МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ 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

Инженерно-техническая защита информации

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **11.05.01 Радиоэлектронные системы и комплексы**
Направленность (профиль) / специализация: **Радиоэлектронные системы передачи информации**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РТС, Кафедра радиотехнических систем**
Курс: **5**
Семестр: **10**
Учебный план набора 2013 года

Распределение рабочего времени

№	Виды учебной деятельности	10 семестр	Всего	Единицы
1	Лекции	32	32	часов
2	Практические занятия	16	16	часов
3	Лабораторные работы	16	16	часов
4	Всего аудиторных занятий	64	64	часов
5	Самостоятельная работа	44	44	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: 10 семестр

Томск 2018

Согласована на портале № 35938

Рассмотрена и одобрена на заседании кафедры
протокол № 12 от « 4 » 7 2018 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 11.05.01 Радиоэлектронные системы и комплексы, утвержденного 11.08.2016 года, рассмотрена и одобрена на заседании кафедры РТС «___» _____ 20__ года, протокол №_____.

Разработчик:

доцент каф. РТС	_____	Б. В. Илюхин
Заведующий обеспечивающей каф. РТС	_____	С. В. Мелихов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан РТФ	_____	К. Ю. Попова
Заведующий выпускающей каф. РТС	_____	С. В. Мелихов

Эксперты:

Старший преподаватель кафедры радиотехнических систем (РТС)	_____	Д. О. Ноздреватых
Доцент кафедры радиотехнических систем (РТС)	_____	В. А. Громов

Согласована на портале № 35938

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.

1.2. Задачи дисциплины

– Задачами изучения дисциплины являются:

– -ознакомление с основными принципами построения технических средств защиты информации, современными тенденциями их развития;

– - получение теоретических знаний и практических навыков в области построения технических средств защиты информации.

2. Место дисциплины в структуре ОПОП

Дисциплина «Инженерно-техническая защита информации» (Б1.Б.31.9) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Защита интеллектуальной собственности, Защита информации в инфокоммуникационных системах и сетях, Каналы передачи информации, Кодирование и шифрование информации в системах связи, Компьютерное проектирование и моделирование систем связи, Системы радиосвязи, Тестирование и диагностика в инфокоммуникационных системах и сетях, Цифровая обработка сигналов.

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:

– ПСК-2.3 способностью проводить оптимизацию радиосистем передачи информации и отдельных ее подсистем;

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 таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		10 семестр
Аудиторные занятия (всего)	64	64
Лекции	32	32
Практические занятия	16	16
Лабораторные работы	16	16
Самостоятельная работа (всего)	44	44
Оформление отчетов по лабораторным работам	16	16

Согласована на портале № 35938

Проработка лекционного материала	18	18
Подготовка к практическим занятиям, семинарам	10	10
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
10 семестр						
1 Концепция инженерно-технической защиты информации	4	0	0	3	7	ПСК-2.3
2 Теоретические основы инженерно-технической защиты информации	8	0	0	4	12	ПСК-2.3
3 Физические основы защиты информации	8	16	0	14	38	ПСК-2.3
4 Технические средства добывания и инженерно-технической защиты информации	8	0	16	19	43	ПСК-2.3
5 Организационные основы инженерно-технической защиты информации	2	0	0	2	4	ПСК-2.3
6 Методическое обеспечение инженерно-технической защиты информации	2	0	0	2	4	ПСК-2.3
Итого за семестр	32	16	16	44	108	
Итого	32	16	16	44	108	

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
10 семестр			
1 Концепция инженерно-технической	Характеристика инженерно-технической защиты информации. Технические средства и методы за-	2	ПСК-2.3

Согласована на портале № 35938

защиты информации	щиты информации. Основные проблемы и параметры инженерно-технической защиты информации. Представление методов и средств защиты информации как системы. Показатели 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.	2	
	Итого	4	
2 Теоретические основы инженерно-технической 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.Побочные электромагнитные излучения и наводки. Виды побочных опасных электромагнитных излучений. Случайные антенны. Виды опасных сигналов на объектах информатизации.	2	ПСК-2.3
	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.	2	
	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.	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 зашум-	2	

