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

Моделирование и оптимизация средств информационной безопасности

Уровень образования: **высшее образование - специалитет**
Направление подготовки / специальность: **10.05.02 Информационная безопасность телекоммуникационных систем**
Направленность (профиль) / специализация: **Безопасность телекоммуникационных систем информационного взаимодействия**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РСС, Кафедра радиоэлектроники и систем связи**
Курс: **3**
Семестр: **6**
Учебный план набора 2012 года

Распределение рабочего времени

№	Виды учебной деятельности	6 семестр	Всего	Единицы
1	Лекции	26	26	часов
2	Практические занятия	46	46	часов
3	Всего аудиторных занятий	72	72	часов
4	Самостоятельная работа	36	36	часов
5	Всего (без экзамена)	108	108	часов
6	Подготовка и сдача экзамена	36	36	часов
7	Общая трудоемкость	144	144	часов
		4.0	4.0	З.Е.

Экзамен: 6 семестр

Томск 2018

Согласована на портале № 40264

Рассмотрена и одобрена на заседании кафедры
протокол № 11 от « 3 » 7 2018 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 10.05.02 Информационная безопасность телекоммуникационных систем, утвержденного 16.11.2016 года, рассмотрена и одобрена на заседании кафедры РСС «___» _____ 20__ года, протокол №_____.

Разработчик:

доцент кафедра Радиоэлектроники и систем связи (РСС) _____ Д. В. Дубинин

Заведующий обеспечивающей каф. РСС _____ А. В. Фатеев

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан РТФ _____ К. Ю. Попова

Заведующий выпускающей каф. РСС _____ А. В. Фатеев

Эксперты:

Профессор кафедры радиоэлектроники и систем связи (РСС) _____ А. С. Задорин

Старший преподаватель кафедры радиоэлектроники и систем связи (РСС) _____ Ю. В. Зеленецкая

Согласована на портале № 40264

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Формирование у студентов устойчивых основ знаний моделирования и оптимизации средств информационной безопасности, приобретения при этом необходимых умений и навыков.

1.2. Задачи дисциплины

– - Формирование понятия системы, понятий, характеризующих строение, функционирование и развитие систем;
– - Изучение закономерности систем, закономерности целеобразования;
– - Понятие проблемы принятия решения;
– - Изучение классификации методов моделирования систем;
– - Методы формализованного представления систем;
– - Системное понятие и модель объекта защиты;
– - Понятие и модель системы защиты информации объекта защиты;
– - Методика практического моделирования систем защиты информации;
– - Практический анализ объекта защиты, выявление проблемной ситуации и постановка задачи;
– - Практическая разработка модели системы защиты информации и оптимизация на этой основе средств информационной безопасности.

2. Место дисциплины в структуре ОПОП

Дисциплина «Моделирование и оптимизация средств информационной безопасности» (Б1.В.ДВ.2.2) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Информатика, Информационные технологии, Основы информационной безопасности.

Последующими дисциплинами являются: Информационная безопасность телекоммуникационных систем, Методы математического моделирования, Организационное и правовое обеспечение информационной безопасности, Техническая защита информации.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ПК-13 способностью организовывать выполнение требований режима защиты информации ограниченного доступа, разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности телекоммуникационных систем;

В результате изучения дисциплины обучающийся должен:

– **знать** Основы моделирования систем и оптимизации средств информационной безопасности.
– **уметь** На концептуальном и практическом уровне разрабатывать модели систем и осуществлять оптимизацию средств информационной безопасности.
– **владеть** Методикой практического моделирования и оптимизации средств информационной безопасности.

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
		6 семестр
Аудиторные занятия (всего)	72	72
Лекции	26	26
Практические занятия	46	46
Самостоятельная работа (всего)	36	36

Согласована на портале № 40264

Проработка лекционного материала	13	13
Подготовка к практическим занятиям, семинарам	23	23
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	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
6 семестр					
1 Введение.	1	0	1	2	ПК-13
2 Понятие системы.	2	3	2	7	ПК-13
3 Понятия, характеризующие строение, функционирование и развитие систем.	3	4	2	9	ПК-13
4 Закономерности систем.	2	4	2	8	ПК-13
5 Закономерности целеобразования.	2	4	2	8	ПК-13
6 Методы и модели теории систем и системного анализа.	2	4	2	8	ПК-13
7 Классификации методов моделирования систем.	2	4	2	8	ПК-13
8 Методы формализованного представления систем.	2	4	2	8	ПК-13
9 Понятие и модель объекта защиты.	2	4	3	9	ПК-13
10 Понятие и модель системы защиты информации (СЗИ) объекта защиты.	2	4	4	10	ПК-13
11 Методика моделирования СЗИ.	2	3	4	9	ПК-13
12 Практический анализ объекта защиты.	2	4	5	11	ПК-13
13 Практическая разработка модели системы защиты информации и оптимизация на этой основе средств информационной безопасности.	2	4	5	11	ПК-13
Итого за семестр	26	46	36	108	
Итого	26	46	36	108	

