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

ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Уровень образования: **высшее образование - магистратура**
Направление подготовки / специальность: **10.04.01 Информационная безопасность**
Направленность (профиль) / специализация: **Информационная безопасность объектов критической информационной инфраструктуры**
Форма обучения: **очная**
Факультет: **Факультет безопасности (ФБ)**
Кафедра: **Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)**
Курс: **2**
Семестр: **3**
Учебный план набора 2023 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	3 семестр	Всего	Единицы
Лекционные занятия	36	36	часов
Практические занятия	36	36	часов
Лабораторные занятия	8	8	часов
Курсовая работа	36	36	часов
Самостоятельная работа	64	64	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	3
Курсовая работа	3

Томск

1. Общие положения

1.1. Цели дисциплины

1. Освоение дисциплинарных компетенций, связанных с созданием и изучением современной защищенных информационных систем различного применения и степени сложности.

2. Обучение принципам и методам защиты информации, комплексного проектирования, построения, обслуживания и анализа защищенных информационных систем, а также содействовать формированию научного мировоззрения и развитию системного мышления.

1.2. Задачи дисциплины

1. Системный анализ прикладной области, выявление угроз и оценка уязвимости информационных систем, разработка требований и критериев оценки информационной безопасности.

2. Обоснование выбора состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов.

3. Разработка систем, комплексов, средств и технологий обеспечения информационной безопасности.

4. Разработка программ и методик испытаний средств и систем обеспечения информационной безопасности.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).

Часть блока дисциплин: Обязательная часть.

Модуль дисциплин: Модуль направления подготовки (hard skills – HS).

Индекс дисциплины: Б1.О.2.4.

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	

ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;	ОПК-1.1. Знает меры (организационные, технические) и технологии обеспечения информационной безопасности
	ОПК-1.2. Знает уязвимости систем и угрозы информационной безопасности
	ОПК-1.3. Знает нормативную базу и ГОСТы, регламентирующие процесс разработки технических заданий на создание систем обеспечения информационной безопасности объектов
	ОПК-1.4. Умеет обосновывать требования к процессам и технологиям обеспечения информационной безопасности
	ОПК-1.5. Умеет осуществлять выбор подсистем, реализующих технологии обеспечения информационной безопасности
	ОПК-1.6. Умеет обосновывать требования к мерам обеспечения информационной безопасности
	ОПК-1.7. Умеет разрабатывать техническое задание на создание подсистемы обеспечения информационной безопасности
	ОПК-1.8. Знает отечественные и зарубежные стандарты в области обеспечения информационной безопасности
	ОПК-1.9. Знает нормативную и правовую базу в области обеспечения информационной безопасности, нормативные методические документы ФСБ России, ФСТЭК России и иных регуляторов в области обеспечения информационной безопасности
	ОПК-1.10. Знает основы управления рисками информационной безопасности
	ОПК-1.11. Умеет оценивать риски информационной безопасности
ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;	ОПК-2.1. Знает принципы организации и этапы разработки системы (подсистемы либо компонента системы) обеспечения информационной безопасности
	ОПК-2.2. Знает средства тестирования системы (подсистемы либо компонента системы) обеспечения информационной безопасности
	ОПК-2.3. Умеет разрабатывать модели угроз и нарушителей информационной безопасности
	ОПК-2.4. Умеет разрабатывать планы и сценарии тестирования системы (подсистемы либо компонента системы) обеспечения информационной безопасности
	ОПК-2.5. Умеет разрабатывать требования к средствам и методам контроля проектируемой системы (подсистемы либо компонента системы) обеспечения информационной безопасности
	ОПК-2.6. Умеет разрабатывать и реализовывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности
Профессиональные компетенции	
-	-

4. Названия разделов (тем) дисциплины

Названия разделов (тем) дисциплины
3 семестр
1 Теоретические вопросы защиты информации и построения информационных систем
2 Проектирование автоматизированных информационных систем
3 Содержание работ на этапах создания автоматизированных информационных систем

4 Способы и методы защиты информации в информационных системах
5 Средства разработки и тестирования автоматизированных информационных систем