МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Директор департамента образования
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Техническая защита информации

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **25.05.03 Техническая эксплуатация транспортного радиооборудования**
Направленность (профиль) / специализация: **Техническая эксплуатация радиоэлектронного оборудования воздушных судов и аэропортов**
Форма обучения: **очная**
Факультет: **РКФ, Радиоконструкторский факультет**
Кафедра: **КИПР, Кафедра конструирования и производства радиоаппаратуры**
Курс: **5**
Семестр: **9**
Учебный план набора 2018 года

Распределение рабочего времени

№	Виды учебной деятельности	9 семестр	Всего	Единицы
1	Лекции	28	28	часов
2	Практические занятия	28	28	часов
3	Лабораторные работы	16	16	часов
4	Всего аудиторных занятий	72	72	часов
5	Самостоятельная работа	36	36	часов
6	Всего (без экзамена)	108	108	часов
7	Подготовка и сдача экзамена	36	36	часов
8	Общая трудоемкость	144	144	часов
		4.0	4.0	З.Е.

Экзамен: 9 семестр

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Шелупанов А.А.
Должность: Ректор
Дата подписания: 20.12.2017
Уникальный программный ключ:
c53e145e-8b20-45aa-9347-a5e4dbb90e8d

Томск

Согласована на портале № 47771

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от «21» 5 2019 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 25.05.03 Техническая эксплуатация транспортного радиооборудования , утвержденного 12.09.2016 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчик:
доцент каф. КИБЭВС _____ Д. В. Кручинин

Заведующий обеспечивающей каф.
КИБЭВС _____ А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан РКФ _____ Д. В. Озеркин

Заведующий выпускающей каф.
КИПР _____ В. М. Карабан

Эксперты:

Доцент кафедры безопасности информационных систем (БИС) _____ О. О. Евсютин

Доцент кафедры конструирования и производства радиоаппаратуры (КИПР) _____ Н. Н. Кривин

Согласована на портале № 47771

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью дисциплины «Техническая защита информации» является теоретическая и практическая подготовка студентов по вопросам защиты информации от утечки по техническим каналам (технической защиты информации) на объектах информатизации и в выделенных помещениях, по вопросам применения нормативных правовых актов в своей профессиональной деятельности, участия в проведении аттестации телекоммуникационных систем по требованиям защиты информации.

1.2. Задачи дисциплины

- Изучение технических каналов утечки информации, их характеристик, способов
- добывания информации техническими средствами разведки;
- Изучение методики выявления технических каналов утечки информации на объекте
- информатизации или в выделенном помещении;
- Изучение способов выявления и оценки утечки информации по
- акустическому/виброакустическому калану утечки информации;
- Изучение способов выявления и оценки утечки информации по каналу побочных
- электромагнитных излучений и наводок;
- Изучение методов и технических средств охраны объекта информатизации и
- выделененного помещения;
- Изучение нормативных докментов и методики оценки соответствия объекта
- информатизации или выделенного помещения требованиям по безопасности от утечки
- информации по техническим каналам.

2. Место дисциплины в структуре ОПОП

Дисциплина «Техническая защита информации» (Б1.Б.37) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Физика.

Последующими дисциплинами являются: Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты, Преддипломная практика.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ОПК-6 способностью понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны;

В результате изучения дисциплины обучающийся должен:

- **знать** технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам.
- **уметь** анализировать и оценивать угрозы информационной безопасности объекта; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем. пользоваться нормативными документами по защите информации.
- **владеть** методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации; методами формирования требований по защите информации; методами расчета и инструментального контроля показателей технической защиты информации.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 4.0 зачетных единицы и представлена в табли-

Согласована на портале № 47771

це 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		9 семестр
Аудиторные занятия (всего)	72	72
Лекции	28	28
Практические занятия	28	28
Лабораторные работы	16	16
Самостоятельная работа (всего)	36	36
Оформление отчетов по лабораторным работам	9	9
Проработка лекционного материала	11	11
Подготовка к практическим занятиям, семинарам	16	16
Всего (без экзамена)	108	108
Подготовка и сдача экзамена	36	36
Общая трудоемкость, ч	144	144
Зачетные Единицы	4.0	4.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лек., ч	Прак. зан., ч	Лаб. раб., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
9 семестр						
1 Концепция инженернотехнической защиты информации	4	0	0	2	6	ОПК-6
2 Теоретические основы инженерно-технической защиты информации	6	0	0	2	8	ОПК-6
3 Физические основы защиты информации	6	16	0	8	30	ОПК-6
4 Технические средства добывания и инженернотехнической защиты информации	8	0	16	12	36	ОПК-6
5 Организационные основы инженернотехнической защиты информации	2	6	0	5	13	ОПК-6
6 Методическое обеспечение инженернотехнической защиты информации	2	6	0	7	15	ОПК-6
Итого за семестр	28	28	16	36	108	
Итого	28	28	16	36	108	