Согласована на портале № 40264

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
6 семестр			
1 Введение.	Цели, структура и задачи курса. Взаимосвязь курса с другими дисциплинами, системный характер проблем при решении задач по моделированию систем информационной безопасности и оптимизации средств информационной безопасности. Специфика курса.	1	ПК-13
	Итого	1	
2 Понятие системы.	Понятие системного подхода, системы, системного анализа, взаимосвязь понятий и их практическое предназначение.	2	ПК-13
	Итого	2	
3 Понятия, характеризующие строение, функционирование и развитие систем.	Взаимосвязь понятий элемента, компонента и подсистемы. Понятие «связь». Системное понятие «цель», структура, поведение, жизненный цикл. Виды и формы представления структур. Классификация систем.	3	ПК-13
	Итого	3	
4 Закономерности систем.	Закономерности взаимодействия части и целого, закономерности иерархической упорядоченности, закономерности, осуществимости систем, закономерности развития систем.	2	ПК-13
	Итого	2	
5 Закономерности целеобразования.	Закономерности возникновения и формулирования целей, закономерности формирования структур целей.	2	ПК-13
	Итого	2	
6 Методы и модели теории систем и системного анализа.	Понятие проблемы принятия решения. Подходы к анализу и проектированию систем.	2	ПК-13
	Итого	2	
7 Классификации методов моделирования систем.	Методы, направленные на активизацию интуиции и опыта специалистов, методы формализованного представления систем, Специальные методы, методики постепенной формализации задачи.	2	ПК-13
	Итого	2	
8 Методы формализованного представления систем.	Введение в понятие аналитических, статистических методов, методов дискретной математики, включая теоретико-множественные, логические, лингвистические, семиотические представления.	2	ПК-13

Согласована на портале № 40264

	Итого	2	
9 Понятие и модель объекта защиты.	Законодательный и нормативно-правовой базис понятия объекта защиты. Системная модель объекта защиты. Основные критерии, определяющие формирование реальных объектов защиты.	2	ПК-13
	Итого	2	
10 Понятие и модель системы защиты информации (СЗИ) объекта защиты.	Законодательный и нормативно-правовой базис понятия объекта защиты. Системная модель системы защиты информации объекта защиты (СЗИ). Критерии, определяющие формирование реальных систем защиты информации.	2	ПК-13
	Итого	2	
11 Методика моделирования СЗИ.	Классификация методов моделирования СЗИ, факторы, определяющие методы моделирования, практические подходы к моделированию СЗИ. Понятие оптимизации средств информационной безопасности.	2	ПК-13
	Итого	2	
12 Практический анализ объекта защиты.	Практический анализ объекта защиты, выявление проблемной ситуации и постановка задачи по обеспечению информационной безопасности.	2	ПК-13
	Итого	2	
13 Практическая разработка модели системы защиты информации и оптимизация на этой основе средств информационной безопасности.	Особенности разработки моделей систем защиты информации объекта вычислительной техники, объекта выделенное помещение, информационной системы персональных данных.Оптимизация средств информационной безопасности объектов защиты.	2	ПК-13
	Итого	2	
Итого за семестр		26	

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	7	8	9	10	11	12	13
Предшествующие дисциплины													
1 Информатика						+	+	+					
2 Информационные технологии						+	+		+		+		
3 Основы информационной безопасности		+	+	+	+	+	+					+	+
Последующие дисциплины													

Согласована на портале № 40264

1 Информационная безопасность телекоммуникационных систем		+					+		+	+		+	+
2 Методы математического моделирования							+	+	+	+	+	+	+
3 Организационное и правовое обеспечение информационной безопасности							+		+	+	+	+	+
4 Техническая защита информации		+	+	+	+	+	+	+	+	+	+		+

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.	Сам. раб.	
ПК-13	+	+	+	Экзамен, Конспект самоподготовки, Опрос на занятиях, Выступление (доклад) на занятии, Тест

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

7. Лабораторные работы

Не предусмотрено РУП.

