МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

УТВЕРЖДАЮ
Проректор по УР
_____Сенченко П.В.
«22» _____02_____ 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ЗАЩИТА ИНФОРМАЦИИ В РАДИОЭЛЕКТРОННЫХ СИСТЕМАХ

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **11.05.01 Радиоэлектронные системы и комплексы**
Направленность (профиль) / специализация: **Радиоэлектронные системы и комплексы**
Форма обучения: **очная**
Факультет: **Радиотехнический факультет (РТФ)**
Кафедра: **Кафедра радиотехнических систем (РТС)**
Курс: **4**
Семестр: **8**
Учебный план набора 2023 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	8 семестр	Всего	Единицы
Лекционные занятия	22	22	часов
Практические занятия	22	22	часов
Лабораторные занятия	16	16	часов
Самостоятельная работа	48	48	часов
Подготовка и сдача экзамена	36	36	часов
Общая трудоемкость (включая промежуточную аттестацию)	144	144	часов
	4	4	з.е.

Формы промежуточной аттестация	Семестр
Экзамен	8

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сенченко П.В.
Должность: Проректор по УР
Дата подписания: 22.02.2023
Уникальный программный ключ:
a1119608-cdff-4455-b54e-5235117c185c

Томск

Согласована на портале № 69953

1. Общие положения

1.1. Цели дисциплины

1. Целью преподавания дисциплины является изучение методов защиты и основных закономерностей передачи информации в цифровых теле- коммуникационных системах.

1.2. Задачи дисциплины

1. Задачей дисциплины является формирование у студентов компетенций, позволяющих самостоятельно проводить математический анализ физических процессов в аналоговых и цифровых устройствах формирования, преобразования и обработки сигналов, оценивать реальные и предельные возможности пропускной способности и помехоустойчивости телекоммуникационных систем и сетей.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).
Часть блока дисциплин: Часть, формируемая участниками образовательных отношений.
Модуль дисциплин: Модуль специализации (major).
Индекс дисциплины: Б1.В.02.09.
Реализуется с применением электронного обучения, дистанционных образовательных технологий.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 3.1):
Таблица 3.1 – Компетенции и индикаторы их достижения

Компетенция	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
Универсальные компетенции		
-	-	-
Общепрофессиональные компетенции		
-	-	-
Профессиональные компетенции		
ПК-7. Способен решать задачи оптимизации существующих и новых технических решений в условиях априорной неопределенности с применением пакетов прикладных программ	ПК-7.1. Знает методы оптимизации существующих и новых технических решений в условиях априорной неопределенности	Знает методы оптимизации существующих и новых технических решений в условиях априорной неопределенности в области защиты информации
	ПК-7.2. Умеет применять современный математический аппарат для решения задачи оптимизации	Умеет применять современный математический аппарат для решения задачи оптимизации в области защиты информации
	ПК-7.3. Владеет методами оптимизации проектируемых радиоэлектронных систем и комплексов	Владеет методами оптимизации проектируемых радиоэлектронных систем и комплексов в области защиты информации

4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем и на самостоятельную работу обучающихся

Согласована на портале № 69953

Общая трудоемкость дисциплины составляет 4 зачетных единиц, 144 академических часов.

Распределение трудоемкости дисциплины по видам учебной деятельности представлено в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины по видам учебной деятельности

Виды учебной деятельности	Всего часов	Семестры
		8 семестр
Контактная аудиторная работа обучающихся с преподавателем, всего	60	60
Лекционные занятия	22	22
Практические занятия	22	22
Лабораторные занятия	16	16
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	48	48
Написание отчета по практическому занятию (семинару)	12	12
Выполнение практического задания	13	13
Подготовка к тестированию	12	12
Подготовка к лабораторной работе, написание отчета	5	5
Написание отчета по лабораторной работе	6	6
Подготовка и сдача экзамена	36	36
Общая трудоемкость (в часах)	144	144
Общая трудоемкость (в з.е.)	4	4

5. Структура и содержание дисциплины

5.1. Разделы (темы) дисциплины и виды учебной деятельности

Структура дисциплины по разделам (темам) и видам учебной деятельности приведена в таблице 5.1.

