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
«__» _____ 2021 г.

Рабочая программа учебной дисциплины

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

образовательной программы высшего образования –
программы бакалавриата

15.03.04 Автоматизация технологических процессов и производств

Направленность: Автоматизация технологических процессов и производств (в машиностроении)
Форма обучения: очная, заочная

Курган 2021

Рабочая программа дисциплины «Технические средства защиты информации» составлена в соответствии с учебным планом по программе бакалавриата «Автоматизация технологических процессов и производств (в машиностроении)», утвержденной для очной и заочной формы обучения «30» августа 2021 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» «29» сентября 2021, протокол № 2.

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

Согласовано:

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

Заведующий кафедрой «Автоматизация производственных процессов»
канд. тех. наук, доцент _____ И.А. Иванова

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

1. ОБЪЕМ ДИСЦИПЛИНЫ

Очная форма

Всего: 3 зачетных единицы трудоемкости (108 академических часа)

Вид учебной работы	На всю дисциплину	Семестр
		3
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**32**	**32**
Лекции	16	16
Лабораторные работы	16	16
Самостоятельная работа, всего часов в том числе:	**76**	**76**
Подготовка к зачету	18	18
Другие виды самостоятельной работы (изучение тем, подготовка к лабораторным работам и рубежному контролю)	58	58
Вид промежуточной аттестации	**зачет**	**зачет**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**108**	**108**

Заочная форма

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».

Результаты обучения по дисциплине необходимы для изучения дисциплин «Проектирование автоматизированных систем», «Диагностика и надёжность автоматизированных систем», «Автоматизированные расчеты в технических системах», «Организация и планирование автоматизированных производств», а также для выполнения разделов курсовых проектов по дисциплинам базовой части и выпускной квалификационной работы.

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:

— способностью собирать и анализировать исходные информационные данные для проектирования технологических процессов изготовления продукции, средств и систем автоматизации, контроля, технологического оснащения, диагностики, испытаний, управления процессами, жизненным циклом продукции и ее качеством; участвовать в работах по расчету и проектированию процессов изготовления продукции и указанных средств и систем с использованием современных информационных технологий, методов и средств проектирования (ПК-1).

В результате изучения дисциплины обучающийся должен:

знать:

- технические каналы утечки информации (для ПК-1);
- основы физической защиты объектов информатизации (для ПК-1);

уметь:

- анализировать и оценивать угрозы информационной безопасности объекта (для ПК-1).

владеть:

- методами и средствами технической защиты информации (для ПК-1);
- методами расчета и инструментального контроля показателей технической защиты информации (для ПК-1).

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-тематический план.

Рубеж	Номер раздела, темы	Наименование раздела, темы	Количество часов контактной работы с преподавателем			
			Очная		Заочная	
			Лекции	Лабор.	Лекции	Лабор.
Рубеж 1	1	**Введение. Концепция инженерно-технической защиты информации.** Цели и задачи курса. Содержание дисциплины. Системный подход к защите информации. Основные концептуальные положения инженерно-технической защиты информации.	**1**	-	-	-
	2	***Теоретические основы технической защиты информации.***	**7**	**9**	**1,2**	2
		Информация как предмет защиты. Источники опасных сигналов.	1		0,2	
		Характеристика технической разведки	1		0,2	
		Технические каналы утечки информации.	1		0,2	
		Средства технической разведки.	2		0,2	
		Методы защиты от технических средств разведки.	1		0,2	
		Организованные каналы утечки (закладные устройства) и борьба с ними	1		0,2	
Рубеж 2	3	**Методы и технические средства обнаружения каналов утечки информации. Методы и технические средства защиты информации.**	**4**		**0,4**	
		Методы обнаружения каналов утечки по ПЭМИН и через закладные устройства. Физические процессы при подавлении опасных сигналов.	2		0,2	
		Методы инженерной защиты и технической охраны объектов. Методы скрытия информации и ее носителей. Средства предотвращения утечки информации по техническим каналам.	2		0,2	
	4	**Организационные основы технической защиты информации.**	**4**	7	**0,4**	2
		Государственная система защиты информации. Моделирование технической защиты информации.	2		0,2	
		Контроль эффективности технической защиты информации. Методические рекомендации по оценке эффективности защиты информации.	2		0,2	
		Всего:	**16**	**16**	**2**	**4**

4.2. Содержание лекционных занятий

Тема 1. Концепция технической защиты информации.

