

Документ подписан электронной подписью  
Информация о владельце:  
ФИО: Сенченко Павел Васильевич  
Должность: Проректор по учебной работе  
Дата подписания: 28.09.2023 10:14:32  
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**

**Прикладная криптография**

Уровень образования: **высшее образование - специалитет**

Направление подготовки / специальность: **25.05.03 Техническая эксплуатация транспортного радиооборудования**

Направленность (профиль) / специализация: **Техническая эксплуатация радиоэлектронного оборудования воздушных судов и аэропортов**

Форма обучения: **очная**

Факультет: **РКФ, Радиоконструкторский факультет**

Кафедра: **КИПР, Кафедра конструирования и производства радиоаппаратуры**

Курс: **4**

Семестр: **8**

Учебный план набора 2018 года

**Распределение рабочего времени**

№	Виды учебной деятельности	8 семестр	Всего	Единицы
1	Лекции	28	28	часов
2	Практические занятия	18	18	часов
3	Лабораторные работы	8	8	часов
4	Всего аудиторных занятий	54	54	часов
5	Самостоятельная работа	54	54	часов
6	Всего (без экзамена)	108	108	часов
7	Общая трудоемкость	108	108	часов
		3.0	3.0	З.Е.

Зачёт: 8 семестр

Томск

## 1. Цели и задачи дисциплины

### 1.1. Цели дисциплины

Основная цель дисциплины «Прикладная криптография» — формирование у студентов представлений о практическом использовании криптографических методов защиты информации для решения отдельных задач обеспечения информационной безопасности.

### 1.2. Задачи дисциплины

– сформировать представление об основных проблемах, связанных с практическим использованием криптографических методов защиты информации; изучить основные криптографические протоколы; изучить инфраструктуру открытого ключа.

## 2. Место дисциплины в структуре ОПОП

Дисциплина «Прикладная криптография» (Б1.Б.32) относится к блоку 1 (базовая часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Математика.

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

## 3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– ОПК-6 способностью понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны;

В результате изучения дисциплины обучающийся должен:

– **знать** основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях

– **уметь** эффективно использовать криптографические методы и средства защиты информации в автоматизированных системах

– **владеть** навыками использования типовых криптографических алгоритмов

## 4. Название разделов (тем) дисциплины

Названия разделов дисциплины
8 семестр
1 Криптографические протоколы: общие понятия.
2 Протоколы распределения ключей.
3 Инфраструктура открытого ключа.
4 Протоколы идентификации и аутентификации.
5 Безопасный канал обмена сообщениями.
6 Практические аспекты реализации средств криптографической защиты информации.