Таблица 5.1 – Разделы (темы) дисциплины и виды учебной деятельности

Названия разделов (тем) дисциплины	Лек. зан., ч	Прак. зан., ч	Лаб. раб.	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
8 семестр						
1 Предмет курса. Информационная безопасность в системе национальной безопасности Российской Федерации	2	-	-	6	8	ПК-7
2 Основные понятия теории информационной безопасности. Анализ угроз информационной безопасности	2	4	-	6	12	ПК-7
3 Методы и средства обеспечения информационной безопасности в радиоэлектронных системах передачи информации	4	6	8	6	24	ПК-7
4 Основы комплексного обеспечения информационной безопасности в радиоэлектронных системах передачи	4	4	4	10	22	ПК-7
5 Стандарты информационной безопасности, критерии и классы оценки защищенности	4	4	-	6	14	ПК-7
6 Методология построения и анализа систем обеспечения информационной безопасности	4	-	-	6	10	ПК-7

Согласована на портале № 69953

7 Технические каналы утечки информации в радиоэлектронных системах передачи	2	4	4	8	18	ПК-7
Итого за семестр	22	22	16	48	108	
Итого	22	22	16	48	108	

5.2. Содержание разделов (тем) дисциплины

Содержание разделов (тем) дисциплины (в т.ч. по лекциям) приведено в таблице 5.2.
Таблица 5.2 – Содержание разделов (тем) дисциплины (в т.ч. по лекциям)

Названия разделов (тем) дисциплины	Содержание разделов (тем) дисциплины (в т.ч. по лекциям)	Трудоемкость (лекционные занятия), ч	Формируемые компетенции
8 семестр			
1 Предмет курса. Информационная безопасность в системе национальной безопасности Российской Федерации	Цели и задачи курса. Предмет, структура и краткое содержание курса. История возникновения и развития систем защиты информации. Понятие национальной безопасности. Виды безопасности личности, общества и государства: экономическая, внутриполитическая, социальная, международная, информационная, военная, пограничная, экологическая и другие. Виды защищаемой информации. Основные понятия и общеметодологические принципы теории информационной безопасности. Роль информационной безопасности в обеспечении национальной безопасности государства. Обеспечение информационной безопасности в нормальных и чрезвычайных ситуациях. Основные правовые и нормативные акты в области информационной безопасности. Методические указания по изучению курса. Рекомендуемая основная и дополнительная литература.	2	ПК-7
	Итого	2	

Согласована на портале № 69953

2 Основные понятия теории информационной безопасности. Анализ угроз информационной безопасности	Основные понятия теории компьютерной безопасности. Понятие информации, ин формационной безопасности АС. Субъектно-объектная модель информационной системы. Основные определения. Язык. Объекты. Субъекты. Доступ. Информационный поток. Монитор безопасности. Ядро безопасности. Иерархические моде ли вычислительных систем и модель взаимодействия открытых систем (OSI/ISO). Ценность информации. Аддитивная модель. Порядковая шкала. Решетка ценности. Анализ угроз информационной безопасности. Угрозы конфиденциальности, целостности, доступности информации, раскрытия параметров информационной системы. Структура теории компьютерной безопасности. Основные уровни защиты информации. Защита машинных носителей информации (МНИ). Защита средств взаимодействия с МНИ. Защита представления информации. Защита содержания информации. Основные виды атак на информационные АС. Классификация основных атак и вредоносных программ.	2	ПК-7
	Итого	2	

Согласована на портале № 69953

3 Методы и средства обеспечения информационной безопасности в радиоэлектронных системах передачи информации	Построение систем защиты от угрозы нарушения конфиденциальности информации. Организационно режимные меры. Защита от несанкционированного доступа (НСД). Построение парольных систем. Криптографические методы защиты. Защита от угрозы нарушения конфиденциальности на уровне содержания информации. Построение систем защиты от угрозы нарушения целостности информации. Организационно-технологические меры защиты. Защита целостности программно-аппаратной среды. Основные методы защиты памяти. Цифровая подпись. Защита от угрозы целостности на уровне содержания информации. Построение системы защиты от угрозы доступности информации. Эксплутационно-технологические меры защиты. Защита от сбоев программно-аппаратной среды. Защита семантического анализа и актуальности информации.Построение системы защиты от угрозы раскрытия параметров информационной системы. Сокрытие характеристик носителей. Мониторинг использования систем защиты. Защита параметров представления и содержания информации.	4	ПК-7
	Итого	4	
4 Основы комплексного обеспечения информационной безопасности в радиоэлектронных системах передачи	Понятие политики безопасности. Политика (стратегия) безопасности. Дискреционная политика разграничения доступа. Мандатная (полномочная) политика разграничения доступа. Разработка и реализация политики безопасности. Модели безопасности. Описание систем защиты с помощью матрицы доступа. Модель Харрисона-Руззо-Ульмана (HRU). Разрешимость проблемы безопасности. Модель распространения прав доступа Take-Grant. Расширенная модель Take-Grant, анализ информационных каналов. Описание модели Белла-Лападулы (BL). Основная теорема безопасности модели Белла-Лападулы. Эквивалентные подходы к определению безопасности модели Белла-Лападулы. Решетка мандатных моделей. Ролевая политика безопасности.	4	ПК-7
	Итого	4	

