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
«__»_____ 2024 г.

Рабочая программа учебной дисциплины

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

образовательной программы высшего образования –
программы бакалавриата

27.03.01 Стандартизация и метрология
Направленность: Стандартизация, метрология и управление качеством
Форма обучения: заочная

Курган 2024

Рабочая программа дисциплины «Технические средства защиты информации» составлена в соответствии с учебным планом по программе бакалавриата «Стандартизация и метрология» (стандартизация, метрология и управление качеством), утвержденной для заочной формы обучения «28» июня 2024 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» «29» августа 2024, протокол № 1.

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

Согласовано:

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

Заведующий кафедрой «АПП»
канд. тех. наук, доцент И.А. Иванова

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

Начальник управления образовательной деятельности И.В. Григоренко

1. ОБЪЕМ ДИСЦИПЛИНЫ

Всего: 3 зачетных единицы трудоемкости (108 академических часа)

Вид учебной работы	На всю дисциплину	Курс	Семестр
		2	4
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**6**	**6**	
Лекции	2	2	
Лабораторные работы	4	4	
Самостоятельная работа, всего часов в том числе:	**102**	**102**	
Подготовка к зачету	18	18	
Другие виды самостоятельной работы (изучение тем, подготовка к лабораторным работам и рубежному контролю)	66	66	
Контрольная работа	18	18	
Вид промежуточной аттестации	**зачет**	**зачет**	
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**108**	**108**	

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Технические средства защиты информации» является дисциплиной по выбору Блока 1 и относится к части, формируемой участниками образовательных отношений.

Изучение дисциплины базируется на результатах обучения, сформированных при изучении дисциплины «Информатика», «Физика».

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Целью дисциплины «Технические средства защиты информации» является формирование у студентов знаний по основам 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 – дать знания:

- об основных понятиях, методах и средствах, используемых в технической защите информации;
- о способах образования технических каналов утечки информации;
- о методах эффективного противодействия утечки информации.

Компетенции, формируемые в результате освоения дисциплины:

- способность производить сбор и анализ исходных информационных данных для проектирования средств измерения, контроля и испытаний (ПК-22).
- способность принимать участие в работах по расчету и проектированию деталей и узлов разрабатываемых средств измерений, испытаний и контроля в соответствии с техническими заданиями и использованием стандартных средств автоматизации проектирования (ПК-23).

Планируемые результаты обучения по дисциплине «Технические средства защиты информации», индикаторы достижения компетенций ПК-22, ПК-23, перечень оценочных средств.

№ п/п	Код индикатора достижения компетенции	Наименование индикатора достижения компетенции	Код планируемого результата обучения	Планируемые результаты обучения	Наименование оценочных средств
1.	ИД-1 ПК-22	Знать: технические каналы утечки информации	З (ИД-1 ПК-22)	Знает: разновидности технических каналов утечки информации и способы их защиты.	Вопросы на зачет
2.	ИД-2 ПК-22	Уметь: анализировать угрозы информационной безопасности объекта	У (ИД-2 ПК-22)	Умеет: защищать акустическую информацию от высокочастотного навязывания и микрофонного эффекта.	Комплекс имитационных задач
3.	ИД-3 ПК-22	Владеть: методами и средствами технической защиты информации	В (ИД-3 ПК-22)	Владеет: навыками обнаруживать электронных устройств перехвата информации.	Комплекс имитационных задач

4.	ИД-1 ПК-23	Знать: основы физической защиты объектов информатизации	З (ИД-1 ПК-23)	Знает: принципы расчета основных показателей технических каналов.	Комплекс имитационных задач
5.	ИД-2 ПК-23	Уметь: оценивать угрозы информационной безопасности объекта	У (ИД-2 ПК-23)	Умеет: обеспечивать контроль и оценку эффективности защиты речевой информации.	Комплекс имитационных задач
6.	ИД-3 ПК-23	Владеть: методами расчета и инструментального контроля показателей технической защиты информации	В (ИД-3 ПК-23)	Владеет: навыками расчёта и контроля показателей ТЗИ.	Вопросы зачёта

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-тематический план.