Согласована на портале № 47771

5.2. Содержание разделов дисциплины (по лекциям)

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины (по лекциям)	Трудоемкость, ч	Формируемые компетенции
9 семестр			
1 Концепция инженернотехническо й защиты информации	Характеристика инженерно-технической защиты информации. Технические средства и методы защиты информаци-и.Основные проблемы и параметры инженерно-технической защиты информации. Представление методов и средств защиты информации как системы. Показатели эффективности инженерно-технической защиты информации.	2	ОПК-6
	Цели и задачи защиты информации.Ресурсы, выделяемые на защиту информации. Основные направления инженерно-технической защиты информации. Принципы защиты информации техническими средствами.	2	
	Итого	4	
2 Теоретические основы инженернотехническо й защиты информации	Информация как предмет защиты. Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения и сигналов. Понятие о текущей и эталонной признаковой структуре.Источники опасных сигналов. Понятие об опасном сигнале. Опасные сигналы и их источники. Основные и вспомогательные технические средства и системы как источники опасных сигналов. Состав и характеристика основных и вспомогательных технических средств и систем. Побочные электромагнитныеизлучения и наводки. Виды побочных опасных электромагнитных излучений. Случайные антенны. Виды опасных сигналов на объектах информатизации.	1	ОПК-6
	Характеристика технической разведки. Основные задачи и органы технической разведки. Принципы техническойразведки. Основные этапы и процедуры добывания информации технической разведкой. Классификация технической разведки по видам носителя информации и средств разведки. Возможности видов технической разведки. Основныенаправления развития технической разведки. Технические каналы утечки информации. Понятие и	2	

Согласована на портале № 47771

	особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их возможности.		
	Методы инженерной защиты и технической охраны объектов. Классификация методов инженерной защиты и технической охраны объектов. Инженерные конструкции. Автономные и централизованные системы охраны объектов. Модели злоумышленников. Подсистемы обнаружения злоумышленников и пожара, видеоконтроля, нейтрализации угроз. Способы повышения помехоустойчивости средств обнаружения злоумышленников и пожара.	2	
	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.	1	
	Итого	6	
3 Физические основы защиты информации	Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. Источники побочных излучений, их физическая природа. Характер электромагнитных излучений в ближней и дальней зонах. Виды паразитных связей и наводок. Паразитная генерация радиоэлектронных средств. Физические явления, вызывающие утечку информации по цепям электропитания, заземления и токопроводящим конструкциям здания	2	ОПК-6
	Распространение сигналов в технических каналах утечки информации. Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях. Распространение оптических сигналов в атмосфере и в световодах	1	
	Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи. Основные показатели среды распространения сигна-	1	

Согласована на портале № 47771

	лов различных технических каналов утечки информации.		
	Физические процессы подавление опасных сигналов. Подавление опасных сигналов акустоэлектрических преобразователей. Экранирование электрических, магнитных, и электромагнитных полей. Требования к экранам. Компенсация полей. Подавление опасных сигналов в цепях электропитания и заземления. Зашумление опасных сигналов помехами.	2	
	Итого	6	
4 Технические средства добывания и инженернотехнической защиты информации	Средства технической разведки. Визуально-оптические приборы. Фотоаппараты. Оптоэлектронные приборы наблюдения в видимом и инфракрасном диапазонах. Акустические приемники. Направленные микрофоны. Структура комплексов перехвата. Особенности сканирующих радиоприемников. Закладные устройства, средства ВЧ-навязывания и лазерногоподслушивания. Автономные средства разведки	2	ОПК-6
	Средства инженерной защиты и технической охраны. Методы и средства инженерной защиты и технической охраны объектов. Скрытие объектов наблюдения. Основные инженерные конструкции, применяемые дляпредотвращения проникновения злоумышленника к источникам информации. Средства управления доступом. Классификация и характеристика охранных, охраннопожарных и пожарных извещателей. Средства видеоконтроля и видеоохраны. Средства нейтрализации угроз. Средства управления и передачи извещений. Автоматизированные интегральные системы охраны.	4	
	Средства предотвращения утечки информации по техническим каналам. Средства маскировки и дезинформирования в оптическом и радиодиапазонах. Скрытие речевой информации в каналах связи. Энергетическое скрытие акустических информативных сигналов. Средства звукоизоляции из звукопоглощения. Обнаружение и локализация закладных устройств, подавление их сигналов. Подавление опасных сигналов акустоэлектрических преобразователей, экранирование и компенсация информативных полей. Подавление информативных сигналов в цепях заземле-	2	

