защиты вспомогательных технических средств и систем. Звукоизоляция помещений. Сертифицированные средства защиты.

15. Объекты вычислительной техники (автоматизированные системы). Общая характеристика и классификация технических каналов утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. Физическая природа побочных электромагнитных излучений.

16. Классификация способов и средств защиты объектов вычислительной техники (принципы построения, основные характеристики,

требования по установке). Экранирование технических средств их соединительных линий. Экранированные помещения.

17. Классификация способов и средств защиты объектов вычислительной техники. Заземление технических средств. Помехоподавляющие фильтры. Системы пространственного и линейного электромагнитного зашумления.

18. Методы выявления электронных устройств негласного получения информации, внедренных в выделенные помещения и технические средства. Средства выявления электронных устройств негласного получения информации.

19. Порядок проверки технических средств и выделенных помещений на наличие электронных устройств негласного получения информации.

20. Основные этапы проведения аттестации объектов информатизации по требованиям безопасности информации: задачи, содержание этапов, методы контроля и оценки состояния ТЗИ.

21. Показатели эффективности защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. Требования к средствам измерения побочных электромагнитных излучений и наводок средств вычислительной техники и условиям проведения измерений.

22. Порядок проведения контроля защищенности информации на объекте вычислительной техники от утечки по каналу побочных электромагнитных излучений средств вычислительной техники.

23. Показатели эффективности защиты речевой информации. Требования к средствам измерения акустических и вибрационных сигналов и условиям проведения измерений.

24. Порядок проведения контроля защищенности выделенных помещений от утечки акустической речевой информации.

6.5 Фонд оценочных средств

Полный банк заданий для текущего и рубежных контролей, 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 литература

1. Зайцев, А. П. Технические средства и методы защиты информации: учебник / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов. — 7-е изд., испр. - Москва: Горячая линия-Телеком, 2018. — 442 с. — ISBN 978-5-9912-0233- 6. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/l 11057.

2. Рагозин, Ю. Н. Инженерно-техническая защита информации на объектах информатизации: учебное пособие / Ю. Н. Рагозин. — Санкт-Петербург: Интермедия, 2019. — 216 с. — ISBN 978-5-4383-0182-0. — Текст:

электронный // Лань: электронно-библиотечная система. — URL: https ://e. lanbook. com/book/161337.

3. Глухарев, М. Л. Технические средства защиты информации: учебное пособие / М. Л. Глухарев, М. Ф. Исаева. — Санкт-Петербург: ПГУПС, 2018. - 55 с. — ISBN 978-5-7641-112-4. — Текст: электронный//Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/111736.

4. Гуляев, В. П. Анализ демаскирующих признаков объектов информатизации и технических каналов утечки информации: учебно-методический комплект: учебно-методическое пособие / В. П. Гуляев. — Екатеринбург: УрФУ, 2014. — 164 с. — ISBN 978-5-7996-1120-0. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https ://e. lanbook. com/book/98260.

5. Новоструев А. В., Солодовников В. М., Терентьева А. А., Дик Д. И. Тезаурус в сфере информационной безопасности: учебное пособие / А. В. Новоструев, В. М. Солодовников, А. А. Терентьева, Д. И. Дик - Курган: КГУ, 2014 - 468 с. - Текст электронный // Электронная библиотека КГУ. - URL: http://hdl.handle.net/123456789/3732.

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

1. Портал «Информационно-коммуникационные технологии в образовании» http:// www.ict.edu.ru.
2. Система поддержки учебного процесса КГУ dist2.kgsu.ru.
3. Официальный сайт ФСБ http://www.fsb.ru/
4. Официальный сайт ФСТЭК http://fstec.ru/
5. ЭБС Лань https://e.lanbook.cот/
6. ЭБС elibrary (периодические издания) http://elibrary.ru
7. Справочно-правовая база «Консультант Плюс», http://www. consultant.ru
8. Открытая база ГОСТов http://Standartgost.rn

9. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1. ЭБС «Лань».
2. ЭБС «Консультант студента».
3. ЭБС «Znanium.com».
4. «Гарант» - справочно-правовая система.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Материально-техническое обеспечение по реализации дисциплины осуществляется в соответствии с требования ФГОС ВО по данной образовательной программе.

11. Для студентов, обучающихся с использованием дистанционных образовательных технологий

При использовании электронного обучения и дистанционных образовательных технологий (далее ЭО и ДОТ) занятия полностью или частично проводятся в режиме онлайн. Объем дисциплины и распределение нагрузки по видам работ соответствует п. 4.1. Распределение баллов соответствует п. 6.2 либо может быть изменено в соответствии с решением кафедры, в случае перехода на ЭО и ДОТ в процессе обучения. Решение кафедры об используемых технологиях и системе оценивания достижений, обучающихся принимается с учетом мнения ведущего преподавателя и доводится до сведения обучающихся.

ПРИЛОЖЕНИЕ 1

Аннотация к рабочей программе дисциплины
«Защита информации от утечек по техническим каналам»

образовательной программы высшего образования –
программы специалитета
10.05.03 – Информационная безопасность автоматизированных систем
Специализация №5

Безопасность открытых информационных систем

Трудоемкость дисциплины: 10 з.е. (360 академических часа)
Семестр: 8,9 (очная форма обучения)

Форма промежуточной аттестации: зачет с оценкой, экзамен

Содержание дисциплины

Основные концептуальные положения инженерно-технической защиты информации. Организационно-правовые основы технической защиты информации. Виды информации, защищаемой техническими средствами. Технические каналы утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. Демаскирующие признаки объектов защиты. Источники и носители информации, защищаемой техническими средствами, принципы записи и съема информации с носителей. Технические каналы утечки акустической (речевой) информации. Способы и средства защиты информации от утечки по техническим каналам. Методы и средства контроля эффективности технической защиты информации, обрабатываемой средствами вычислительной техники и автоматизированными системами. Методы и средства контроля эффективности защиты выделенных помещений от утечки речевой информации по техническим каналам. Принципы добывания и обработки информации техническими средствами. Классификация и структура технических каналов утечки информации. Средства предотвращения утечки информации по техническим каналам. Методы и средства выявления электронных устройств негласного получения информации. Основы физической защиты объектов информатизации. Организация технической защиты информации на объектах информатизации.