Согласована на портале № 35938

	ления сигналов.		
	Итого	8	
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	ПСК-2.3
	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.	2	
	Распространение радиосигналов различных диапазонов в пространстве и по направляющим линиям связи. Основные показатели среды распространения сигналов различных технических каналов утечки информации.	2	
	Физические процессы подавления 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	8	
4 Технические средства добывания и инженерно-технической 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 лазерного подслушивания. Автономные средства разведки.	2	ПСК-2.3
	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.	4	

Согласована на портале № 35938

	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.	2	
	Итого	8	
5 Организационные основы инженерно-технической 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	ПСК-2.3
	Итого	2	
6 Методическое обеспечение инженерно-технической защиты информации	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	2	ПСК-2.3

Согласована на портале № 35938

	оценки размеров опасных зон I и II.		
	Итого	2	
Итого за семестр		32	

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 Защита интеллектуальной собственности	+		+		+	+
2 Защита информации в инфокоммуникационных системах и сетях	+	+		+		
3 Каналы передачи информации				+		
4 Кодирование и шифрование информации в системах связи				+		
5 Компьютерное проектирование и моделирование систем связи			+	+	+	
6 Системы радиосвязи		+	+			
7 Тестирование и диагностика в инфокоммуникационных системах и сетях	+		+	+		
8 Цифровая обработка сигналов				+		
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.	
ПСК-2.3	+	+	+	+	Домашнее задание, Защита отчета, Опрос на занятиях, Тест

Согласована на портале № 35938

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
10 семестр			
4 Технические средства добывания и инженерно-технической защиты информации	Статистический анализ загрузки заданного радио-диапазона и обнаружение радио-закладных устройств в охраняемом помещении.	4	ПСК-2.3
	Охрана выделенных помещений. Охранная сигнализация.	4	
	Ограничение доступа в выделенное помещение. Система контроля и управления доступом.	4	
	Охрана выделенных помещений. Система видеонаблюдения.	4	
	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
10 семестр			
3 Физические основы защиты информации	Моделирование систем нелинейной локации	4	ПСК-2.3
	Организационные мероприятия по подготовке и проведению аттестации объектов информатизации по требованиям безопасности	6	
	Методическое обеспечение проведения аттестации объектов информатизации по требованиям безопасности. Расчёт размеров опасных зон I и II	6	
	Итого	16	
Итого за семестр		16	

9. Самостоятельная работа

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

Согласована на портале № 35938

Таблица 9.1 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
10 семестр				
1 Концепция инженерно-технической защиты информации	Проработка лекционного материала	2	ПСК-2.3	Опрос на занятиях
	Проработка лекционного материала	1		
	Итого	3		
2 Теоретические основы инженерно-технической защиты информации	Проработка лекционного материала	1	ПСК-2.3	Опрос на занятиях
	Проработка лекционного материала	1		
	Проработка лекционного материала	1		
	Проработка лекционного материала	1		
	Итого	4		
3 Физические основы защиты информации	Подготовка к практическим занятиям, семинарам	4	ПСК-2.3	Домашнее задание, Опрос на занятиях, Тест
	Подготовка к практическим занятиям, семинарам	4		
	Подготовка к практическим занятиям, семинарам	2		
	Проработка лекционного материала	1		
	Проработка лекционного материала	1		
	Проработка лекционного материала	1		
	Проработка лекционного материала	1		
	Итого	14		
4 Технические средства добывания и инженерно-технической защиты информации	Проработка лекционного материала	1	ПСК-2.3	Защита отчета, Опрос на занятиях, Тест
	Проработка лекционного материала	1		
	Проработка лекционного материала	1		

Согласована на портале № 35938

	Оформление отчетов по лабораторным работам	4		
	Оформление отчетов по лабораторным работам	4		
	Оформление отчетов по лабораторным работам	4		
	Оформление отчетов по лабораторным работам	4		
	Итого	19		
5 Организационные основы инженерно-технической защиты информации	Проработка лекционного материала	2	ПСК-2.3	Опрос на занятиях
	Итого	2		
6 Методическое обеспечение инженерно-технической защиты информации	Проработка лекционного материала	2	ПСК-2.3	Опрос на занятиях
	Итого	2		
Итого за семестр		44		
	Подготовка и сдача экзамена	36		Экзамен
Итого		80		