Согласована на портале № 47771

	ния и электропитания. Подавление опасных сигналов. Генераторы линейного и пространственного зашумления.		
	Итого	8	
5 Организационные основы инженернотехническо й защиты информации	Государственная система защиты информации. Характеристика государственной системы противодействия технической разведке. Нормативные документы по противодействию технической разведке. Основные организационные и технические меры по защите информации. Аттестация объектов, лицензирование деятельности по защите информации и сертификация ее средств.Контроль эффективности инженерно-технической защиты информации. Виды контроля эффективности защиты информации. Основные положения методологии инженерно-технической защиты информации. Требования по защите информации от утечки по техническим каналам. Методы расчета и инструментального контроля показателей защиты информации. Особенности инструментального контроля эффективности инженерно-технической защиты информации.	2	ОПК-6
	Итого	2	
6 Методическое обеспечение инженернотехническо й защиты информации	Моделирование инженерно-технической защиты информации. Концепция и методы инженерно-технической защитыинформации. Основные этапы проектирования и оптимизации системы инженерно-технической защиты информации. Принципы моделирования объектов защиты. Моделирование угроз безопасности информации. Методические рекомендации по выбору рациональных вариантов защиты. Пути оптимизации мер инженерно-технической защиты информации.Принципы оценки эффективности инженерно-технической защиты информации. Принципы оценки эффективности охраны объектов защиты. Возможности оценки видовых признаковобъектов наблюдения. Подходы к определению безопасности речевой информации в защищаемых помещениях. Принципы оценки размеров опасных зон Iи II.	2	ОПК-6
	Итого	2	
Итого за семестр		28	

Согласована на портале № 47771

5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представлены в таблице 5.3.

Таблица 5.3 – Разделы дисциплины и междисциплинарные связи

Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин					
	1	2	3	4	5	6
Предшествующие дисциплины						
1 Физика		+	+			
Последующие дисциплины						
1 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты		+		+	+	+
2 Преддипломная практика	+	+	+	+	+	+

5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4.

Таблица 5.4 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Компетенции	Виды занятий				Формы контроля
	Лек.	Прак. зан.	Лаб. раб.	Сам. раб.	
ОПК-6	+	+	+	+	Экзамен, Отчет по лабораторной работе, Опрос на занятиях, Тест

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Таблица 7.1 – Наименование лабораторных работ

Названия разделов	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
9 семестр			
4 Технические средства добывания и инженернотехнической защиты информации	Статистический анализ загрузки заданного радиодиапазона и обнаружение радиозакладных устройств в охраняемомпомещении.	2	ОПК-6
	Нелинейная локация.	2	
	Обнаружение активных прослушивающих устройств с помощью индикатораэлектромагнитного поля	2	
	Аппаратно-программный комплекс имитации сигналов закладочных устройств «АВРОРА-Т»	2	
	Охрана выделенных помещений.Пожарная	2	

Согласована на портале № 47771

	сигнализация.		
	Охрана выделенных помещений.Охранная сигнализация.	2	
	Ограничение доступа в выделенное помещение. Система контроля и управления доступом.	2	
	Охрана выделенных помещений. Система видеонаблюдения.	2	
	Итого	16	
Итого за семестр		16	

8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8.1 – Наименование практических занятий (семинаров)

Названия разделов	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
9 семестр			
3 Физические основы защиты информации	Моделирование систем нелинейнойлокации	6	ОПК-6
	Моделирование пассивных фильтров(низкой и высокой частоты, полосовых ирежекторных фильтров)	6	
	Моделирование активных фильтров	4	
	Итого	16	
5 Организационные основы инженернотехническ ой защиты информации	Организационные мероприятия поподготовке и проведению аттестациюобъектов информатизации по требованиямбезопасности	6	ОПК-6
	Итого	6	
6 Методическое обеспечение инженернотехническ ой защиты информации	Методическое обеспечение проведенияаттестации объектов информатизации потребованиям безопасности. Расчётразмеров опасных зон I и II	6	ОПК-6
	Итого	6	
Итого за семестр		28	

9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Таблица 9.1 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
9 семестр				
1 Концепция инженернотехнической защиты информации	Проработка лекционного материала	1	ОПК-6	Тест
	Проработка лекционного материала	1		