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
6 семестр			
2 Понятие системы.	Понятие системного подхода, системы, системного анализа, взаимосвязь понятий и их практическое предназначение.	3	ПК-13
	Итого	3	
3 Понятия, характеризующие строение, функционирование и	Взаимосвязь понятий элемента, компонента и подсистемы. Понятие «связь». Системное понятие «цель», структура, поведение, жизненный цикл. Виды и формы представления структур. Класси-	4	ПК-13

Согласована на портале № 40264

развитие систем.	фикация систем.		
	Итого	4	
4 Закономерности систем.	Закономерности взаимодействия части и целого, закономерности иерархической упорядоченности, закономерности, осуществимости систем, закономерности развития систем.	4	ПК-13
	Итого	4	
5 Закономерности целеобразования.	Закономерности возникновения и формулирования целей, закономерности формирования структур целей.	4	ПК-13
	Итого	4	
6 Методы и модели теории систем и системного анализа.	Понятие проблемы принятия решения. Подходы к анализу и проектированию систем.	4	ПК-13
	Итого	4	
7 Классификации методов моделирования систем.	Методы, направленные на активизацию интуиции и опыта специалистов, методы формализованного представления систем. Специальные методы, методики постепенной формализации задачи.	4	ПК-13
	Итого	4	
8 Методы формализованного представления систем.	Введение в понятие аналитических, статистических методов, методов дискретной математики, включая теоретико-множественные, логические, лингвистические, семиотические представления.	4	ПК-13
	Итого	4	
9 Понятие и модель объекта защиты.	Законодательный и нормативно-правовой базис понятия объекта защиты. Системная модель объекта защиты. Основные критерии, определяющие формирование реальных объектов защиты.	4	ПК-13
	Итого	4	
10 Понятие и модель системы защиты информации (СЗИ) объекта защиты.	Законодательный и нормативно-правовой базис понятия объекта защиты. Системная модель системы защиты информации объекта защиты (СЗИ). Критерии, определяющие формирование реальных систем защиты информации.	4	ПК-13
	Итого	4	
11 Методика моделирования СЗИ.	Классификация методов моделирования СЗИ, факторы, определяющие методы моделирования, практические подходы к моделированию СЗИ. Понятие оптимизации средств информационной безопасности.	3	ПК-13
	Итого	3	
12 Практический анализ объекта защиты.	Практический анализ объекта защиты, выявление проблемной ситуации и постановка задачи по обеспечению информационной безопасности.	4	ПК-13
	Итого	4	
13 Практическая	Особенности разработки моделей систем защиты	4	ПК-13

Согласована на портале № 40264

разработка модели системы защиты информации и оптимизация на этой основе средств информационной безопасности.	информации объекта вычислительной техники, объекта выделенное помещение, информационной системы персональных данных.Оптимизация средств информационной безопасности объектов защиты.		
	Итого	4	
Итого за семестр		46	

9. Самостоятельная работа

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

Таблица 9.1 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
6 семестр				
1 Введение.	Проработка лекционного материала	1	ПК-13	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Тест, Экзамен
	Итого	1		
2 Понятие системы.	Подготовка к практическим занятиям, семинарам	1	ПК-13	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Тест, Экзамен
	Проработка лекционного материала	1		
	Итого	2		
3 Понятия, характеризующие строение, функционирование и развитие систем.	Подготовка к практическим занятиям, семинарам	1	ПК-13	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Тест, Экзамен
	Проработка лекционного материала	1		
	Итого	2		
4 Закономерности систем.	Подготовка к практическим занятиям, семинарам	1	ПК-13	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Тест, Экзамен
	Проработка лекционного материала	1		
	Итого	2		
5 Закономерности целеобразования.	Подготовка к практическим занятиям, семинарам	1	ПК-13	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Тест, Экзамен
	Проработка лекционного материала	1		
	Итого	2		

