

Документ подписан электронной подписью  
Информация о владельце:  
ФИО: Сенченко Павел Васильевич  
Должность: Проректор по учебной работе  
Дата подписания: 22.09.2023 08:37:57  
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**

**Защита информации в компьютерных сетях**

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: **3**

Семестр: **6**

Учебный план набора 2016 года

**Распределение рабочего времени**

№	Виды учебной деятельности	6 семестр	Всего	Единицы
1	Лекции	28	28	часов
2	Практические занятия	18	18	часов
3	Лабораторные работы	44	44	часов
4	Всего аудиторных занятий	90	90	часов
5	Из них в интерактивной форме	26	26	часов
6	Самостоятельная работа	54	54	часов
7	Всего (без экзамена)	144	144	часов
8	Подготовка и сдача экзамена	36	36	часов
9	Общая трудоемкость	180	180	часов
		5.0	5.0	З.Е.

Экзамен: 6 семестр

Томск

## 1. Цели и задачи дисциплины

### 1.1. Цели дисциплины

Обучить студентов основам построения и эксплуатации вычислительных сетей, принципам и методам защиты информации в компьютерных сетях, навыкам комплексного проектирования, построения, обслуживания и анализа защищенных вычислительных сетей.

### 1.2. Задачи дисциплины

- Дать основы:
- – архитектуры вычислительных сетей;
- – программно-аппаратных и технических средств создания сетей;
- – принципов построения сетей и управления ими;
- – использования программных и аппаратных технологий защиты сетей;
- – методологии проектирования, развертывания и сопровождения безопасных сетей;
- – обследования и анализа защищенных вычислительных сетей.
- 

## 2. Место дисциплины в структуре ОПОП

Дисциплина «Защита информации в компьютерных сетях» (Б1.Б.38.4) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Администрирование сетей ЭВМ, Основы информационной безопасности.

Последующими дисциплинами являются: Распределенные автоматизированные информационные системы.

## 3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ПК-8 способностью проводить анализ эффективности технических и программно-аппаратных средств защиты телекоммуникационных систем;
- ПК-14 способностью выполнять установку, настройку и обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем;
- ПСК-10.5 способностью проводить оценку уровня защищенности и обеспечивать эффективное применение средств защиты информационных ресурсов компьютерных сетей и систем беспроводной связи;

В результате изучения дисциплины обучающийся должен:

- **знать** средства и методы хранения и передачи информации; эталонную модель взаимодействия открытых систем; основные стандарты в области инфокоммуникационных систем и технологий; основные нормативно правовые акты и нормативные методические документы в области инфокоммуникационных систем; принципы построения защищенных телекоммуникационных систем; механизмы реализации атак в компьютерных сетях; защитные механизмы и средства обеспечения сетевой безопасности; средства и методы предотвращения и обнаружения вторжений.

- **уметь** применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты в соответствии с требованиями нормативно правовых актов и нормативных методических документов.

- **владеть** навыками конфигурирования локальных сетей, навыками реализации сетевых протоколов с помощью программных средств; навыками настройки межсетевых экранов; навыками применения нормативно правовых актов и нормативных методических документов в области инфокоммуникационных систем; методикой анализа сетевого трафика; методикой анализа результатов работы средств обнаружения вторжений.

## 4. Название разделов (тем) дисциплины

Названия разделов дисциплины
6 семестр
1 Основные понятия информационной безопасности
2 Технологии обеспечения безопасности в локальных сетях
3 Обеспечение безопасности сетей на базе сетевых операционных систем
4 Обеспечение безопасности межсетевого взаимодействия
5 Правовые основы защиты информации в компьютерных сетях. Защищенный документооборот