Номер раздела, темы	Наименование раздела, темы	Количество часов контактной работы с преподавателем	
		Лекции	Лабор.
1	***Теоретические основы технической защиты информации.***	**1,2**	2
	Информация как предмет защиты. Источники опасных сигналов.	0,2	-
	Характеристика технической разведки	0,2	-
	Технические каналы утечки информации.	0,2	-
	Средства технической разведки.	0,2	-
	Методы защиты от технических средств разведки.	0,2	-
	Организованные каналы утечки (закладные устройства) и борьба с ними	0,2	-
2	**Методы и технические средства обнаружения каналов утечки информации. Методы и технические средства защиты информации.**	**0,4**	**-**
	Методы обнаружения каналов утечки по ПЭМИН и через закладные устройства. Физические процессы при подавлении опасных сигналов.	0,2	-
	Методы инженерной защиты и технической охраны объектов. Методы скрытия информации и ее носителей. Средства предотвращения утечки информации по техническим каналам.	0,2	-
3	**Организационные основы технической защиты информации.**	**0,4**	2
	Государственная система защиты информации. Моделирование технической защиты информации.	0,2	-
	Контроль эффективности технической защиты информации. Методические рекомендации по оценке эффективности защиты информации.	0,2	-
	Итого	2	4

4.2. Содержание лекционных занятий

Тема 1. Теоретические основы технической защиты информации.

1.1. 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.

1.2. Источники опасных сигналов. Понятие об опасном сигнале. Основные и вспомогательные технические средства и системы, их классификация и характеристика. Виды опасных сигналов в помещении.

1.3. Характеристика технической разведки. Основные задачи и органы технической разведки. Принципы технической разведки. Основные этапы и процессы добывания информации технической разведкой. Классификация технической разведки.

1.4. 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.

1.5. 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.

1.6. Методы защиты от технических средств разведки. Экранирование. Компенсация излучения двухпроводной линии. Применение витых пар. Электростатические экраны. Магнитные экраны. Влияние крышек и металлических корпусов. Одновременное экранирование электрического и магнитного полей. Влияние отверстий и щелей. Конструкция крышек экранов. Экранирование электромагнитного поля излучения.

1.7 Организованные каналы утечки (закладные устройства) и борьба с ними. Организованные каналы утечки (съема) информации – закладные устройства. Закладные устройства с проводными каналами передачи. Закладные устройства с радиоканалом. Типы закладных устройств. Примеры схемных реализаций и конструктивного исполнения. Обеспечение энергетической скрытности. Проблемы обнаружения и борьбы с закладными устройствами. Потенциал радиоканала.

Тема 2. Методы и технические средства обнаружения каналов утечки информации. Методы и технические средства защиты информации.

2.1. Методы обнаружения каналов утечки по ПЭМИН и через закладные устройства. Методы обнаружения утечки за счет побочных излучений и излучений закладных устройств. Широкополосные индикаторы напряженности поля. Сканирующие узкополосные приемники. Проблемы их использования. Акустическое зондирование. Методы локализации закладных устройств. Нелинейные локаторы.

2.2. Физические процессы при подавлении 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.

*2.3. Методы инженерной защиты и технической охраны объектов***.** Классификация методов инженерной защиты и технической охраны объектов защиты. Инженерные конструкции. Автономные и централизованные системы охраны. Подсистемы обнаружения злоумышленников и пожара, видеоконтроля, нейтрализации угроз и управления охраной.

2.4. 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.

2.5. 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.

Тема 3. Организационные основы технической защиты информации.

3.1. 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.

