МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

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

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

КОМПЛЕКСНЫЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В СЕТЯХ И СИСТЕМАХ СВЯЗИ

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки / специальность: **11.03.02 Инфокоммуникационные технологии и системы связи**
Направленность (профиль) / специализация: **Защищенные системы и сети связи**
Форма обучения: **очная**
Факультет: **Радиотехнический факультет (РТФ)**
Кафедра: **Кафедра радиоэлектроники и систем связи (РСС)**
Курс: **4**
Семестр: **7**
Учебный план набора 2021 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	7 семестр	Всего	Единицы
Лекционные занятия	28	28	часов
Практические занятия	18	18	часов
в т.ч. в форме практической подготовки	18	18	часов
Лабораторные занятия	16	16	часов
в т.ч. в форме практической подготовки	16	16	часов
Курсовая работа	18	18	часов
в т.ч. в форме практической подготовки	18	18	часов
Самостоятельная работа	100	100	часов
Подготовка и сдача экзамена	36	36	часов
Общая трудоемкость (включая промежуточную аттестацию)	216	216	часов
	6	6	з.е.

Формы промежуточной аттестация	Семестр
Экзамен	7
Курсовая работа	7

Томск

1. Общие положения

1.1. Цели дисциплины

1. Целью преподавания дисциплины является формирование у студентов устойчивых основ знаний организации комплексных систем защиты информации в сетях и системах связи и методов ее управления, приобретения при этом необходимых умений и навыков.

1.2. Задачи дисциплины

1. Основными задачами изучения дисциплины являются: – изучение сущности и задач комплексной системы защиты информации (КСЗИ); – изучение принципов организации и этапов разработки КСЗИ, факторов, влияющих на организацию КСЗИ; – определение и нормативное закрепление состава защищаемой информации; – определение объектов защиты; – анализ и оценка угроз безопасности информации: выявление и оценка источников, – способов и результатов дестабилизирующего воздействия на информацию; – определение потенциальных каналов и методов несанкционированного доступа к информации, определение возможностей несанкционированного доступа к защищаемой информации; – определение компонентов и условий функционирования КСЗИ, разработка модели, технологического и организационного построения КСЗИ; – кадровое, материально-техническое и нормативно-методическое обеспечение функционирования КСЗИ; – назначение, структура и содержание управления КСЗИ, изучение принципов и методы планирования, сущности и содержание контроля функционирования КСЗИ; – изучение особенностей управления КСЗИ в условиях чрезвычайных ситуаций; – изучение состава методов и моделей оценки эффективности КСЗИ.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).

Часть блока дисциплин: Часть, формируемая участниками образовательных отношений.

Модуль дисциплин: Модуль направленности (профиля) (major).

Индекс дисциплины: Б1.В.02.11.

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
Универсальные компетенции	
-	-
Общепрофессиональные компетенции	
-	-
Профессиональные компетенции	

ПКР-6. Способен оценивать параметры безопасности и защищать программное обеспечение и сетевые устройства администрируемой сети с помощью специальных средств управления безопасностью	ПКР-6.1. Знает архитектуру, протоколы и общие принципы функционирования аппаратных, программных и программно аппаратных средств администрируемой сети.
	ПКР-6.2. Знает основные принципы, криптографические протоколы и программные средства обеспечения информационной безопасности сетевых устройств.
	ПКР-6.3. Умеет применять программные, аппаратные и программно-аппаратные средства защиты сетевых устройств от несанкционированного доступа.
	ПКР-6.4. Пользоваться нормативно-технической документацией в области обеспечения информационной безопасности инфокоммуникационных систем.
	ПКР-6.5. Владеет навыками и средствами установки и управления специализированными программными средствами защиты сетевых устройств администрируемой сети от несанкционированного доступа.
ПКР-22. Способен проводить расчеты по проекту сетей, сооружений и средств инфокоммуникаций в соответствии с техническим заданием с использованием как стандартных методов, приемов и средств автоматизации проектирования, так и самостоятельно создаваемых оригинальных программ	ПКР-22.1. Знает нормативно-правовые, нормативно-технические и организационно-методические документы, регламентирующие проектную подготовку, внедрение и эксплуатацию систем связи (телекоммуникационных систем), строительство объектов связи.
	ПКР-22.2. Знает принципы построения технического задания при автоматизации проектирования средств и сетей связи и их элементов; структуру и основы подготовки технической и проектной документации.
	ПКР-22.3. Умеет выявлять и анализировать преимущества и недостатки вариантов проектных решений, оценивать риски, связанные с реализацией проекта.
	ПКР-22.4. Владеет навыками сбора исходных данных, необходимых для разработки проектной документации.

4. Названия разделов (тем) дисциплины

Названия разделов (тем) дисциплины
7 семестр
1 Введение.
2 Содержание и этапы проведения работ по организации комплексной системы защиты информации
3 Определение компонентов КСЗИ.
4 Технология определения и классификации состава и защищенности информации.
5 Построение комплексной системы защиты информации.
6 Управление комплексной системой защиты информации
7 Служба защиты информации.
8 Особенности управления КСЗИ в условиях чрезвычайных ситуаций.
9 Состав методов и моделей оценки эффективности КСЗИ
10 Экзамен