Согласована на портале № 47771

	Итого	2		
2 Теоретические основы инженернотехнической защиты информации	Проработка лекционного материала	1	ОПК-6	Тест
	Проработка лекционного материала	1		
	Итого	2		
3 Физические основы защиты информации	Подготовка к практическим занятиям, семинарам	6	ОПК-6	Опрос на занятиях, Тест, Экзамен
	Проработка лекционного материала	1		
	Проработка лекционного материала	1		
	Итого	8		
4 Технические средства добывания и инженернотехнической защиты информации	Проработка лекционного материала	1	ОПК-6	Отчет по лабораторной работе, Тест
	Проработка лекционного материала	1		
	Проработка лекционного материала	1		
	Оформление отчетов по лабораторным работам	9		
	Итого	12		
5 Организационные основы инженернотехнической защиты информации	Подготовка к практическим занятиям, семинарам	4	ОПК-6	Опрос на занятиях, Тест, Экзамен
	Проработка лекционного материала	1		
	Итого	5		
6 Методическое обеспечение инженернотехнической защиты информации	Подготовка к практическим занятиям, семинарам	6	ОПК-6	Опрос на занятиях, Тест, Экзамен
	Проработка лекционного материала	1		
	Итого	7		
Итого за семестр		36		
	Подготовка и сдача экзамена	36		Экзамен
Итого		72		

Согласована на портале № 47771

10. Курсовой проект / курсовая работа

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

Элементы учебной деятельности	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
9 семестр				
Опрос на занятиях	5	5	10	20
Отчет по лабораторной работе	5	5	10	20
Тест	10	10	10	30
Итого максимум за период	20	20	30	70
Экзамен				30
Нарастающим итогом	20	40	70	100

11.2. Пересчет баллов в оценки за контрольные точки

Пересчет баллов в оценки за контрольные точки представлен в таблице 11.2.

Таблица 11.2 – Пересчет баллов в оценки за контрольные точки

Баллы на дату контрольной точки	Оценка
≥ 90% от максимальной суммы баллов на дату КТ	5
От 70% до 89% от максимальной суммы баллов на дату КТ	4
От 60% до 69% от максимальной суммы баллов на дату КТ	3
< 60% от максимальной суммы баллов на дату КТ	2

11.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 11.3.

Таблица 11.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка (ГОС)	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 - 100	A (отлично)
4 (хорошо) (зачтено)	85 - 89	B (очень хорошо)
	75 - 84	C (хорошо)
	70 - 74	D (удовлетворительно)
3 (удовлетворительно) (зачтено)	65 - 69	
	60 - 64	E (посредственно)
2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

Согласована на портале № 47771

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Инженерно-техническая защита информации [Электронный ресурс]: Учебное пособие / А. А. Титов - 2010. 195 с. — Режим доступа: https://edu.tusur.ru/publications/654 (дата обращения: 24.06.2019).
2. Защита информации от утечки по техническим каналам [Электронный ресурс]: Учебное пособие / А. М. Голиков - 2015. 256 с. — Режим доступа: https://edu.tusur.ru/publications/5263 (дата обращения: 24.06.2019).

12.2. Дополнительная литература

1. Закон Российской Федерации «О государственной тайне» от 21 июля 1993 г. № 5485-1. [Электронный ресурс] / Доступ из сети Интернет. [Электронный ресурс] [Электронный ресурс]: — Режим доступа: (дата обращения: 19.05.2018). — Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&n=220985&base=LAW&rnd=244973.253852992#08952597261322699 (дата обращения: 24.06.2019).
2. Закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. №149-ФЗ. [Электронный ресурс] / Доступ из сети Интернет. (дата обращения [Электронный ресурс]: 19.05.2018). — Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&n=286904&base=LAW&rnd=244973.246476619#07577379674885092 (дата обращения: 24.06.2019).
3. Закон Российской Федерации «О персональных данных» от 27 июля 2006 г. №152-ФЗ. [Электронный ресурс] / Доступ из сети Интернет. (дата обращения [Электронный ресурс]: 19.05.2018). — Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&n=286959&base=LAW&rnd=244973.626813432#0458630399804713 (дата обращения: 24.06.2019).
4. Зайцев, Александр Петрович. Технические средства обеспечения информационной безопасности [] : Учебное пособие для вузов. Ч. 2 : Средства защиты информации по техническим каналам : учебное пособие. - Томск : ТМЦДО , 2004. - 279 с. (наличие в библиотеке ТУСУР - 30 экз.)
5. Зайцев, Александр Петрович. Технические средства обеспечения информационной безопасности [] : Учебное пособие для вузов. Ч. 1 : Технические каналы утечки информации. - Томск : ТМЦДО , 2004. - 199 с. (наличие в библиотеке ТУСУР - 30 экз.)