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

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

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

4.3 Лабораторные работы

Номер темы	Наименование темы	Наименование тем лабораторных работ	Норматив времени, час.
1	Теоретические основы технической защиты информации.	*Лабораторная работа* № 1. Исследование способов защиты акустической информации от высокочастотного навязывания и микрофонного эффекта	1
		Лабораторная работа №2. Обнаружения электронных устройств перехвата информации с использованием принципов нелинейной локации	1
3	Организационные основы технической защиты информации.	*Лабораторная работа №3.* Расчет основных показателей технических каналов утечки информации.	1
		Лабораторная работа №4. Контроль и оценка эффективности защиты речевой информации.	1
		Итого	**4**

4.4 Контрольная работа.

Контрольная работа по дисциплине способствует овладению обучающимися знаний и умений по технической защите объектов информатизации с применением современных технических средств. Тема контрольной работы «Моделирование технической разведки для объекта информатизации».

Контрольная работа заключается в моделировании технической разведки для объекта информатизации в соответствии с его легендой и план-схемой. Выбор объекта информатизации согласуется с преподавателем индивидуально. Объем контрольной работы 20-25 страниц. К защите работы должны быть представлена пояснительная записка. Рекомендуемая структура пояснительной записки:

- титульный лист;
- информационная часть;
- введение;
- основная часть;
- заключение;
- список использованных источников.

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 работе.

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 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.

Преподавателем запланировано применение на лабораторных работах технологий развивающейся кооперации, коллективного взаимодействия, разбора конкретных ситуаций.

Выполнение самостоятельной работы подразумевает самостоятельное изучение разделов дисциплины, подготовку к лабораторным работам, выполнение контрольной работы и подготовку к зачету.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Самостоятельное изучение тем:	**62**
Теоретические основы технической защиты информации.	6
Методы и технические средства обнаружения каналов утечки информации. Методы и технические средства защиты информации.	6
Организационные основы технической защиты информации.	6
Физические процессы при подавлении опасных сигналов.	6
Методы инженерной защиты и технической охраны объектов.	6
Методы скрытия информации и ее носителей.	6
Средства предотвращения утечки информации по техническим каналам.	6
Моделирование технической защиты информации.	7
Контроль эффективности технической защиты информации.	7
Методические рекомендации по оценке эффективности защиты информации.	6
Подготовка к лабораторным работам (по 2 часа на каждое занятие)	4
Контрольная работа	18
Подготовка к зачету	18
Всего:	**102**

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Перечень оценочных средств

1. Отчеты студентов по лабораторным работам.
2. Контрольная работа
3. Вопросы к зачету.

6.2. Процедура оценивания результатов освоения дисциплины

Зачет проводится в форме ответа на вопросы билета. Билет состоит из 2 вопросов. Вопросы к зачету доводятся до обучающихся на последней лекции в семестре. На подготовку ответа обучающемуся отводится 1 астрономический час.

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

6.3. Примеры оценочных средств для зачета

1. Характеристика технической защиты информации как области информационной безопасности.
2. Основные проблемы 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 технической защиты информации. Показатели эффективности 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. Источники опасных сигналов. 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. Виды опасных сигналов в помещении.
14. Основные задачи и органы технической разведки. Принципы технической разведки.
15. Основные этапы и процессы добывания информации технической разведкой.
16. Классификация технической разведки по видам носителя информации и средств разведки. Возможности видов технической разведки по добыванию разведывательной информации.
17. Средства технической разведки. Визуально-оптические приборы. Акустические приемники.
18. Структура комплексов перехвата. Особенности сканирующих радиоприемников.
19. Методы защиты от технических средств разведки. Экранирование. Виды экранов.
20. Организованные каналы утечки (съема) информации – закладные устройства и их виды.
21. Примеры схемных реализаций и конструктивного исполнения закладных устройств.
22. Обеспечение энергетической скрытности. Проблемы обнаружения и борьбы с закладными устройствами.
23. Понятие и особенности утечки информации.

24. Структура, классификация и основные характеристики технических каналов утечки информации.

25. Простые и составные технические каналы утечки информации.