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
10 семестр				
Домашнее задание	10	8	8	26
Защита отчета	8	12	8	28
Опрос на занятиях	6	5	5	16
Итого максимум за период	24	25	21	70
Экзамен				30
Нарастающим итогом	24	49	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

Согласована на портале № 35938

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)

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Защита информации от утечки по техническим каналам [Электронный ресурс]: Учебное пособие / Голиков А. М. - 2015. 256 с. - Режим доступа: http://edu.tusur.ru/publications/5263 (дата обращения: 08.07.2018).

2. Защита информации в инфокоммуникационных системах и сетях [Электронный ресурс]: Учебное пособие / Голиков А. М. - 2015. 284 с. - Режим доступа: http://edu.tusur.ru/publications/5262 (дата обращения: 08.07.2018).

12.2. Дополнительная литература

1. Основы защиты информации : Учебное пособие: В 3 ч. Ч. 1 / Министерство образования и науки Российской Федерации, Томский государственный университет систем управления и радиоэлектроники, Центр технологий безопасности ; сост. : А. А. Шелупанов [и др.]. - 3-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 150[2] с. : ил. (наличие в библиотеке ТУСУР - 81 экз.)

2. Основы защиты информации : Учебное пособие: В 3 ч. Ч. 2 / Министерство образования и науки Российской Федерации, Томский государственный университет систем управления и радиоэлектроники, Центр технологий безопасности ; сост. : А. А. Шелупанов [и др.]. - 3-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 185[1] с. : ил. (наличие в библиотеке ТУСУР - 81 экз.)

3. Основы защиты информации : Учебное пособие: В 3 ч. Ч. 3 / Министерство образования и науки Российской Федерации, Томский государственный университет систем управления и радиоэлектроники, Центр технологий безопасности ; сост. : А. А. Шелупанов [и др.]. - 3-е изд., перераб. и доп. - Томск : В-Спектр, 2007. - 98[2] с. : ил., табл. (наличие в библиотеке ТУСУР - 81 экз.)

4. Защита и охрана личности, собственности, информации : Справочное пособие / Алексей Васильевич Петраков. - М. : Радио и связь, 1997. - 320 с. : ил. (наличие в библиотеке ТУСУР - 11 экз.)

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Технические средства и методы защиты информации : Лабораторный практикум: Учебное пособие / А. П. Зайцев, А. А. Шелупанов ; Федеральное агентство по образованию, Томский государственный университет систем управления и радиоэлектроники, Кафедра комплексной информационной безопасности электронно-вычислительных систем. - 2-е изд., испр. и доп. - Томск :

Согласована на портале № 35938

В-Спектр, 2007. - 119[1] с. : ил. (наличие в библиотеке ТУСУР - 61 экз.)

2. Самостоятельная работа студента при изучении дисциплин математическо-естественно-научного, общепрофессионального (профессионального), специального циклов [Электронный ресурс]: Учебно-методическое пособие по самостоятельной работе / Кологривов В. А., Мелихов С. В. - 2012. 9 с. - Режим доступа: http://edu.tusur.ru/publications/1845 (дата обращения: 08.07.2018).

3. Защита информации в инфокоммуникационных системых и сетях [Электронный ресурс]: Учебное пособие для практических и семинарских занятий (Часть 1) / Голиков А. М. - 2015. 103 с. - Режим доступа: http://edu.tusur.ru/publications/5330 (дата обращения: 08.07.2018).

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.

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.biblioclub.ru – полнотекстовая электронная библиотека;
3. http://www.elibrary.ru – научная электронная библиотека;
4. http://www.edu.ru – веб-сайт системы федеральных образовательных порталов.
5. При изучении дисциплины рекомендуется обращаться к базам данных, информационно-справочным и поисковым системам, к которым у ТУСУРа открыт доступ: https://lib.tusur.ru/ru/resursy/bazy-dannyh

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 радиоэлектронных систем передачи информации

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа, помещение для курсового проектирования (выполнения курсовых работ)

634034, Томская область, г. Томск, Вершинина улица, д. 47, 401 ауд.