Согласована на портале № 69953

5 Стандарты информационной безопасности, критерии и классы оценки защищенности	Основные критерии защищенности информационных автоматизированных систем (АС). Классы защищенности АС. Критерии и классы защищенности средств вычислительной техники (СВТ) и АС. Стандарты по оценки защищенности АС. Стандарт оценки безопасности компьютерных систем TCSEC («Оранжевая книга»). Основные требования к системам защиты в TCSEC. Классы защиты TCSEC. Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ. Классификация СВТ по документам Гостехкомиссии. Классификация АС по документам Гостехкомиссии, требования классов защиты. Единые критерии безопасности информационных технологий (Common Criteria). Основные положения «Единых критериев». Требования безопасности. Профили защиты.	4	ПК-7
	Итого	4	
6 Методология построения и анализа систем обеспечения информационной безопасности	Применение иерархического метода для построения защищенной АС. Исследование корректности реализации и методы верификации АС. Теория безопасных систем (ТСВ). Информационные АС и программные средства, сертифицированные в соответствии с требованиями «Оранжевой книги». Проблемы компьютерной безопасности. Перспективные направления исследований в области компьютерной безопасности. Центры компьютерной безопасности. Рекомендации по самостоятельному углубленному изучению разделов курса.	4	ПК-7
	Итого	4	
7 Технические каналы утечки информации в радиоэлектронных системах передачи	Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Простые и составные технические каналы утечки информации. Характеристика и возможности оптических, акустических, радиоэлектронных и материально-вещественных каналов утечки информации.	2	ПК-7
	Итого	2	
Итого за семестр		22	
Итого		22	

5.3. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 5.3.
Таблица 5.3. – Наименование практических занятий (семинаров)

Согласована на портале № 69953

Названия разделов (тем) дисциплины	Наименование практических занятий (семинаров)	Трудоемкость, ч	Формируемые компетенции
8 семестр			
2 Основные понятия теории информационной безопасности. Анализ угроз информационной безопасности	Стандарты информационной безопасности и критерии оценки безопасности систем и сетей передачи информации	4	ПК-7
	Итого	4	
3 Методы и средства обеспечения информационной безопасности в радиоэлектронных системах передачи информации	Разработка архитектуры модели безопасности информационных систем и сетей	6	ПК-7
	Итого	6	
4 Основы комплексного обеспечения информационной безопасности в радиоэлектронных системах передачи	Разработка практических рекомендаций по обеспечению безопасности информационных систем	4	ПК-7
	Итого	4	
5 Стандарты информационной безопасности, критерии и классы оценки защищенности	Законодательство в области информационной безопасности	4	ПК-7
	Итого	4	
7 Технические каналы утечки информации в радиоэлектронных системах передачи	Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Простые и составные технические каналы утечки информации. Характеристика и возможности оптических, акустических, радиоэлектронных и материально-вещественных каналов утечки информации.	4	ПК-7
	Итого	4	
Итого за семестр		22	
Итого		22	

5.4. Лабораторные занятия

Наименование лабораторных работ приведено в таблице 5.4.

Таблица 5.4 – Наименование лабораторных работ

Названия разделов (тем) дисциплины	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
8 семестр			

Согласована на портале № 69953

3 Методы и средства обеспечения информационной безопасности в радиоэлектронных системах передачи информации	Изучение международного стандарта безопасности информационных систем ISO. Исследование системы защиты информации «Страж NT». Система защиты информации SecretNet. Система защиты информации Dallas	8	ПК-7
	Итого	8	
4 Основы комплексного обеспечения информационной безопасности в радиоэлектронных системах передачи	Система анализа рисков и проверки политики информационной безопасности предприятия	4	ПК-7
	Итого	4	
7 Технические каналы утечки информации в радиоэлектронных системах передачи	Энергетическое скрытие речевой информации. Скремблеры.	4	ПК-7
	Итого	4	
Итого за семестр		16	
Итого		16	

5.5. Курсовой проект / курсовая работа

Не предусмотрено учебным планом

5.6. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 5.6.

Таблица 5.6. – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов (тем) дисциплины	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
8 семестр				
1 Предмет курса. Информационная безопасность в системе национальной безопасности Российской Федерации	Написание отчета по практическому занятию (семинару)	2	ПК-7	Отчет по практическому занятию (семинару)
	Выполнение практического задания	2	ПК-7	Практическое задание
	Подготовка к тестированию	2	ПК-7	Тестирование
	Итого	6		
2 Основные понятия теории информационной безопасности. Анализ угроз информационной безопасности	Написание отчета по практическому занятию (семинару)	2	ПК-7	Отчет по практическому занятию (семинару)
	Выполнение практического задания	2	ПК-7	Практическое задание
	Подготовка к тестированию	2	ПК-7	Тестирование
	Итого	6		