26. Характеристика и возможности оптических, акустических каналов утечки информации.

27. Характеристика и возможности радиоэлектронных и материально-вещественных каналов утечки информации.

28. Классификация методов технической защиты информации. Инженерная защита и техническая охрана объектов.

29. Пространственное, энергетическое и структурное скрытие информации и ее носителей.

30. Дезинформирование как метод скрытия.

31. Комплексное применение методов защиты.

32. Классификация методов инженерной защиты и технической охраны объектов защиты.

33. Инженерные конструкции. Автономные и централизованные системы охраны.

34. Модели злоумышленника.

35. Подсистемы обнаружения злоумышленников и пожара, видеоконтроля, нейтрализации угроз и управления охраной.

36. Пространственное скрытие объектов наблюдения и сигналов. Структурное и энергетическое скрытие объектов наблюдения.

37. Звукоизоляция и звукопоглощение.

38. Энергетическое скрытие радио и электрических сигналов. Виды и условия зашумления сигналов.

39. Основные инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.

40. Средства управления доступом.

41. Классификация и характеристика охранных, охранно-пожарных и пожарных извещателей.

42. Средства видеоконтроля и видеоохраны.

43. Средства нейтрализации угроз.

44. Средства управления и передачи извещений.

45. Автоматизированные интегральные системы охраны.

46. Средства маскировки и дезинформирования в оптическом и радиодиапазонах.

47. Средства звукоизоляции и звукопоглощения.

48. Средства обнаружения, локализации и подавления сигналов закладных устройств.

49. Средства подавления сигналов акустоэлектрических преобразователей, цепей электропитания и заземления.

50. Основные организационные и технические меры по защите информации.

51. Аттестация объектов, лицензирование деятельности по защите информации и сертификация ее средств.

52. Виды контроля эффективности технической защиты информации.

53. Особенности инструментального контроля эффективности инженерно-технической защиты информации.

54. Принципы моделирования объектов защиты.

55. Моделирование угроз безопасности информации.

56. Методические рекомендации по выбору рациональных вариантов защиты.

57. Способы оптимизации мер технической защиты информации.

58. Способы оценки эффективности охраны объектов защиты.

59. Оценка эффективности защиты видовых признаков объектов наблюдения.

60. Способы оценки безопасности речевой информации в помещении.

Примерные тематики контрольных работ

1. Защита информации с помощью инженерных средств.

2. Защита информации с помощью технических систем охранно-пожарной сигнализации.

3. Техническая разведка как угроза безопасности информации.

4. Виды и основные характеристики датчиков охраны и пожара.

5. Защита информации с помощью технических систем управления доступом.

6. Защита информации с помощью технических систем охранного телевидения.

7. Защита информации с помощью интегрированных систем охраны.

8. Понятие и классификация технических каналов утечки информации; роль и значение соответствующей системы понятий и определений в теории и практике ИТЗИ.

9. Технические каналы утечки информации «типовых» объектов информатизации.

10. Выявление электрических каналов утечки информации служебных кабинетов.

11. Поисковые приборы, используемые в сфере защиты информации.

12. Защита информации от несанкционированных воздействий.

6.5. Фонд оценочных средств

Полный банк заданий для текущего контроля 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]: Учебное пособие для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков, И.В. Голубятников. - 4-е изд., испр. и доп. – М.: Горячая линия-Телеком, 2012 г., 616 с. – Доступ из ЭБС «Консультант студента»

2. Инструментальный контроль и защита информации. [Электронный ресурс]: учеб. Пособие / Свинарев Н.А., Ланкин О.В., Данилкин А.П., Потехецкий С.В., Перетокин О.И. – Воронеж: ВГ*УИТ, 2013. – 192 с. – Доступ из ЭБС «Консультант студента»

7.2. Дополнительная литература

1. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации [Электронный ресурс] / Бузов Г.А. – М.: Горячая линия – Телеком, 2010. – 240 с. – Доступ из ЭБС «Консультант студента»

2. Защита информации ограниченного доступа от утечки по техническим каналам [Электронный ресурс] / Бузов Г.А. – М.: Горячая линия – Телеком, 2015. – 586 с. – Доступ из ЭБС «Консультант студента»

7.3 Методическая литература

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 и направления 10.03.01. КГУ. 2016. – Доступ из ЭБС КГУ.