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Зайцев, Александр Петрович. Технические средства и методы защиты информации : Лабораторный практикум: Учебное пособие. - Томск : В-Спектр , 2007. - 119[1] с. (наличие в библиотеке ТУСУР - 65 экз.)
2. Защита информации [Электронный ресурс]: Методические указания к выполнению лабораторных работ / В. Г. Спицын - 2012. 77 с. — Режим доступа: https://edu.tusur.ru/publications/1826 (дата обращения: 24.06.2019).
3. Защита информации [Электронный ресурс]: Методические указания к выполнению самостоятельных работ / В. Г. Спицын - 2012. 78 с. — Режим доступа: https://edu.tusur.ru/publications/2261 (дата обращения: 24.06.2019).
4. Защита речевой информации от утечки по акустическим и виброакустическим каналам [Электронный ресурс]: Руководство к практическим занятиям и лабораторным работам / Р. С. Круглов, М. В. Южанин - 2007. 49 с. — Режим доступа: https://edu.tusur.ru/publications/994 (дата обращения: 24.06.2019).

12.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа лиц с ограниченными возможностями здоровья и инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Согласована на портале № 47771

Для лиц с нарушениями зрения:

– в форме электронного документа;
– в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

– в форме электронного документа;
– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

– в форме электронного документа;
– в печатной форме.

12.4. Профессиональные базы данных и информационные справочные системы

1. https://edu.tusur.ru – образовательный портал университета;
2. http://www.iqlib.ru – электронная интернет-библиотека;
3. http://www.biblioclub.ru – полнотестовая электронная библиотека;
4. http://www.elibrary.ru – научная электронная библиотека;
5. http://www.edu.ru – веб-сайт системы федеральных образовательных порталов.
6. http://lib.tusur.ru/ru/resursy/bazy-dannyh - профессиональные базы данных, доступ к которым оформлен библиотекой ТУСУРа в текущий момент времени

13. Материально-техническое обеспечение дисциплины и требуемое программное обеспечение

13.1. Общие требования к материально-техническому и программному обеспечению дисциплины

13.1.1. Материально-техническое и программное обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью. Имеются демонстрационное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

13.1.2. Материально-техническое и программное обеспечение для практических занятий

Лаборатория защищенных автоматизированных систем

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 511 ауд.

Описание имеющегося оборудования:

- Компьютеры: AMD A6-3670/ Asus F1A75-M Pro / DDR3 4 Gb/ ST3250410AS 250 Gb / мышь/ клавиатура/ монитор (5 шт.);
- ИБП Ippon;
- Стенд "Средства контроля и управления доступом" в составе: Сетевой контроллер СКУД Gate-4000 UPS, контроллер управления доступом UnitECO LOCK 2S-LO-SMB, турникет PERCo-KT03/600-1;
- Стенд "Пожаро-охранные сигнализации" в составе: Охранное устройство Мираж-GSM-A4-03, ИК извещатель, «стандарт» РАПИД, извещатель радиоволновый Астра-552, комбинированный извещатель Астра-8;
- Климатическая станция Vantage PRO2;
- Приемопередатчики видеосигнала по витой паре на TTP111VLH; видеосервер Domination D7-8-H264;
- Видеорегистратор Videorox DVR VR 3294;
- Стандартная цветная видеокамера под объектив MSC-512S;
- Купольная видеокамера SCW-422;
- Пульт управления камерами SPEED DOME SCJ-200;
- Видео камера сетевая SPEED DOME Beward BD75-5;
- Уличная видеокамера SPEED;

Согласована на портале № 47771

- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

– Microsoft Windows 7 Pro

13.1.3. Материально-техническое и программное обеспечение для лабораторных работ

Лаборатория технической защиты информации

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа

634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 512 ауд.

