**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

# Техническая защита информации

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки / специальность: **10.03.01 Информационная безопасность**
Направленность (профиль) / специализация: **Безопасность автоматизированных систем**
Форма обучения: **очная**
Факультет: **ФБ, Факультет безопасности**
Кафедра: **КИБЭВС, Кафедра комплексной информационной безопасности электронно-вычислительных систем**
Курс: **4**
Семестр: **7**
Учебный план набора 2020 года

Распределение рабочего времени

| № | Виды учебной деятельности | 7 семестр | Всего | Единицы |
|---|---|---|---|---|
| 1 | Лекции | 28 | 28 | часов |
| 2 | Практические занятия | 16 | 16 | часов |
| 3 | Лабораторные работы | 20 | 20 | часов |
| 4 | Всего аудиторных занятий | 64 | 64 | часов |
| 5 | Самостоятельная работа | 80 | 80 | часов |
| 6 | Всего (без экзамена) | 144 | 144 | часов |
| 7 | Подготовка и сдача экзамена | 36 | 36 | часов |
| 8 | Общая трудоемкость | 180 | 180 | часов |
| | | 5.0 | 5.0 | З.Е. |

Экзамен: 7 семестр

Томск

## 1. Цели и задачи дисциплины

### 1.1. Цели дисциплины

Целью дисциплины «Техническая защита информации» является теоретическая и практическая подготовка студентов:

1) по вопросам защиты информации от утечки по техническим каналам (технической защиты информации) на объектах информатизации и в выделенных помещениях;

2) по вопросам организации и сопровождения аттестации объекта информатизации по требованиям безопасности информации;

3) по вопросам установки, настройки и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

4) по вопросам организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации.

### 1.2. Задачи дисциплины

– Дать основы по выявлению на объекте информатизации или в выделенном помещении технических каналов утечки информации; оценке уровня шумов/информативных сигналов/помех; оценке соответствия объекта информатизации или выделенного помещения требованиям по безопасности от утечки информации по техническим каналам.

## 2. Место дисциплины в структуре ОПОП

Дисциплина «Техническая защита информации» (Б1.Б1.06.06) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Основы информационной безопасности, Управление средствами защиты информации, Физика.

Последующими дисциплинами являются: Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты, Преддипломная практика.

## 3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ОПК-7 способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты ;

– ПК-1 способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации ;

– ПК-5 способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации ;

– ПК-6 способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации ;

В результате изучения дисциплины обучающийся должен:

– **знать** технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, принципы работы программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

– **уметь** анализировать и оценивать угрозы информационной безопасности объекта; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем. пользоваться нормативными документами по защите информации, работать с программными, программно-аппаратными (в том числе криптографическими) и техническими средствами защиты информации;

– **владеть** методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации; методами формирования требований по защите информации; методами расчета и инструментального контроля показателей технической защиты информации, навыками работы в программных, программно-аппаратных (в том числе крип-

тографических) и технических средствах защиты информации.

## 4. Название разделов (тем) дисциплины

| Названия разделов дисциплины |
|---|
| 7 семестр |
| 1 Концепция инженерно-технической защиты информации |
| 2 Теоретические основы инженерно-технической защиты информации |
| 3 Физические основы защиты информации |
| 4 Технические средства добывания и инженерно-технической защиты информации |
| 5 Организационные основы инженерно-технической защиты информации |
| 6 Методическое обеспечение инженерно-технической защиты информации |