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 и студентов очно-заочной формы обучения направления 10.03.01. КГУ. 2016. – Доступ из ЭБС КГУ.

3. Методические указания к выполнению лабораторной работы «Обнаружение оптических сигналов передатчиков ИК-диапазона» по дисциплине «Техническая защита информации» для студентов специальности 10.05.03 и студентов очно-заочной формы обучения направления 10.03.01. КГУ. 2016. – Доступ из ЭБС КГУ.

4. Методические указания к выполнению лабораторной работы «Обнаружение сигналов линейных и сетевых закладок» по дисциплине «Техническая защита информации» для студентов специальности 10.05.03 и студентов очно-заочной формы обучения направления 10.03.01. КГУ. 2016. – Доступ из ЭБС КГУ.

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 и студентов очно-заочной формы обучения направления 10.03.01. КГУ. 2016. – Доступ из ЭБС КГУ.

6. Методические указания к выполнению лабораторной работы «Оценка защищенности помещения от утечки информации по каналам акустоэлектрических преобразований технических средств с помощью

комплекса «Спрут-мини» по дисциплине «Техническая защита информации» для студентов специальности 10.05.03 и студентов очно-заочной формы обучения направления 10.03.01. КГУ. 2017. – Доступ из ЭБС КГУ.

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 и студентов очно-заочной формы обучения направления 10.03.01. КГУ. 2017. – Доступ из ЭБС КГУ.

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 и студентов очно-заочной формы обучения направления 10.03.01. 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 и студентов очно-заочной формы обучения направления 10.03.01. КГУ. 2017.

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

1. Официальный сайт Федеральной службы по техническому 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. Единое окно доступа к образовательным ресурсам. – http://window.edu.ru/;
7. Научная электронная библиотека - http://elibrary.ru/;
8. Электронная библиотека КГУ - http://dspace.kgsu.ru/xmlui/;
9. Информационный онлайн портал ISO27000.ru - http://www.iso27000.ru/;

10. Безопасность - http://groteck.ru/security;

11. Статьи по теме «Средства защиты информации» - http://www.bnti.ru/articles.asp?lvl=04.03.

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

«Технические средства защиты информации»

образовательной программы высшего образования –
программы бакалавриата

27.03.01 Стандартизация и метрология
Стандартизация, метрология и управление качеством

Трудоемкость дисциплины: 3 з.е. (108 академических часа)
Семестр: 4
Форма промежуточной аттестации: зачет
Содержание дисциплины. Основные разделы.

Концепция технической защиты информации. Теоретические основы технической защиты информации. Методы и технические средства обнаружения каналов утечки информации. Методы и технические средства защиты информации. Организационные основы технической защиты информации.

ЛИСТ
регистрации изменений (дополнений) в рабочую программу
учебной дисциплины
«Технические средства защиты информации»

Изменения / дополнения в рабочую программу
на 20___ / 20___ учебный год:

_____
_____
_____
_____
_____
_____

Ответственный преподаватель _____ / Москвин В.В. /

Изменения утверждены на заседании кафедры «___»_____20___ г.,
Протокол № ___

Заведующий кафедрой _____ «___»_____20___ г.

Изменения / дополнения в рабочую программу
на 20___ / 20___ учебный год:

_____
_____
_____
_____
_____
_____

Ответственный преподаватель _____ / Москвин В.В. /

Изменения утверждены на заседании кафедры «___»_____20___ г.,
Протокол № ___

Заведующий кафедрой _____ «___»_____20___ г.