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

ВЫЯВЛЕНИЕ ИНЦИДЕНТОВ И ПРОТИВОДЕЙСТВИЕ АТАКАМ НА ОБЪЕКТЫ КИИ

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: **1**
Семестр: **2**
Учебный план набора 2023 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	2 семестр	Всего	Единицы
Лекционные занятия	28	28	часов
Лабораторные занятия	52	52	часов
в т.ч. в форме практической подготовки	36	36	часов
Самостоятельная работа	64	64	часов
Подготовка и сдача экзамена	36	36	часов
Общая трудоемкость	180	180	часов
(включая промежуточную аттестацию)	5	5	з.е.

Формы промежуточной аттестация	Семестр
Экзамен	2

Томск

1. Общие положения

1.1. Цели дисциплины

1. Изучить основные принципы управления инцидентами информационной безопасности.
2. Изучить основы мониторинга инфраструктуры организации, а также формирование знаний о процессах и системах мониторинга.

1.2. Задачи дисциплины

1. Получение студентами знаний о принципах определения событий информационной безопасности (ИБ) как инцидентов ИБ.
2. Получение студентами умений и навыков по оценке и реагированию на идентифицированные инциденты ИБ.
3. Получение студентами знаний об основных методах контроля обеспечения информационной безопасности в организации.
4. Получение студентами умений и навыков нормативному обеспечению управления инцидентами информационной безопасности.
5. Получение студентами умений и навыков планирования, подготовки, использования, анализа и улучшения процесса управления инцидентами информационной безопасности.
6. Получение студентами умений и навыков реагирования на инциденты информационной безопасности.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).

Часть блока дисциплин: Часть, формируемая участниками образовательных отношений.

Модуль дисциплин: Модуль профессиональной подготовки (major).

Индекс дисциплины: Б1.В.1.4.

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	
-	-
Профессиональные компетенции	

ПК-1. Способен обеспечивать анализ, проектирование, разработку, функционирование, эксплуатацию систем информационной безопасности объектов критической информационной инфраструктуры и ее частей;	ПК-1.1. Знает общие принципы проектирования систем информационной безопасности объектов критической информационной инфраструктуры и ее частей, принципы построения систем информационной безопасности объектов критической информационной инфраструктуры и ее частей, состав технико-экономического обоснования проектируемых систем информационной безопасности объектов критической информационной инфраструктуры и ее частей
	ПК-1.2. Умеет разрабатывать необходимую техническую документацию в области проектирования систем информационной безопасности объектов критической информационной инфраструктуры и ее частей с учетом действующих нормативных и методических документов, проводить подготовку исходных данных для технико-экономического обоснования проектируемых систем информационной безопасности объектов критической информационной инфраструктуры и ее частей
	ПК-1.3. Владеет навыками проектирования элементов систем информационной безопасности объектов критической информационной инфраструктуры
ПК-3. Способен разрабатывать организационно-распорядительные документы, регламентирующие функционирование систем информационной безопасности объектов критической информационной инфраструктуры	ПК-3.1. Знает содержание и порядок деятельности персонала по эксплуатации систем информационной безопасности объектов критической информационной инфраструктуры
	ПК-3.2. Знает нормативную базу, регламентирующую процессы проектирования, построения и эксплуатации систем информационной безопасности объектов критической информационной инфраструктуры
	ПК-3.3. Умеет разрабатывать технические задания на создание систем информационной безопасности объектов критической информационной инфраструктуры с учетом действующих нормативных и методических документов
	ПК-3.4. Владеет инструментами проведения и фиксации результатов проверки функционирования систем информационной безопасности объектов критической информационной инфраструктуры
	ПК-3.5. Умеет осуществлять планирование и организацию работы персонала систем информационной безопасности объектов критической информационной инфраструктуры с учетом требований по защите информации.

4. Названия разделов (тем) дисциплины

Названия разделов (тем) дисциплины
2 семестр
1 Нормативная база управления инцидентами информационной безопасности и обеспечение непрерывности бизнеса
2 Управление инцидентами информационной безопасности
3 Процесс управления инцидентами информационной безопасности
4 SIEM-системы