Согласована на портале № 69953

3 Методы и средства обеспечения информационной безопасности в радиоэлектронных системах передачи информации	Написание отчета по практическому занятию (семинару)	1	ПК-7	Отчет по практическому занятию (семинару)
	Выполнение практического задания	1	ПК-7	Практическое задание
	Подготовка к тестированию	1	ПК-7	Тестирование
	Подготовка к лабораторной работе, написание отчета	1	ПК-7	Лабораторная работа
	Написание отчета по лабораторной работе	2	ПК-7	Отчет по лабораторной работе
	Итого	6		
4 Основы комплексного обеспечения информационной безопасности в радиоэлектронных системах передачи	Написание отчета по практическому занятию (семинару)	2	ПК-7	Отчет по практическому занятию (семинару)
	Выполнение практического задания	2	ПК-7	Практическое задание
	Подготовка к тестированию	2	ПК-7	Тестирование
	Подготовка к лабораторной работе, написание отчета	2	ПК-7	Лабораторная работа
	Написание отчета по лабораторной работе	2	ПК-7	Отчет по лабораторной работе
	Итого	10		
5 Стандарты информационной безопасности, критерии и классы оценки защищенности	Написание отчета по практическому занятию (семинару)	2	ПК-7	Отчет по практическому занятию (семинару)
	Выполнение практического задания	2	ПК-7	Практическое задание
	Подготовка к тестированию	2	ПК-7	Тестирование
	Итого	6		
6 Методология построения и анализа систем обеспечения информационной безопасности	Написание отчета по практическому занятию (семинару)	2	ПК-7	Отчет по практическому занятию (семинару)
	Выполнение практического задания	2	ПК-7	Практическое задание
	Подготовка к тестированию	2	ПК-7	Тестирование
	Итого	6		

Согласована на портале № 69953

7 Технические каналы утечки информации в радиоэлектронных системах передачи	Написание отчета по практическому занятию (семинару)	1	ПК-7	Отчет по практическому занятию (семинару)
	Выполнение практического задания	2	ПК-7	Практическое задание
	Подготовка к тестированию	1	ПК-7	Тестирование
	Подготовка к лабораторной работе, написание отчета	2	ПК-7	Лабораторная работа
	Написание отчета по лабораторной работе	2	ПК-7	Отчет по лабораторной работе
	Итого	8		
Итого за семестр		48		
	Подготовка и сдача экзамена	36		Экзамен
Итого		84		

5.7. Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности

Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности представлено в таблице 5.7.

Таблица 5.7 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Формируемые компетенции	Виды учебной деятельности				Формы контроля
	Лек. зан.	Прак. зан.	Лаб. раб.	Сам. раб.	
ПК-7	+	+	+	+	Лабораторная работа, Отчет по лабораторной работе, Отчет по практическому занятию (семинару), Практическое задание, Тестирование, Экзамен

6. Рейтинговая система для оценки успеваемости обучающихся

6.1. Балльные оценки для форм контроля

Балльные оценки для форм контроля представлены в таблице 6.1.

Таблица 6.1 – Балльные оценки

Формы контроля	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
8 семестр				
Лабораторная работа	8	10	10	28
Практическое задание	4	4	4	12
Тестирование	2	2	2	6
Отчет по лабораторной работе	4	4	4	12

Согласована на портале № 69953

Отчет по практическому занятию (семинару)	4	4	4	12
Экзамен				30
Итого максимум за период	22	24	24	100
Нарастающим итогом	22	46	70	100

6.2. Пересчет баллов в оценки за текущий контроль

Пересчет баллов в оценки за текущий контроль представлен в таблице 6.2.

Таблица 6.2 – Пересчет баллов в оценки за текущий контроль

Баллы на дату текущего контроля	Оценка
≥ 90% от максимальной суммы баллов на дату ТК	5
От 70% до 89% от максимальной суммы баллов на дату ТК	4
От 60% до 69% от максимальной суммы баллов на дату ТК	3
< 60% от максимальной суммы баллов на дату ТК	2

6.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 6.3.

Таблица 6.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка	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)

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература

1. Защита информации в радиоэлектронных системах передачи информации [Электронный ресурс]: Курс лекций, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу / Голиков А. М. - 2017. 913 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/7072 .

7.2. Дополнительная литература

1. Голиков, А. М. Защита информации в радиоэлектронных системах передачи информации: Сборник компьютерных лабораторных работ [Электронный ресурс] / А. М. Голиков. — Томск: ТУСУР, 2018. — 224 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/8806 .