Описание имеющегося оборудования:

- Компьютер (8 шт.);
- Монитор (19” SAMSUNG 1730S) (8 шт.);
- Клавиатура (8 шт.);

Согласована на портале № 35938

- Мышь (оптическая) (8 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

– Microsoft Windows XP
– OpenOffice
– Opera

Лаборатория радиоэлектронных систем передачи информации

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа, помещение для курсового проектирования (выполнения курсовых работ)

634034, Томская область, г. Томск, Вершинина улица, д. 47, 401 ауд.

Описание имеющегося оборудования:

- Компьютер (8 шт.);
- Монитор (19” SAMSUNG 1730S) (8 шт.);
- Клавиатура (8 шт.);
- Мышь (оптическая) (8 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

– Google Chrome
– Microsoft Windows XP
– OpenOffice
– Opera

13.1.3. Материально-техническое и программное обеспечение для лабораторных работ

Лаборатория радиоэлектронных систем передачи информации

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа, помещение для курсового проектирования (выполнения курсовых работ)

634034, Томская область, г. Томск, Вершинина улица, д. 47, 401 ауд.

Описание имеющегося оборудования:

- Компьютер (8 шт.);
- Монитор (19” SAMSUNG 1730S) (8 шт.);
- Клавиатура (8 шт.);
- Мышь (оптическая) (8 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

– Google Chrome
– Microsoft Windows XP
– OpenOffice

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:

Согласована на портале № 35938

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

1.1 Основной эффект от создания сети:
a Удобство передачи информации;
b Экономия средств;
c Полная доступность ресурсов сети для пользователей;
d Возможность удаленных вычислений.
1.2 В компьютерных сетях, как правило, относительная стоимость передачи данных за счет совместного использования каналов связи многими абонентами:
a Существенно повышается;
b Не изменяется;
c Существенно снижается;
d Повышается.
1.3 Не существует основного типа сетей:
a Локальных.
b Корпоративных.
c Региональных.
d Глобальных.
1.4 Выбор той или иной топологии не влияет на:
a Состав необходимого сетевого оборудования;

Согласована на портале № 35938

b Вид электрического сигнала;
c Возможности сетевого оборудования;
d Возможности расширения сети;
e Способ управления сетью;
1.5 В сети с топологией «шина»:
a Передача ведется всеми компьютерами одновременно;
b Прием ведется всеми компьютерами одновременно;
c Электрический сигнал принимает только компьютер – получатель;
d Одновременно передавать сигнал могут не более двух компьютеров.
1.6 Выбор той или иной топологии не влияет на:
a Выбор периферийных устройств для подключения к сети;
b Выбор типа кабеля;
c Скорость работы сети;
d Выбор сетевой ОС.
1.7 Производительность сети это:
a Среднестатистическое время доставки сообщения адресату.
b Суммарная производительность главных компьютеров.
c Средняя пропускная способность сети.
d Скорость вычислений в сети.
1.8 Единица информации, передаваемая между устройствами сети как единое целое:
a Сеанс;
b Байт;
c Пакет;
d Бит.
1.9 Сеть можно представить как совокупность систем, связанных между собой:
a Линиями связи;
b Логически;
c Некоторой передающей средой;
d Физически.
1.10 Зачем нужна преамбула в пакетах Ethernet?
a Туда записывается характеристика последующего пакета;
b Служит для синхронизации приемника;
c Позволяет выделить начало пакета;
d Служит для прерывания приема в случае, когда не зарегистрирован конец предшествующего пакета.
1.11 Можно ли построить фрагмент сети Ethernet, в котором не будет столкновений?
a Невозможно.
b Сейчас трудно из-за ограничений современных технологий.
c Можно.
d Это зависит от версии используемого протокола.
1.12 Работа протоколов должна быть скоординирована так, чтобы:
a Исключить конфликты или незаконченные операции;
b Обеспечить наибольшую скорость передачи;
c Повысить надежность передачи;
d Исключить коллизии.
1.13 стандартом де-факто для межсетевого взаимодействия является:
a набор протоколов OSI;
b стек протоколов TCP/IP;
c NetBEUI;
d стек протоколов TCP.
1.14 Какие уровни описывают правила для проведения сеансов связи и интерпретации приложений:
a Высокие;
b Верхние;

Согласована на портале № 35938

c Средние;

d Нижние.