Согласована на портале № 40264

6 Методы и модели теории систем и системного анализа.	Подготовка к практическим занятиям, семинарам	1	ПК-13	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Тест, Экзамен
	Проработка лекционного материала	1		
	Итого	2		
7 Классификации методов моделирования систем.	Подготовка к практическим занятиям, семинарам	1	ПК-13	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Тест, Экзамен
	Проработка лекционного материала	1		
	Итого	2		
8 Методы формализованного представления систем.	Подготовка к практическим занятиям, семинарам	1	ПК-13	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Тест, Экзамен
	Проработка лекционного материала	1		
	Итого	2		
9 Понятие и модель объекта защиты.	Подготовка к практическим занятиям, семинарам	2	ПК-13	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Тест, Экзамен
	Проработка лекционного материала	1		
	Итого	3		
10 Понятие и модель системы защиты информации (СЗИ) объекта защиты.	Подготовка к практическим занятиям, семинарам	3	ПК-13	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Тест, Экзамен
	Проработка лекционного материала	1		
	Итого	4		
11 Методика моделирования СЗИ.	Подготовка к практическим занятиям, семинарам	3	ПК-13	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Тест, Экзамен
	Проработка лекционного материала	1		
	Итого	4		
12 Практический анализ объекта защиты.	Подготовка к практическим занятиям, семинарам	4	ПК-13	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Тест, Экзамен
	Проработка лекционного материала	1		
	Итого	5		
13 Практическая разработка модели системы защиты	Подготовка к практическим занятиям, семинарам	4	ПК-13	Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на за-

Согласована на портале № 40264

информации и оптимизация на этой основе средств информационной безопасности.	Проработка лекционного материала	1		нятиях, Тест, Экзамен
	Итого	5		
Итого за семестр		36		
	Подготовка и сдача экзамена	36		Экзамен
Итого		72		

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
6 семестр				
Выступление (доклад) на занятии	5	5	10	20
Конспект самоподготовки	5	5	5	15
Опрос на занятиях	5	5	5	15
Тест	5	5	10	20
Итого максимум за период	20	20	30	70
Экзамен				30
Нарастающим итогом	20	40	70	100

11.2. Пересчет баллов в оценки за контрольные точки

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

Таблица 11.2 – Пересчет баллов в оценки за контрольные точки

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

11.3. Пересчет суммы баллов в традиционную и международную оценку

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

Таблица 11.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка (ГОС)	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)

Согласована на портале № 40264

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. Основы теории систем и системного анализа [Электронный ресурс]: Учебное пособие / М. П. Силич, В. А. Силич - 2013. 342 с. - Режим доступа: https://edu.tusur.ru/publications/5452 (дата обращения: 23.07.2018).

12.2. Дополнительная литература

1. Теория организации [Электронный ресурс]: Учебное пособие / М. П. Силич, Л. В. Кудряшова - 2016. 200 с. - Режим доступа: https://edu.tusur.ru/publications/6778 (дата обращения: 23.07.2018).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. Теория систем и системный анализ [Электронный ресурс]: Методические указания к выполнению практических работ для студентов направления подготовки 231000.62 «Программная инженерия» (бакалавриат) часть 2 / М. П. Силич - 2015. 43 с. - Режим доступа: https://edu.tusur.ru/publications/5449 (дата обращения: 23.07.2018).
2. Теория систем и системный анализ [Электронный ресурс]: Методические указания к выполнению самостоятельной работы для студентов направления подготовки 231000.62 «Программная инженерия» (бакалавриат) / М. П. Силич - 2013. 5 с. - Режим доступа: https://edu.tusur.ru/publications/5447 (дата обращения: 23.07.2018).

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. При изучении дисциплины рекомендуется использовать базы данных и информационно-справочные системы, к которым у ТУСУРа есть доступ https://lib.tusur.ru/ru/resursy/bazydannyh

Согласована на портале № 40264

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

Учебная лаборатория радиоэлектроники / Лаборатория ГПО

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

634034, Томская область, г. Томск, Вершинина улица, д. 47, 407 ауд.

Описание имеющегося оборудования:

- Доска магнитно-маркерная;
- Коммутатор D-Link Switch 24 port;
- Компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. (12 шт.);
- Вольтметр В3-38 (7 шт.);
- Генератор сигналов специальной формы АКИП ГСС-120 (2 шт.);
- Кронштейн PTS-4002;
- Осциллограф EZ Digital DS-1150C (3 шт.);
- Осциллограф С1-72 (4 шт.);
- Телевизор плазменный Samsung;
- Цифровой генератор сигналов РСС-80 (4 шт.);
- Цифровой осциллограф GDS-810C (3 шт.);
- Автоматизированное лабораторное место по схемотехнике и радиоавтоматике (7 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- 7-Zip
- Adobe Acrobat Reader
- Far Manager
- Google Chrome
- LibreOffice
- Microsoft Windows
- Mozilla Firefox
- PDFCreator
- WinDjView

13.1.3. Материально-техническое и программное обеспечение для самостоятельной работы

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

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

Состав оборудования:

- учебная мебель;

Согласована на портале № 40264

- 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. Системный подход определяется как…

Совокупность методологических средств, используемых для подготовки и обоснования решений по сложным проблемам.