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

Согласована на портале № 69953

1. Голиков, А. М. Кодирование и шифрование информации в радиоэлектронных системах передачи информации. Часть 2. Шифрование: Курс лекций, компьютерные лабораторные работы, компьютерный практикум, задание на самостоятельную работу. — [Электронный ресурс] / А. М. Голиков. — Изд. перераб. и доп. — Томск: ТУСУР, 2018. — 377 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/8846 .

7.3.2. 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.

7.4. Современные профессиональные базы данных и информационные справочные системы

1. При изучении дисциплины рекомендуется обращаться к современным базам данных, информационно-справочным и поисковым системам, к которым у ТУСУРа открыт доступ: https://lib.tusur.ru/ru/resursy/bazy-dannyh.

8. Материально-техническое и программное обеспечение дисциплины

8.1. 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 достаточным количеством посадочных мест для учебной группы, оборудованная доской и стандартной учебной мебелью. Имеются мультимедийное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

8.2. 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.);
- Мышь (оптическая) (8 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- 7-Zip;
- Adobe Acrobat Reader;
- Far Manager;
- Free Pascal;
- Free Pascal Lazarus (версия 1.6);
- GIMP;
- Google Chrome;
- Microsoft Windows Server 2008;

Согласована на портале № 69953

- Microsoft Windows XP;
- Mozilla Firefox;
- OpenOffice;
- Opera;
- Opera Developer;
- PTC Mathcad 13, 14;
- Scilab;

8.3. 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:
- 7-Zip;
- Adobe Acrobat Reader;
- Far Manager;
- Free Pascal;
- Free Pascal Lazarus (версия 1.6);
- GIMP;
- Google Chrome;
- Microsoft Windows Server 2008;
- Microsoft Windows XP;
- Mozilla Firefox;
- OpenOffice;
- Opera;
- Opera Developer;
- PTC Mathcad 13, 14;
- Scilab;

8.4. 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, 209 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Описание имеющегося оборудования:
- учебная мебель;
- компьютеры;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду ТУСУРа.

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

Согласована на портале № 69953

8.5. 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 зрения** 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.

9. Оценочные материалы и методические рекомендации по организации изучения дисциплины

9.1. Содержание оценочных материалов для текущего контроля и промежуточной аттестации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы, представленные в таблице 9.1.

Таблица 9.1 – Формы контроля и оценочные материалы

Названия разделов (тем) дисциплины	Формируемые компетенции	Формы контроля	Оценочные материалы (ОМ)
1 Предмет курса. Информационная безопасность в системе национальной безопасности Российской Федерации	ПК-7	Практическое задание	Темы практических заданий
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по практическому занятию (семинару)	Темы практических занятий
2 Основные понятия теории информационной безопасности. Анализ угроз информационной безопасности	ПК-7	Практическое задание	Темы практических заданий
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по практическому занятию (семинару)	Темы практических занятий

Согласована на портале № 69953

3 Методы и средства обеспечения информационной безопасности в радиоэлектронных системах передачи информации	ПК-7	Лабораторная работа	Темы лабораторных работ
		Практическое задание	Темы практических заданий
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по лабораторной работе	Темы лабораторных работ
		Отчет по практическому занятию (семинару)	Темы практических занятий
4 Основы комплексного обеспечения информационной безопасности в радиоэлектронных системах передачи	ПК-7	Лабораторная работа	Темы лабораторных работ
		Практическое задание	Темы практических заданий
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по лабораторной работе	Темы лабораторных работ
		Отчет по практическому занятию (семинару)	Темы практических занятий
5 Стандарты информационной безопасности, критерии и классы оценки защищенности	ПК-7	Практическое задание	Темы практических заданий
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по практическому занятию (семинару)	Темы практических занятий

Согласована на портале № 69953

6 Методология построения и анализа систем обеспечения информационной безопасности	ПК-7	Практическое задание	Темы практических заданий
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по практическому занятию (семинару)	Темы практических занятий
7 Технические каналы утечки информации в радиоэлектронных системах передачи	ПК-7	Лабораторная работа	Темы лабораторных работ
		Практическое задание	Темы практических заданий
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
		Отчет по лабораторной работе	Темы лабораторных работ
		Отчет по практическому занятию (семинару)	Темы практических занятий

Шкала оценки сформированности отдельных планируемых результатов обучения по дисциплине приведена в таблице 9.2.