Описание имеющегося оборудования:

- Компьютер: DEPO Neos DF226/ i3-7100/ DDR4 8G/ Жесткий диск 500G/ мышь/ клавиатура/ монитор;
- Нелинейный локатор NR 900 EM;
- Индикатор поля ST06 SEL SP-77 "Ловец";
- Многофунцкциональный поисковый прибор ST 034;
- Анализатор спектра цифровой GSP-7930;
- Ручной металлодетектор «АКА»;
- Блокиратор сотовых телефонов C-GUARD 300YK;
- Электронно-оптическое устройство "Алмаз";
- Электронно-оптическое устройство "Вега";
- Портативная установка НОРКА-МАКСИ-Д;
- Детектор радиополя D-008;
- RS turboMobile – L;
- Специализированное оборудование по защите информации от утечки по акустическому, акустоэлектрическому каналам, каналу побочных электромагнитных излучений и наводок: Система виброакустической защиты "Соната-АВ" мод. 1М, Пьезоизлучатель ПИ-45, Аудиоизлучатель АИ-65, Система защиты от утечки информации Гром ЗИ-4Б, Блок электропитания и управления «Соната-ИП4.3», Размыкатель телефонной линии «Соната-ВК4.1», Размыкатель слаботочной линии «Соната-ВК4.2», Размыкатель линии Ethernet «Соната-ВК4.3», Средство активной защиты информации от утечки за счет наводок информационного сигнала на цепи заземления и электропитания «Соната-РС3»;

Технические средства контроля эффективности защиты информации от утечки по акустическому каналу, каналу побочных электромагнитных излучений и наводок: Программно-аппаратный комплекс для проведения измерений «СПРУТ 7», Программно-аппаратный измерительный комплекс «Гриф АЭ-1001», ПАК Легенда;

- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

– Kaspersky endpoint security

– Microsoft Windows 10

13.1.4. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 201 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Состав оборудования:

- учебная мебель;
- компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 5 шт.;

Согласована на портале № 47771

- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета.

Перечень программного обеспечения:
- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

13.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися **с нарушениями зрениями** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для комфортного просмотра.

При занятиях с обучающимися **с нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах, мобильной системы обучения для людей с инвалидностью.

14. Оценочные материалы и методические рекомендации по организации изучения дисциплины

14.1. Содержание оценочных материалов и методические рекомендации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы в составе:

14.1.1. Тестовые задания

1. На каком расстоянии от пола должен располагаться излучатель тестового акустического сигнала при проведении акустических измерений разборчивости речи через ограждающие конструкции?
1) 0.5м
2) 1м
3) 1.5м
4) 1.7м

2. На каком расстоянии от ограждающей конструкции должен располагаться микрофон при проведении акустических измерений разборчивости речи через ограждающие конструкции?
1) 0.5м
2) 1м
3) 1.5м
4) 0.7м

3. При превышении какого значения разборчивости речи можно говорить о достижении уровня непреднамеренного прослушивания?
1) 10%
2) 20%
3) 30%
4) 40%

4. Как называется устройство про помощи которого выполняется измерение ограждающих

Согласована на портале № 47771

конструкций при проведении виброакустических измерений разборчивости речи?
1) Акселерометр
2) Микрофон
3) Акустический излучатель
4) Лучевая трубка
5. Устройство, используемое для проведения измерений ТС на побочные электромагнитные излучения (ПЭМИ)?
1) Анализатор спектра
2) Шумомер
3) Низкочастотный анализатор
4) Все варианты
6. Устройства, подлежащие исследованию на побочные электромагнитные излучения и наводки (ПЭМИН)?
1) Накопители на жестких дисках
2) Принтер
3) Клавиатура
4) Все варианты
7. Какая из среднегеометрических частот не входит в стандартные октавные полосы?
1) 250 Гц
2) 1 кГц
3) 500 Гц
4) 750 Гц
8. Создаваемый уровень звукового давления при выступлении человека в аудитории без средств звукоусиления?
1) 100 дБ
2) 70 дБ
3) 84 дБ
4) 50 дБ
9. Что изучается при определение значений сигналов АЭП речевого диапазона частот в отходящей от ВТСС линии, выходящей за пределы КЗ?
1) Телефония
2) Система сигнализации
3) Цепи электропитания
4) Все перечисленное
10. Какие объекты информатизации подлежат обязательной аттестации?
1) Для обработки информации, составляющей государственную тайну
2) Для ведения секретных переговоров
3) Для управления экологически опасными объектами
4) Все перечисленное
11. Мероприятия технического контроля состоят в осуществлении инструментальных проверок эффективности защиты информации от утечки по техническим каналам, возникающим
за счет:
1) Побочных электромагнитных излучений (ПЭМИ) при работе основных технических средств и систем (ОТСС) объекта информатизации
2) Наводок информационного сигнала на соединительных линиях ВТСС, расположенных в зоне действия ПЭМИ ОТСС
3) Неравномерности потребления тока в сети электропитания ОТСС
4) Все варианты
12. Каким методом может осуществляться контроль эффективности мер защиты информации?
1) Инструментальным методом
2) Инструментально-расчетным методом
3) Расчетным методом

Согласована на портале № 47771

4) Все варианты

13. При превышении какого значения разборчивости речи можно говорить о достижении уровня сокрытия факта переговоров?

