

Документ подписан электронной подписью  
Информация о владельце:  
ФИО: Сенченко Павел Васильевич  
Должность: Проректор по учебной работе  
Дата подписания: 22.09.2023 08:37:55  
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**

**Криптографические методы защиты 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: **3**

Семестр: **5**

Учебный план набора 2016 года

**Распределение рабочего времени**

№	Виды учебной деятельности	5 семестр	Всего	Единицы
1	Лекции	36	36	часов
2	Практические занятия	28	28	часов
3	Всего аудиторных занятий	64	64	часов
4	Из них в интерактивной форме	18	18	часов
5	Самостоятельная работа	44	44	часов
6	Всего (без экзамена)	108	108	часов
7	Подготовка и сдача экзамена	36	36	часов
8	Общая трудоемкость	144	144	часов
		4.0	4.0	З.Е.

Экзамен: 5 семестр

Томск

## 1. Цели и задачи дисциплины

### 1.1. Цели дисциплины

Целью дисциплины «Криптографические методы защиты информации» является формирование у студентов общих представлений о криптографических методах защиты информации, о применении криптографических методов защиты информации для решения отдельных задач обеспечения информационной безопасности и об основных принципах, лежащих в основе функционирования криптографических средств защиты информации.

### 1.2. Задачи дисциплины

- дать представление о криптографических методах защиты информации;
- изучить математические основы современной криптографии;
- изучить современные стандарты симметричного шифрования;
- изучить основные криптографические алгоритмы с открытым ключом;
- изучить криптографические функции хеширования;
- сформировать умение применять полученные знания для компьютерной реализации криптографических алгоритмов.

## 2. Место дисциплины в структуре ОПОП

Дисциплина «Криптографические методы защиты информации» (Б1.Б.10) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Алгебра, Геометрия, Дискретная математика, Информатика, Основы информационной безопасности.

Последующими дисциплинами являются: Прикладная криптография.

## 3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ОПК-2 способностью применять соответствующий математический аппарат для решения профессиональных задач;

В результате изучения дисциплины обучающийся должен:

- **знать** основные виды криптографических методов и алгоритмов; принципы построения криптографических алгоритмов и предъявляемые к ним требования; математические основы современной криптографии; криптографические стандарты и их использование в информационных системах; простейшие методы криптоанализа.

- **уметь** эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах; применять простейшие методы криптоанализа.

- **владеть** криптографическими методами и средствами защиты информации; простейшими методами криптоанализа; методами оценки стойкости криптографических алгоритмов.

## 4. Название разделов (тем) дисциплины

Названия разделов дисциплины
5 семестр
1 Основные цели и задачи криптографии
2 Математические основы криптографии
3 Историческая криптография
4 Симметричное шифрование
5 Хеширование
6 Криптография с открытым ключом
7 Электронная подпись
8 Защита индивидуальных заданий