Таблица 9.2 – Шкала оценки сформированности планируемых результатов обучения по дисциплине

Оценка	Баллы за ОМ	Формулировка требований к степени сформированности планируемых результатов обучения		
		знать	уметь	владеть
2 (неудовлетворительно)	< 60% от максимальной суммы баллов	отсутствие знаний или фрагментарные знания	отсутствие умений или частично освоенное умение	отсутствие навыков или фрагментарные применение навыков
3 (удовлетворительно)	от 60% до 69% от максимальной суммы баллов	общие, но не структурированные знания	в целом успешно, но не систематически осуществляемое умение	в целом успешное, но не систематическое применение навыков
4 (хорошо)	от 70% до 89% от максимальной суммы баллов	сформированные, но содержащие отдельные проблемы знания	в целом успешное, но содержащие отдельные пробелы умение	в целом успешное, но содержащие отдельные пробелы применение навыков

Согласована на портале № 69953

5 (отлично)	≥ 90% от максимальной суммы баллов	сформированные систематические знания	сформированное умение	успешное и систематическое применение навыков

Шкала комплексной оценки сформированности компетенций приведена в таблице 9.3.

Таблица 9.3 – Шкала комплексной оценки сформированности компетенций

Оценка	Формулировка требований к степени компетенции
2 (неудовлетворительно)	Не имеет необходимых представлений о проверяемом материале или Знать на уровне **ориентирования**, представлений. Обучающийся знает основные признаки или термины изучаемого элемента содержания, их отнесенность к определенной науке, отрасли или объектам, узнает в текстах, изображениях или схемах и знает, к каким источникам нужно обращаться для более детального его усвоения.
3 (удовлетворительно)	Знать и уметь на **репродуктивном** уровне. Обучающихся знает изученный элемент содержания репродуктивно: произвольно воспроизводит свои знания устно, письменно или в демонстрируемых действиях.
4 (хорошо)	Знать, уметь, владеть на **аналитическом** уровне. Зная на репродуктивном уровне, указывать на особенности и взаимосвязи изученных объектов, на их достоинства, ограничения, историю и перспективы развития и особенности для разных объектов усвоения.
5 (отлично)	Знать, уметь, владеть на **системном** уровне. Обучающийся знает изученный элемент содержания системно, произвольно и доказательно воспроизводит свои знания устно, письменно или в демонстрируемых действиях, учитывая и указывая связи и зависимости между этим элементом и другими элементами содержания дисциплины, его значимость в содержании дисциплины.

9.1.1. Примерный перечень тестовых заданий

1. Какие три основные составляющие информационной безопасности вам известны: 1) зашифрованность, целостность, доступность; 2) конфиденциальность, закрытость, доступность; 3) конфиденциальность, целостность, защищенность; 4) конфиденциальность, целостность, доступность.
2. Какие классы АС наиболее за.щищены, согласно руководящим документам Гостехкомиссии РФ: 1) 3Б и 3А; 2) 2Б и 2А; 3) 1Д, 1Г, 1В; 4) 1Б, 1А;
3. Какая модель является моделью произвольного (дискреционного) управлению доступом: 1) Модель Белла – ЛаПадула; 2) Модель Биба; 3) Хиррисона–Руззо-Ульмана; 4) Модель Кларка – Вилсона.
4. Какая модель является моделью мандатного управлению доступом: 1) Модель Белла – ЛаПадула; 2) Модель Биба; 3) Хиррисона–Руззо-Ульмана; 4) Модель Кларка – Вилсона.
5. Перечислите три основных вида угроз информационной безопасности: 1) угроза нарушения конфиденциальности, угроза нарушения целостности, угроза нарушения защищенности; 2) угроза нарушения конфиденциальности, угроза нарушения целостности, угроза нарушения доступности; 3) угроза нарушения конфиденциальности, угроза нарушения закрытости, угроза нарушения доступности; 4) угроза нарушения зашифрованности, угроза нарушения целостности, угроза нарушения доступности
6. Какая аутентификация наиболее сильная: 1) цифровая подпись; 2) пароль; 3) биометрическая; 4) уникальный предмет;
7. Какие два основных вида требований безопасности содержат «Общие критерии»: 1) требованиях безопасности, проектирование и разработка: 2) использование ресурсов, криптографическая поддержка; 3 оценка уязвимостей, оценка задания по безопасности; 4

Согласована на портале № 69953

функциональные, требования доверия;

8. Какие межсетевые экраны используют на границе локальной сети и сети Интернет: 1) коммутаторы, функционирующие на канальном уровне; 2) сетевые или пакетные фильтры; 3) шлюзы сеансового уровня (circuit-level proxy); 4) пакетные фильтры.
9. Какие методы защиты информации используются в стандарте IEEE802.11 (WiFi): 1) PAW, EWR; 2) WER, WAP; 3) PEW, APW; 4) WEP, WPA.
10. Какие виды скремблеров являются наиболее защищенными: 1) временные; 2) частотные; 3) комбинированные; 4) поточные.