1) 10%
2) 20%
3) 30%
4) 40%

14. Какой тип информации ограниченного доступа обладает грифом секретности?

1) Государственная тайна
2) Финансовая тайна
3) Конфиденциальная информация
4) Персональные данные

15. Данный тип информации ограниченного доступа содержит информацию конфиденциального характера из любой сферы производственной и управленческой деятельности государственного или частного предприятия

1) Финансовая тайна
2) Промышленная тайна
3) Коммерческая тайна
4) Государственная тайна

16. Самый высокий гриф секретности государственной тайны это

1) Совершенно секретно
2) Секретно
3) Особой важности
4) Для служебного пользования

17. Эта процедура представляет собой изучение технических средств и систем (ТСС) объекта защиты с целью выявления закладных устройств, технических доработок по изменению свойств ТСС

1) Специальная проверка
2) Специальное исследование
3) Специальное обследование
4) Специальный осмотр

18. Какие данные об ТСС должна предоставить организация при проведении специальной проверки?

1) Данные о техническом средстве
2) Сведения о планируемом применении технического средства
3) Данные о месте размещения технического средства
4) Все перечисленное

19. На какой максимальный срок может быть выдан "Аттестат соответствия" объекта информатизации?

1) 2 года
2) 3 года
3) 4 года
4) 5 лет

20. Создаваемый уровень звукового давления при выступлении человека в аудитории со средствами звукоусиления?

1) 100 дБ
2) 70 дБ
3) 84 дБ
4) 50 дБ

14.1.2. Экзаменационные вопросы

1. Дайте определение информации, документированной информации. Каково отличие государственной тайны, конфиденциальной информации и открытой информации.

Согласована на портале № 47771

2. Классификация технической разведки. Эффективность добывания информации технической разведкой.
3. Государственная система защиты информации. Эффективность защиты информации.
4. Основные объекты защиты информации.
5. Дайте определение демаскирующих признаков. Для чего они используются. Приведите примеры.
6. Дайте определение терминам Контролируемая зона, Опасная зона, Опасная зона 1, Опасная зона 2.
7. Состав технического канала утечки информации.
8. Классификация технических каналов утечки информации.
9. Перечислите технические каналы утечки информации, обрабатываемой ОТСС. Приведите примеры.
10. Перечислите технические каналы утечки информации при передаче по каналам связи. Приведите примеры.
11. Перечислите каналы утечки речевой информации. Приведите примеры.
12. Перечислите каналы утечки видовой информации. Приведите примеры.
13. Каково влияние паразитных емкостных, индуктивных и резистивных связей в каналах связи.
14. Перечислите методы противодействия утечке информации по техническим каналам.
15. Способы скрытого видеонаблюдения. Характеристики оборудования для скрытого видеонаблюдения.
16. Способы скрытого прослушивания переговоров в помещении. Демаскирующие признаки радиозакладок. Демаскирующие признаки проводных закладок.
17. Способы прослушивания переговоров по телефонным линиям. Демаскирующие признаки акустических закладок типа «телефонное ухо».
18. Направленные микрофоны. Принцип действия.
19. Охранные системы. Назначение. Структура. Приведите примеры охранных систем объектов и помещений.
20. Датчики охранных систем. Принципы действия датчиков.
21. Охранное видеонаблюдение. Назначение. Структура. Основные характеристики.
22. Средства радиотехнической разведки. Состав. Характеристики.
23. Охрана объектов. Особенности охраны объектов различного класса. Задачи средств охраны объектов.
24. Периметровые средства охраны. Датчики периметровых систем охраны.
25. Охрана выделенных (защищаемых) помещений. Технические средства охраны помещений.
26. Экранирование электромагнитных волн.
27. Экранирование акустических сигналов.
28. Фильтрация опасных сигналов. Приведите примеры.
29. Маскировка опасных сигналов зашумлением. Приведите примеры.
30. Металлодетекторы. Сферы применения. Принцип действия.
31. Локаторы нелинейностей. Сферы применения. Принцип действия.
32. Аттестация объектов информатизации по требованиям безопасности. Назначение. Порядок проведения аттестации.
33. Специальная проверка. Специальное обследование. Специальное исследование.
34. Проведение измерений акустических и виброакустических характеристик. Приведите примеры.
35. Проведение измерений побочных электромагнитных излучений. Приведите примеры.