Направление методологии специально-научного познания и социальной практики, в основе которого лежит исследование объектов как систем.

Направление исследования объектов и систем по совокупности и взаимосвязи установленных критериев.

Особый вид познавательной деятельности, нацеленный на выработку объективных, системно организованных и обоснованных знаний о действительности.

2. Система обеспечения информационной безопасности организации - это...

Система, направленная на устранение (нейтрализацию, парирование) внутренних и внешних угроз информационной безопасности организации или на минимизацию ущерба от возможной реализации таких угроз.

Система обеспечения информационной безопасности, предусматривающая установление временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режимы работы объекта информатизации.

Система, объединенная целевой направленностью упорядоченной совокупности документов, взаимосвязанных по признакам происхождения, назначения, вида, сферы деятельности, еди-

Согласована на портале № 40264

ных требований к их оформлению и регламентирующих в организации деятельность по обеспечению информационной безопасности.

Система, направленная на предотвращения ущерба интересам организации в условиях угроз в информационной сфере на основе разработки СЗИ с использованием имеющихся в её распоряжении активов.

3. Система защиты информации организации определяется как...

Организационно-техническая структура системы менеджмента информационной безопасности организации, реализующая решение определенной задачи, направленной на противодействие угрозам информационной безопасности организации.

Система, обеспечивающая скоординированные действия по руководству и управлению организацией в части обеспечения ее информационной безопасности в соответствии с изменяющимися условиями внутренней и внешней среды организации.

Совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации.

Совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

4. Защищаемая информация – это…

Сведения (сообщения, данные) независимо от формы их представления, подлежащие защите.

Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Сведения, в том числе излучения, знаки, сигналы, голосовая информация, письменный текст, изображения, звуки или сообщения любого рода, подлежащие защите.

Любая информация, требующая защиты по критериям конфиденциальности, доступности и целостности.

5. Организация защиты информации на предприятии обеспечивается по...

Совокупности подсистем организационно-правовой, технической, криптографической и физической защиты информации.

Совокупности критериев системы менеджмента обеспечения информационной безопасности.

Совокупности критериев системы защиты информации на предприятии.

Совокупности и взаимосвязи всех видов и направлений защиты информации.

6. Техника защиты информации определяется как...

Совокупность средств защиты информации, в том числе средств физической защиты информации, криптографические средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

Совокупность технических средств, используемых для обеспечения информационной безопасности объекта защиты.

Совокупность технических, программных и программно-технических средств средств, используемых для обеспечения информационной безопасности объекта защиты.

Совокупность технических средств и средств физической защиты информации, используемых для обеспечения информационной безопасности объекта защиты.

7. Контролируемая зона - это...

Согласована на портале № 40264

Территория, принадлежащая организации, на которой исключено пребывание посторонних лиц и транспортных средств, не имеющих постоянного или разового допуска.

Пространство, в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.

Пространство, принадлежность которого организации юридически подтверждена и в котором исключено пребывание посторонних лиц и транспортных средств, не имеющих постоянного или разового допуска.

Территория, принадлежащая организации и обозначенная средствами технической укрепленности, на которой исключено пребывание посторонних лиц и транспортных средств, не имеющих постоянного или разового допуска.

8. Технический канал утечки информации (ТКУИ) определяется как...

Совокупность канала передачи информации и средств перехвата информативных сигналов.

Совокупность информации, информативных сигналов и технических средств перехвата информации.

Совокупность источника информации, канала передачи (физической среды с шумами) и приемника информации.

Совокупность источника информации физической среды передачи и средств перехвата информации.

9. Подсистема технической защиты информации (ЗИ) на предприятии – это…

Подсистема ЗИ, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

Подсистема ЗИ, заключающаяся в обеспечении системы защиты информации (данных) путем применения комплекса средств техники защиты информации.

Подсистема ЗИ, заключающаяся в обеспечении безопасности информации (данных) путем применения комплекса средств техники защиты информации.