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

1.2. Системный подход к защите информации. Характеристика технической защиты информации как области информационной безопасности. Основные проблемы технической защиты информации. Представление сил и средств защиты информации в виде системы. Основные параметры системы защиты информации.

1.3. Основные концептуальные положения технической защиты информации. Цели и задачи защиты информации. Ресурсы, выделяемые на защиту информации. Принципы защиты информации техническими средствами. Основные направления технической защиты информации. Показатели эффективности технической защиты информации.

Тема 2. Теоретические основы 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. 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.

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.

2.5. 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.

2.6. 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.

2.7 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 3. Методы и технические средства обнаружения каналов утечки информации. Методы и технические средства защиты информации.

3.1. 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.

3.2. 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.

3.3. 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.

3.4. 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.

3.5. 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 4. Организационные основы технической защиты информации.

4.1. 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.

4.2. 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.

4.3. 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.

4.4. 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.	
			очная	заочная
2	***Теоретические основы технической защиты информации.***	*Лабораторная работа* № 1. Исследование способов защиты акустической информации от высокочастотного навязывания и микрофонного эффекта	4	1
2	***Теоретические основы технической защиты информации.***	*Лабораторная работа №2.* Обнаружения электронных устройств перехвата информации с использованием принципов нелинейной локации	4	1
	1-ый рубежный контроль	***Тестирование***	***1***	-
4	**Организационные основы технической защиты информации.**	*Лабораторная работа №3.* Расчет основных показателей технических каналов утечки информации.	2	1
4	**Организационные основы технической защиты информации.**	*Лабораторная работа №4.* Контроль и оценка эффективности защиты речевой информации.	4	1
	2-ой рубежный контроль	***Тестирование***	***1***	-
		Итого	**16**	**4**

4.4 Контрольная работа (для заочной формы).

Контрольная работа по дисциплине способствует овладению студентами 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.

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 работах в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает самостоятельное изучение разделов дисциплины, подготовку к лабораторным работам, выполнение контрольной работы (для заочной формы), к рубежным контролям (для очной формы) и подготовку к зачету.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы
Очная форма

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Самостоятельное изучение тем:	**46**
Теоретические основы технической защиты информации.	4

Методы обнаружения каналов утечки по ПЭМИН и через закладные устройства.	3
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.	5
Моделирование технической защиты информации.	6
Контроль эффективности технической защиты информации.	4
Методические рекомендации по оценке эффективности защиты информации.	6
Подготовка к лабораторным работам (по 2 часа на каждое занятие)	8
Подготовка к рубежным контролям (по 2 часа на каждый рубежный контроль)	4
Подготовка к зачету	18
Всего:	**76**

Заочная форма

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Самостоятельное изучение тем:	**62**
Теоретические основы технической защиты информации.	6
Методы обнаружения каналов утечки по ПЭМИН и через закладные устройства.	6
Физические процессы при подавлении опасных сигналов.	6
Методы инженерной защиты и технической охраны объектов.	8
Методы скрытия информации и ее носителей.	8
Средства предотвращения утечки информации по техническим каналам.	6
Моделирование технической защиты информации.	8
Контроль эффективности технической защиты информации.	6
Методические рекомендации по оценке эффективности защиты информации.	8
Подготовка к лабораторным работам (по 1 часу 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. Балльно-рейтинговая система контроля и оценки академической активности студентов в КГУ (очная форма обучения).
2. Отчеты студентов по лабораторным работам.
3. Банк тестовых заданий к рубежным контролям № 1, № 2. (очная форма обучения)
4. Контрольная работа (заочная форма).
5. Вопросы к зачету.