9.1.2. Перечень экзаменационных вопросов

1. Выделите два основных типа межсетевых экранов. Какие действия по умолчанию осуществляются межсетевым экраном в отношении трафика? Является ли один из типов межсетевых экранов более безопасным, нежели другой? Что межсетевой экран прикладного уровня по умолчанию делает с внутренними адресами?
2. В чем сходство межсетевого экрана с фильтрацией пакетов и маршрутизатора? Когда рекомендуется выбирать межсетевой экран с пакетной фильтрацией? Что должен обеспечивать межсетевой экран для проверки состояния? При каком условии межсетевой экран прикладного уровня может называться гибридным?
3. Угрозы информации. Виды угроз. Основные нарушения. Характер происхождения угроз. Источники угроз. Предпосылки появления угроз.
4. Что такое информационная безопасность? Какие компоненты входят в информационную безопасность?
5. Назовите два типа биометрических систем. Назовите основные категории атак.
6. Система защиты информации. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации.
7. Методы и модели оценки уязвимости информации. Общая модель воздействия на информацию. Общая модель процесса нарушения физической целостности информации.
8. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных.
9. Для предотвращения перехвата должно использоваться шифрование - вместе с какой службой безопасности? Может ли служба обеспечения доступности предотвратить атаки на отказ в обслуживании?
10. Назовите три типа аутентификационных факторов. Почему двухфакторная аутентификация.
11. Методологические подходы к оценке уязвимости информации. Модель защиты системы. с полным перекрытием. Рекомендации по использованию моделей оценки уязвимости информации. Допущения в моделях оценки уязвимости информации.
12. Методы определения требований к защите информации. Факторы, обусловливающие конкретные требования к защите, обусловленные спецификой автоматизированной обработки ин- формации. Классификация требований к средствам защиты информации.
13. Требования к защите, определяемые структурой автоматизированной системы обработки данных. Требования к защите, обусловливаемые видом защищаемой информации. Требования, обусловливаемые взаимодействием пользователя с комплексом средств автоматизации.
14. Должна ли политика безопасности определять конкретные требования реализации для каждого типа систем внутри самой политики? Почему в политику безопасности включают отказы от защиты?
15. Назовите две составляющих риска. Каков уровень риска при отсутствии угроз?
16. Назовите две составляющих риска. Каков уровень риска при отсутствии угроз? Что такое уязвимость? Назовите четыре цели для угроз. Может ли угроза иметь более одной цели?
17. Где расположены доступные из интернета системы в архитектуре с одним межсетевым экраном? Почему порядок правил в наборе правил межсетевого экрана играет важную роль?
18. Можно ли рассматривать использование SSH как реализацию VPN? Почему пользовательские VPN требуют строгой аутентификации?

Согласована на портале № 69953

19. Может ли шифрование полностью защитить данные, передаваемые через VPN. С чем необходимо комбинировать политику, чтобы обеспечить безопасность VPN?
20. Пригодны ли межузловые VPN для использования между организациями? Почему адресация является потенциальной проблемой, связанной с межузловыми VPN?
21. Анализ существующих методик определения требований к защите информации.
22. Факторы, влияющие на требуемый уровень защиты информации. Функции и задачи защиты информации. Основные положения механизмов непосредственной защиты и механизмы управления механизмами непосредственной защиты. Методы формирования функций защиты. События, возникающие при формировании функций защиты.
23. Если информация очень секретна, какой метод аутентификации следует использовать? Где должны храниться записи аудита в идеальном случае?
24. В чем сходство межсетевого экрана с фильтрацией пакетов и маршрутизатора? Когда рекомендуется выбирать межсетевой экран с пакетной фильтрацией
25. Какое скремблирование реализует данный скремблер? (аналоговое или цифровое). Какой вид частотного преобразования осуществляет данный скремблер?
26. Каковы преимущества и недостатки данного вида скремблирования? Какова разборчивость выходного сигнала? Какую полосу частот занимает выходной сигнал?
27. Способы и средства защиты информации. Способы «абсолютной системы защиты». Архитектура систем защиты информации. Требования. Общеметодологических принципов архитектуры системы защиты информации.
28. На каких системах должны устанавливаться антивирусные программы? Какой длины должны быть пароли?
29. Что должен обеспечивать межсетевой экран для проверки состояния? При каком условии межсетевой экран прикладного уровня может называться гибридным?
30. Согласно ГОСТ Р ИСО/МЭК 1 - какие три группы факторов необходимо учитывать при формировании требований в области информационной безопасности?
31. Какие основные информационные активы должны быть учтены и закреплены за ответственными владельцами для обеспечения информационной безопасности организации?
32. Ключевые моменты этапа анализа рисков: (перечислите)
33. Пригодны ли межузловые VPN для использования между организациями? Почему адресация является потенциальной проблемой, связанной с межузловыми VPN?
34. Какие два критерия должны использоваться для определения того, какое устройство следует использовать - межсетевой экран или VPN-сервер на отдельной системе? Если используется отдельный VPN-сервер, должен ли он размещаться в демилитаризованной зоне интернета?
35. Каким набором параметров может быть идентифицирован риск. По какой формуле может быть вычислена стоимость риска?
36. Перечислите стандарте ОК 11 классов функциональных требований.
37. Как производится вычисление потенциала нападения?
38. Можно ли рассматривать использование SSH как реализацию VPN? Почему пользовательские VPN требуют строгой аутентификации?