Подсистема ЗИ, заключающаяся в обеспечении безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, путем применения технических и программно-технических средств.

10. Подсистема организационно-правовой защиты информации (ЗИ) на предприятии определяется как…

Подсистема ЗИ правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль их исполнения.

Подсистема ЗИ, включающая в себя объединенную целевой направленностью упорядоченную совокупность документов, взаимосвязанных по признакам происхождения, назначения, вида, сферы деятельности, единых требований к их оформлению и регламентирующих в организации деятельность по обеспечению информационной безопасности.

Подсистема ЗИ организационно-правовыми методами, включающая в себя разработку организационно-распорядительных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль их исполнения.

Подсистема ЗИ, включающая в себя совокупность документов, взаимосвязанных по признакам происхождения, назначения, вида, сферы деятельности, единых требований к их оформлению и регламентирующих в организации деятельность по обеспечению информационной безопасности, а также надзор и контроль их исполнения.

11. Подсистема криптографической защиты информации (ЗИ) на предприятии – это…

Подсистема ЗИ с помощью её криптографического преобразования.

Подсистема ЗИ с использованием средств криптографического преобразования.

Согласована на портале № 40264

Подсистема ЗИ на основе шифрования информации с использованием криптографических средств.

Подсистема ЗИ на основе шифрования и дешифрования информации с использованием криптографических средств.

12. Подсистема физической защиты информации (ЗИ) на предприятии определяется как…

Подсистема ЗИ на основе применения организационных мер и путем использования средств технической укреплённости объекта защиты.

Подсистема ЗИ путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

Подсистема ЗИ на основе применения организационных и технических мер обеспечения безопасности объекта защиты.

Подсистема ЗИ на основе применения организационных мер и путем использования средств противокриминальной защиты объекта.

13. Подсистема криптографической защиты информации (ЗИ) на предприятии – это…

Подсистема ЗИ с помощью её криптографического преобразования.

Подсистема ЗИ с использованием средств криптографического преобразования.

Подсистема ЗИ на основе шифрования информации с использованием криптографических средств.

Подсистема ЗИ на основе шифрования и дешифрования информации с использованием криптографических средств.

14. Подсистема технической защиты информации (ЗИ) объектов информатизации на предприятии включает…

Подсистемы ЗИ от перехвата информации по ТКУИ, от ПНВ и НПВ на основе технических средств ЗИ.

Подсистемы ЗИ от перехвата информации по ТКУИ и от НСД в АС с использованием технических средств ЗИ.

Подсистемы ЗИ от перехвата информации по ТКУИ, криптозащиты, от ПНВ и НПВ на основе технических средств ЗИ.

Подсистемы ЗИ от перехвата информации по ТКУИ, от НСД в АС, от ПНВ и НПВ.

15. Модель угроз безопасности информации определяется как…

Совокупность факторов и условий, создающих опасность нарушения информационной безопасности организации, вызывающую или способную вызвать негативные последствия (ущерб/вред) для организации.

Формальное изложение правил поведения, процедур, практических приемов или руководящих принципов в области информационной безопасности, которыми руководствуется организация в своей деятельности.

Физическое, математическое, описательное представление свойств и характеристик угроз безопасности информации.

Заранее намеченный результат обеспечения информационной безопасности организации в соответствии с установленными требованиями в политике ИБ (организации).

16. Модель нарушителя информационной безопасности определяется как…

Описание и классификация нарушителей информационной безопасности (ИБ), включая описание их опыта, знаний, доступных ресурсов, необходимых для реализации угрозы, возможной мотивации их действий, а также способы реализации угроз ИБ со стороны указанных нарушителей.

Физическое, математическое, описательное представление свойств и характеристик нарушителя информационной безопасности организации.

Описание и классификация нарушителей информационной безопасности (ИБ) на основе

Согласована на портале № 40264

физического, математического, описательного представления их свойств и характеристик.

Описание и классификация нарушителей ИБ с использованием аппарата моделирования систем.

17. Техническая реализация ПТЗИ объектов информатизации на предприятии включает…

Подсистемы ЗИ от перехвата информации по ТКУИ, от ПНВ и НПВ на основе технических средств ЗИ и организационные меры меры .

Подсистемы ЗИ от перехвата информации по ТКУИ и от НСД в АС с использованием технических средств ЗИ и организационные меры.

