

Документ подписан электронной подписью  
Информация о владельце:  
ФИО: Сенченко Павел Васильевич  
Должность: Проректор по учебной работе  
Дата подписания: 22.09.2023 08:37:56  
Уникальный программный ключ:  
27e516f4c088deb62ba68945f4406e13fd454355

**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 - специалитет**

Направление подготовки / специальность: **10.05.02 Информационная безопасность телекоммуникационных систем**

Направленность (профиль) / специализация: **Защита информации в системах связи и управления**

Форма обучения: **очная**

Факультет: **ФБ, Факультет безопасности**

Кафедра: **БИС, Кафедра безопасности информационных систем**

Курс: **4**

Семестр: **7**

Учебный план набора 2016 года

**Распределение рабочего времени**

№	Виды учебной деятельности	7 семестр	Всего	Единицы
1	Лекции	28	28	часов
2	Практические занятия	18	18	часов
3	Лабораторные работы	36	36	часов
4	Всего аудиторных занятий	82	82	часов
5	Из них в интерактивной форме	22	22	часов
6	Самостоятельная работа	26	26	часов
7	Всего (без экзамена)	108	108	часов
8	Подготовка и сдача экзамена	36	36	часов
9	Общая трудоемкость	144	144	часов
		4.0	4.0	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 по вопросам защиты информации от утечки по техническим каналам (технической защиты информации) на объектах информатизации и в выделенных помещениях, по вопросам применения нормативных правовых актов в своей профессиональной деятельности, участия в проведении аттестации телекоммуникационных систем по требованиям защиты информации.

### 1.2. Задачи дисциплины

- Изучение технических каналов утечки информации, их характеристик, способов добытия информации техническими средствами разведки;
- Изучение методики выявления технических каналов утечки информации на объекте информатизации или в выделенном помещении;
- Изучение способов выявления и оценки утечки информации по акустическому/виброакустическому каналу утечки информации;
- Изучение способов выявления и оценки утечки информации по каналу побочных электромагнитных излучений и наводок;
- Изучение методов и технических средств охраны объекта информатизации и выделенного помещения;
- Изучение нормативных документов и методики оценки 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.Б.7) относится к блоку 1 (базовая 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 применять нормативные правовые акты в своей профессиональной деятельности;
- ПК-9 способностью участвовать в проведении аттестации телекоммуникационных систем по требованиям 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.
- **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.
- **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.

## 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