9.1.3. Темы практических заданий

1. Стандарты информационной безопасности и критерии оценки безопасности систем и сетей передачи информации
2. Разработка архитектуры модели безопасности информационных систем и сетей
3. Разработка практических рекомендаций по обеспечению безопасности информационных систем
4. Законодательство в области информационной безопасности
5. Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Простые и составные технические каналы утечки информации. Характеристика и возможности оптических, акустических, радиоэлектронных и материально-вещественных каналов утечки информации.

Согласована на портале № 69953

9.1.4. Темы практических занятий

1. Стандарты информационной безопасности и критерии оценки безопасности систем и сетей передачи информации
2. Разработка архитектуры модели безопасности информационных систем и сетей
3. Разработка практических рекомендаций по обеспечению безопасности информационных систем
4. Законодательство в области информационной безопасности
5. Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Простые и составные технические каналы утечки информации. Характеристика и возможности оптических, акустических, радиоэлектронных и материально-вещественных каналов утечки информации.

9.1.5. Темы лабораторных работ

1. Изучение международного стандарта безопасности информационных систем ISO. Исследование системы защиты информации «Страж NT». Система защиты информации SecretNet. Система защиты информации Dallas
2. Система анализа рисков и проверки политики информационной безопасности предприятия
3. Энергетическое скрытие речевой информации. Скремблеры.

9.2. Методические рекомендации

Учебный материал излагается в форме, предполагающей самостоятельное мышление студентов, самообразование. При этом самостоятельная работа студентов играет решающую роль в ходе всего учебного процесса.

Начать изучение дисциплины необходимо со знакомства с рабочей программой, списком учебно-методического и программного обеспечения. Самостоятельная работа студента включает работу с учебными материалами, выполнение контрольных мероприятий, предусмотренных учебным планом.

В процессе изучения дисциплины для лучшего освоения материала необходимо регулярно обращаться к рекомендуемой литературе и источникам, указанным в учебных материалах; пользоваться через кабинет студента на сайте Университета образовательными ресурсами электронно-библиотечной системы, а также общедоступными интернет-порталами, содержащими научно-популярные и специализированные материалы, посвященные различным аспектам учебной дисциплины.

При самостоятельном изучении тем следуйте рекомендациям:

– чтение или просмотр материала осуществляйте со скоростью, достаточной для индивидуального понимания и освоения материала, выделяя основные идеи; на основании изученного составить тезисы. Освоив материал, попытаться соотнести теорию с примерами из практики;

– если в тексте встречаются незнакомые или малознакомые термины, следует выяснить их значение для понимания дальнейшего материала;

– осмысливайте прочитанное и изученное, отвечайте на предложенные вопросы.

Студенты могут получать индивидуальные консультации, в т.ч. с использованием средств телекоммуникации.

По дисциплине могут проводиться дополнительные занятия, в т.ч. в форме вебинаров. Расписание вебинаров и записи вебинаров публикуются в электронном курсе / электронном журнале по дисциплине.

9.3. 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 9.4.

Таблица 9.4 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Согласована на портале № 69953

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, определяющимися исходя из состояния обучающегося на момент проверки

9.4. 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:
– 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 № 69953

ЛИСТ СОГЛАСОВАНИЯ

Рассмотрена и одобрена на заседании кафедры РТС
протокол № 5 от « 1 » 12 2022 г.

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Заведующий выпускающей каф. РТС	А.А. Мещеряков	Согласовано, 5bbb058c-a625-4513-8e7f-25eb16694704
Заведующий обеспечивающей каф. РТС	А.А. Мещеряков	Согласовано, 5bbb058c-a625-4513-8e7f-25eb16694704
И.О. начальника учебного управления	И.А. Лариошина	Согласовано, c3195437-a02f-4972-a7c6-ab6ee1f21e73

ЭКСПЕРТЫ:

Доцент, каф. РТС	В.А. Громов	Согласовано, bbaa5b2b-4c38-484f-a5bb-85f9ddafe277
Старший преподаватель, каф. РТС	Д.О. Ноздреватых	Согласовано, bd0039b0-9c48-4859-9803-60c9ddba7116

РАЗРАБОТАНО:

Доцент, каф. РТС	А.М. Голиков	Разработано, d76b3893-b3a9-44a5-84f8-e53e691ec9d0

Согласована на портале № 69953