1.15 TCP/IP — промышленный стандартный набор протоколов, которые обеспечивают связь…

a В параметрической среде;

b В среде с распределенными параметрами;

c В однородной среде;

d В неоднородной среде.

1.16 Протокол UDP – это:

a Протокол, осуществляющий передачу информации от узла к узлу сети в виде дискретных блоков пакетов;

b Протокол управления передачей данных;

c Дейтаграммный протокол передачи данных;

d Протокол, обеспечивающий целостность или сохранение порядка потока пакетов.

1.17 Какого пожелания способа доставки дейтограммы не существует:

a минимального количества маршрутизаторов;

b минимальной задержки;

c высокой пропускной способности;

d высокой надежности.

1.18 Зачем нужна сетевая маска?

a Это нужно для организации подсетей;

b Это необходимо для обеспечения дополнительных мер безопасности;

c Этим достигается уменьшение количества широковещательных пакетов;

d Маска используется при шифровании передаваемых данных.

1.19 С помощью таблицы маршрутизации, управляя передачей пакетов в сегменты, мосты способны:

a Увеличить сетевой трафик;

b Уменьшить сетевой трафик;

c Увеличить пропускную способность канала;

d Уменьшить пропускную способность канала.

1.20 Могут ли маршрутизаторы непосредственно обращаться к удаленным компьютерам?:

a Нет;

b Да;

c Да, если известен адрес сети и локальной платы сетевого адаптера;

d Да, если известен адрес узла сети.

14.1.2. Экзаменационные вопросы

Перечислите нормативно правовые акты, регламентирующие построение технических средств защиты информациии

Перечислите типы устройств защиты от прослушивания помещений

Перечислите технические каналы утечки информации.

Охарактеризуйте методы инженерной защиты и технической охраны объектов

Перечислите методы скрытия информации и ее носителей

Охарактеризуйте физические явления, вызывающие утечку информации по цепям электропитания, заземления и токопроводящим конструкциям здания.

Перечислите виды средств технической разведки

Производительность сети это:

a Среднестатистическое время доставки сообщения адресату.

b Суммарная производительность главных компьютеров.

c Средняя пропускная способность сети.

d Скорость вычислений в сети.

Перечислите основные НПА в области защиты информации

Перечислите основные типы нормативно-правовых актов в области защиты информации

Технические средства охраны это:

Относится ли система пожаротушения к техническим средствам охраны?

Согласована на портале № 35938

Как называется федеральный орган исполнительной власти, регламентирующий вопросы защиты информации?

Что такое модель угроз?

Перечислите основные типы угроз информации

Перечислите основные способы физической защиты информации

Перечислите основные средства предотвращения утечки информации по техническим каналам.

Перечислите основные средства предотвращения утечки информации по техническим каналам.

Перечислите основные средства маскировки и дезинформирования в оптическом и радиодиапазонах.

Перечислите основные средства маскировки и дезинформирования в оптическом и радиодиапазонах.

Перечислите основные способы обнаружения и локализации закладных устройств, подавление их сигналов.

Перечислите основные способы обнаружения и локализации закладных устройств, подавление их сигналов.

Как осуществляется подавление опасных сигналов акустоэлектрических преобразователей, экранирование и компенсация информативных полей.

Как осуществляется подавление опасных сигналов акустоэлектрических преобразователей, экранирование и компенсация информативных полей.

14.1.3. Темы домашних заданий

Основные этапы и процедуры добывания информации технической разведкой.

Объясните, что такое прозрачность (распределения) и приведите примеры различных видов прозрачности.

Методы и средства инженерной защиты и технической охраны объектов

Нормативные документы по противодействию технической разведке.

14.1.4. 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 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.

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

Согласована на портале № 35938

.

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 световодах.

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

Физические процессы подавления 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.

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 рацио-

Согласована на портале № 35938

нальных 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.

14.1.5. Методические рекомендации

Последующие дисциплины: преддипломная практика, защита ВКР

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:

- 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:

Согласована на портале № 35938

– 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 № 35938