

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Сенченко Павел Васильевич  
Должность: Проректор по учебной работе  
Дата подписания: 19.06.2024 23:06:43  
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**

**ОСНОВЫ КРИПТОГРАФИИ**

Уровень образования: **высшее образование - бакалавриат**

Направление подготовки / специальность: **11.03.02 Инфокоммуникационные технологии и системы связи**

Направленность (профиль) / специализация: **Программируемые защищенные системы связи**

Форма обучения: **очная**

Факультет: **Радиотехнический факультет (РТФ)**

Кафедра: **радиоэлектроники и систем связи (РСС)**

Курс: **3**

Семестр: **6**

Учебный план набора 2024 года

**Объем дисциплины и виды учебной деятельности**

Виды учебной деятельности	6 семестр	Всего	Единицы
Лекционные занятия	18	18	часов
Практические занятия	12	12	часов
Лабораторные занятия	16	16	часов
Самостоятельная работа	62	62	часов
Общая трудоемкость	108	108	часов
(включая промежуточную аттестацию)	3	3	з.е.

Формы промежуточной аттестации	Семестр
Зачет	6

## 1. Общие положения

### 1.1. Цели дисциплины

1. Целью дисциплины «Основы криптографии» 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

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

## 2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).

Часть блока дисциплин: Часть, формируемая участниками образовательных отношений.

Модуль дисциплин: Модуль направленности (профиля) (major).

Индекс дисциплины: Б1.В.02.08.

Реализуется с применением электронного обучения, дистанционных образовательных технологий.

## 3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 3.1):

Таблица 3.1 – Компетенции и индикаторы их достижения

Компетенция	Индикаторы достижения компетенции
<b>Универсальные компетенции</b>	
-	-
<b>Общепрофессиональные компетенции</b>	
-	-
<b>Профессиональные компетенции</b>	
ПК-1. Способен выполнять математическое и компьютерное моделирование объектов и процессов инфокоммуникационных сетей и систем по типовым методикам для решения профессиональных задач	ПК-1.1. Знает математическое и компьютерное моделирование объектов и процессов инфокоммуникационных сетей и систем по типовым методикам
	ПК-1.2. Умеет выполнять математическое и компьютерное моделирование объектов и процессов инфокоммуникационных сетей и систем по типовым методикам для решения профессиональных задач
	ПК-1.3. Владеет математическим и компьютерным моделированием объектов и процессов инфокоммуникационных сетей и систем по типовым методикам для решения профессиональных задач

## 4. Названия разделов (тем) дисциплины

Названия разделов (тем) дисциплины
<b>6 семестр</b>

1 Математические основы криптографии
2 Основные цели и задачи криптографии
3 Историческая криптография
4 Симметричное шифрование
5 Хеширование
6 Поточное шифрование
7 ГСПЧ и проверка их качества
8 Криптография с открытым ключом
9 Электронная подпись