Подсистемы ЗИ от перехвата информации по ТКУИ, криптозащиты, от ПНВ и НПВ на основе технических средств ЗИ и организационные меры .

Подсистемы ЗИ от перехвата информации по ТКУИ, от НСД в АС, от ПНВ, НПВ и организационные меры.

18. Автоматизированная система - это…

Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Система, состоящая из комплекса средств автоматизации и реализующая информационную технологию выполнения установленных функций.

19. Система защиты информации от несанкционированного доступа в автоматизированной системе – это…

Комплекс организационно-технических мероприятий, направленных на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации.

Подсистемы ЗИ от перехвата информации по ТКУИ и от НСД в АС с использованием технических средств ЗИ.

Комплекс программно-технических и организационных решений по защите информации от несанкционированного доступа.

Совокупность мер, направленных на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

20. Сеть связи – это…

Совокупность технических средств, образующих вторичную сеть на базе типовых физических цепей, типовых каналов передачи и сетевых трактов первичной сети, и подсистем нумерации, сигнализации, тарификации, технического обслуживания и управления, обеспечивающая электросвязь определенного вида.

Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Организационно-техническая структура системы менеджмента информационной безопасности организации, реализующая решение определенной задачи, предназначенная для электросвязи в организации.

Технологическая система, включающая в себя средства и линии связи и предназначенная для электросвязи или почтовой связи.

14.1.2. Экзаменационные вопросы

Понятие системного подхода, системы, системного анализа, взаимосвязь понятий и их практическое предназначение.

Взаимосвязь понятий элемента, компонента и подсистемы. Понятие «связь». Системное по-

Согласована на портале № 40264

нятие «цель», структура, поведение, жизненный цикл. Виды и формы представления структур. Классификация систем.

Закономерности взаимодействия части и целого, закономерности иерархической упорядоченности, закономерности, осуществимости систем, закономерности развития систем.

Закономерности возникновения и формулирования целей, закономерности формирования структур целей.

Понятие проблемы принятия решения. Подходы к анализу и проектированию систем.

Методы, направленные на активизацию интуиции и опыта специалистов, методы формализованного представления систем, Специальные методы, методики постепенной формализации задачи.

Введение в понятие аналитических, статистических методов, методов дискретной математики, включая теоретико-множественные, логические, лингвистические, семиотические представления.

Законодательный и нормативно-правовой базис понятия объекта защиты. Системная модель объекта защиты. Основные критерии, определяющие формирование реальных объектов защиты.

Законодательный и нормативно-правовой базис понятия объекта защиты. Системная модель системы защиты информации объекта защиты (СЗИ). Критерии, определяющие формирование реальных систем защиты информации.

Классификация методов моделирования СЗИ, факторы, определяющие методы моделирования, практические подходы к моделированию СЗИ. Понятие оптимизации средств информационной безопасности.

Практический анализ объекта защиты, выявление проблемной ситуации и постановка задачи по обеспечению информационной безопасности.

Особенности разработки моделей систем защиты информации объекта вычислительной техники, объекта выделенное помещение, информационной системы персональных данных.Оптимизация средств информационной безопасности объектов защиты.

14.1.3. Темы опросов на занятиях

Цели, структура и задачи курса. Взаимосвязь курса с другими дисциплинами, системный характер проблем при решении задач по моделированию систем информационной безопасности и оптимизации средств информационной безопасности. Специфика курса.

Понятие системного подхода, системы, системного анализа, взаимосвязь понятий и их практическое предназначение.

Взаимосвязь понятий элемента, компонента и подсистемы. Понятие «связь». Системное понятие «цель», структура, поведение, жизненный цикл. Виды и формы представления структур. Классификация систем.

Закономерности взаимодействия части и целого, закономерности иерархической упорядоченности, закономерности, осуществимости систем, закономерности развития систем.

Закономерности возникновения и формулирования целей, закономерности формирования структур целей.

Понятие проблемы принятия решения. Подходы к анализу и проектированию систем.

Методы, направленные на активизацию интуиции и опыта специалистов, методы формализованного представления систем, Специальные методы, методики постепенной формализации задачи.

Введение в понятие аналитических, статистических методов, методов дискретной математики, включая теоретико-множественные, логические, лингвистические, семиотические представления.

Законодательный и нормативно-правовой базис понятия объекта защиты. Системная модель объекта защиты. Основные критерии, определяющие формирование реальных объектов защиты.