6.2. Система балльно-рейтинговой оценки работы студентов по дисциплине

№	Наименование	Содержание					
1	Распределение баллов за семестр по видам учебной работы, сроки сдачи учебной работы *(доводятся до сведения студентов на первом учебном занятии)*	Распределение баллов, 3 семестр					
		Вид учебной работы:	Посещение лекций	Выполнение лабораторной работы	Рубежный контроль №1	Рубежный контроль №2	Зачет
		Балльная оценка:	$2_б$ х 8= $16_б$	$7_б$ х 4 =$28_б$	13	13	30
2	Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и зачета	60 и менее баллов – неудовлетворительно; не зачтено; 61…73 – удовлетворительно; зачтено; 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 (зачету) студент должен набрать по итогам текущего и рубежного контроля не менее 50 баллов и должен выполнить все лабораторные работы и контрольную работу (для заочной формы). Для получения зачета «автоматически» студенту необходимо набрать 61 балл. По согласованию с преподавателем студенту могут быть добавлены дополнительные (бонусные) баллы за активность на лабораторных работах, активное участие в научной и методической работе, оригинальность принятых решений в ходе выполнения лабораторных работ, за участие в значимых учебных и внеучебных мероприятиях кафедры.					
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) 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 работ. Формы дополнительных заданий (назначаются преподавателем): - выполнение и защита пропущенной лабораторной работы (при невозможности дополнительного проведения лабораторной работы преподаватель устанавливает форму дополнительного задания по тематике пропущенной лабораторной работы самостоятельно) – до 7 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 состоят для 1 и 2 рубежного контроля из 13 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 проводится в форме ответа на вопросы билета. Билет состоит из 2 вопросов. Вопросы к зачету доводятся до студентов на последней лекции в семестре. Каждый вопрос оценивается в 15 баллов. На подготовку ответа студенту 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 студента.

6.4. Примеры оценочных средств для рубежных контролей и зачета

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: _____

3. 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

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.

3. 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

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

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. 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. Средства технической разведки. Визуально-оптические приборы. Акустические приемники.
20. Структура комплексов перехвата. Особенности сканирующих радиоприемников.
21. Методы защиты от технических средств разведки. Экранирование. Виды экранов.
22. Организованные каналы утечки (съема) информации – закладные устройства и их виды.
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.
37. Основные инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.

38. Средства управления доступом.
39. Классификация и характеристика охранных, охранно-пожарных и пожарных извещателей.
40. Средства видеоконтроля и видеоохраны.
41. Средства нейтрализации угроз.
42. Средства управления и передачи извещений.
43. Автоматизированные интегральные системы охраны.
44. Средства маскировки и дезинформирования в оптическом и радиодиапазонах.
45. Средства звукоизоляции и звукопоглощения.
46. Средства обнаружения, локализации и подавления сигналов закладных устройств.
47. Средства подавления сигналов акустоэлектрических преобразователей, цепей электропитания и заземления.
48. Основные организационные и технические меры по защите информации.
49. Аттестация объектов, лицензирование деятельности по защите информации и сертификация ее средств.
50. Виды контроля эффективности технической защиты информации.
51. Особенности инструментального контроля эффективности инженерно-технической защиты информации.
52. Принципы моделирования объектов защиты.
53. Моделирование угроз безопасности информации.
54. Методические рекомендации по выбору рациональных вариантов защиты.
55. Способы оптимизации мер технической защиты информации.
56. Способы оценки эффективности охраны объектов защиты.
57. Оценка эффективности защиты видовых признаков объектов наблюдения.
58. Способы оценки безопасности речевой информации в помещении.

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]: 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

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

При чтении лекций используются слайдовые презентации.

Программные средства обеспечения учебного процесса включают в себя: базовые (операционные системы); инструментальные средства программирования), вспомогательные (программы презентационной графики; текстовые редакторы; графические редакторы) и средства защиты.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Материально-техническое обеспечение дисциплины включает в себя учебные аудитории и лаборатории, оснащенные проекционным оборудованием с экраном, современными компьютерами (все – в стандартной комплектации для практических занятий и самостоятельной работы), объединенными локальными вычислительными сетями с выходом в Интернет, средства выявления каналов утечки информации, средства проверки на соответствие требованиям защиты от утечек по техническим каналам. Обучающемуся предоставляется возможность практической работы.

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

15.03.04 Автоматизация технологических процессов и производств
Направленность: Автоматизация технологических процессов и производств (в машиностроении)

Трудоемкость дисциплины: 3 з.е. (108 академических часа для очной и заочной форм обучения)

Семестр: 3 (очная форма обучения)

Семестр: 4 (заочная форма обучения)

Форма промежуточной аттестации: зачет (очная форма обучения)

Форма промежуточной аттестации: зачет + КР (заочная форма обучения)

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.