14.1.3. Темы опросов на занятиях

Характеристика инженерно-технической защиты информации. Технические средства и методы защиты информации. Основные проблемы и параметры инженерно-технической защиты информации. Представление методов и средств защиты информации как системы. Показатели

Согласована на портале № 47771

эффективности инженерно-технической защиты информации.

Цели и задачи защиты информации. Ресурсы, выделяемые на защиту информации.

Основные направления инженерно-технической защиты информации. Принципы защиты информации техническими средствами.

Информация как предмет защиты. Особенности информации как предмета защиты.

Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения и сигналов. Понятие о текущей и эталонной признаковой структуре.

Источники опасных сигналов. Понятие об опасном сигнале. Опасные сигналы и их источники. Основные и вспомогательные технические средства и системы как источники опасных сигналов. Состав и характеристика основных и вспомогательных технических средств и систем.

Побочные электромагнитные излучения и наводки. Виды побочных опасных электромагнитных излучений. Случайные антенны. Виды опасных сигналов на объектах информатизации.

Характеристика технической разведки. Основные задачи и органы технической разведки.

Принципы технической разведки. Основные этапы и процедуры добывания информации технической разведкой. Классификация технической разведки по видам носителя информации и средств разведки. Возможности видов технической разведки. Основные направления развития технической разведки.

Технические каналы утечки информации. Понятие и особенности утечки информации.

Структура, классификация и основные характеристики технических каналов утечки информации.

Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их возможности.

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

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.

Физические основы побочных электромагнитных излучений и наводок.

Акустоэлектрические преобразования. Источники побочных излучений, их физическая природа.

Характер электромагнитных излучений в ближней и дальней зонах. Виды паразитных связей и наводок. Паразитная генерация радиоэлектронных средств. Физические явления, вызывающие утечку информации по цепям электропитания, заземления и токопроводящим конструкциям здания.

Распространение сигналов в технических каналах утечки информации. Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях. Распространение оптических сигналов в атмосфере и в

Согласована на портале № 47771

световодах.

Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи. Основные показатели среды распространения сигналов различных технических каналов утечки информации.

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

Средства технической разведки. Визуально-оптические приборы. Фотоаппараты.

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

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

Средства предотвращения утечки информации по техническим каналам. Средства маскировки и дезинформирования в оптическом и радиодиапазонах. Скрытие речевой информации в каналах связи. Энергетическое скрытие акустических информативных сигналов.

Средства звукоизоляции из звукопоглощения. Обнаружение и локализация закладных устройств, подавление их сигналов. Подавление опасных сигналов акустоэлектрических преобразователей, экранирование и компенсация информативных полей. Подавление информативных сигналов в цепях заземления и электропитания. Подавление опасных сигналов. Генераторы линейного и пространственного зашумления.

Государственная система защиты информации. Характеристика государственной системы противодействия технической разведке. Нормативные документы по противодействию технической разведке. Основные организационные и технические меры по защите информации.

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

Контроль эффективности инженерно-технической защиты информации. Виды контроля эффективности защиты информации. Основные положения методологии инженерно-технической защиты информации. Требования по защите информации от утечки по техническим каналам.

Методы расчета и инструментального контроля показателей защиты информации. Особенности инструментального контроля эффективности инженерно-технической защиты информации.

Согласована на портале № 47771

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

Принципы оценки эффективности инженерно-технической защиты информации. Принципы оценки эффективности охраны объектов защиты. Возможности оценки видовых признаков объектов наблюдения. Подходы к определению безопасности речевой информации в защищаемых помещениях. Принципы оценки размеров опасных зон I и II.

14.1.4. Темы лабораторных работ

Статистический анализ загрузки заданного радиодиапазона и обнаружение радио-закладных устройств в охраняемом помещении.

Нелинейная локация.

Обнаружение активных прослушивающих устройств с помощью индикатора электромагнитного поля

14.2. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 14.

Таблица 14 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами исходя из состояния обучающегося на момент проверки

14.3. Методические рекомендации по оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной форме;
- в печатной форме с увеличенным шрифтом;
- в форме электронного документа;
- методом чтения ассистентом задания вслух;
- предоставление задания с использованием сурдоперевода.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

Согласована на портале № 47771

– письменно на бумаге;
– набор ответов на компьютере;
– набор ответов с использованием услуг ассистента;
– представление ответов устно.

Процедура оценивания результатов обучения лиц с ограниченными возможностями здоровья и инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:
– в форме электронного документа;
– в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:
– в форме электронного документа;
– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:
– в форме электронного документа;
– в печатной форме.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.

Согласована на портале № 47771