Законодательный и нормативно-правовой базис понятия объекта защиты. Системная модель системы защиты информации объекта защиты (СЗИ). Критерии, определяющие формирование реальных систем защиты информации.

Классификация методов моделирования СЗИ, факторы, определяющие методы моделирования, практические подходы к моделированию СЗИ. Понятие оптимизации средств информацион-

Согласована на портале № 40264

ной безопасности.

Практический анализ объекта защиты, выявление проблемной ситуации и постановка задачи по обеспечению информационной безопасности.

Особенности разработки моделей систем защиты информации объекта вычислительной техники, объекта выделенное помещение, информационной системы персональных данных.Оптимизация средств информационной безопасности объектов защиты.

14.1.4. Темы докладов

Понятие системного подхода, системы, системного анализа, взаимосвязь понятий и их практическое предназначение.

Взаимосвязь понятий элемента, компонента и подсистемы. Понятие «связь». Системное понятие «цель», структура, поведение, жизненный цикл. Виды и формы представления структур. Классификация систем.

Закономерности взаимодействия части и целого, закономерности иерархической упорядоченности, закономерности, осуществимости систем, закономерности развития систем.

Закономерности возникновения и формулирования целей, закономерности формирования структур целей.

Понятие проблемы принятия решения. Подходы к анализу и проектированию систем.

Методы, направленные на активизацию интуиции и опыта специалистов, методы формализованного представления систем, Специальные методы, методики постепенной формализации задачи.

Введение в понятие аналитических, статистических методов, методов дискретной математики, включая теоретико-множественные, логические, лингвистические, семиотические представления.

Законодательный и нормативно-правовой базис понятия объекта защиты. Системная модель объекта защиты. Основные критерии, определяющие формирование реальных объектов защиты.

Законодательный и нормативно-правовой базис понятия объекта защиты. Системная модель системы защиты информации объекта защиты (СЗИ). Критерии, определяющие формирование реальных систем защиты информации.

Классификация методов моделирования СЗИ, факторы, определяющие методы моделирования, практические подходы к моделированию СЗИ. Понятие оптимизации средств информационной безопасности.

Практический анализ объекта защиты, выявление проблемной ситуации и постановка задачи по обеспечению информационной безопасности.

Особенности разработки моделей систем защиты информации объекта вычислительной техники, объекта выделенное помещение, информационной системы персональных данных.Оптимизация средств информационной безопасности объектов защиты.

14.1.5. Вопросы на самоподготовку

Цели, структура и задачи курса. Взаимосвязь курса с другими дисциплинами, системный характер проблем при решении задач по моделированию систем информационной безопасности и оптимизации средств информационной безопасности. Специфика курса.

Понятие системного подхода, системы, системного анализа, взаимосвязь понятий и их практическое предназначение.

Взаимосвязь понятий элемента, компонента и подсистемы. Понятие «связь». Системное понятие «цель», структура, поведение, жизненный цикл. Виды и формы представления структур. Классификация систем.

Закономерности взаимодействия части и целого, закономерности иерархической упорядоченности, закономерности, осуществимости систем, закономерности развития систем.

Закономерности возникновения и формулирования целей, закономерности формирования структур целей.

Понятие проблемы принятия решения. Подходы к анализу и проектированию систем.

Методы, направленные на активизацию интуиции и опыта специалистов, методы формализованного представления систем, Специальные методы, методики постепенной формализации задачи.

Введение в понятие аналитических, статистических методов, методов дискретной математи-

Согласована на портале № 40264

ки, включая теоретико-множественные, логические, лингвистические, семиотические представления.

Законодательный и нормативно-правовой базис понятия объекта защиты. Системная модель объекта защиты. Основные критерии, определяющие формирование реальных объектов защиты.

Законодательный и нормативно-правовой базис понятия объекта защиты. Системная модель системы защиты информации объекта защиты (СЗИ). Критерии, определяющие формирование реальных систем защиты информации.

Классификация методов моделирования СЗИ, факторы, определяющие методы моделирования, практические подходы к моделированию СЗИ. Понятие оптимизации средств информационной безопасности.

Практический анализ объекта защиты, выявление проблемной ситуации и постановка задачи по обеспечению информационной безопасности.

Особенности разработки моделей систем защиты информации объекта вычислительной техники, объекта выделенное помещение, информационной системы персональных данных.Оптимизация средств информационной безопасности объектов защиты.

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.

Согласована на портале № 40264

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 № 40264