

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Смирнов Сергей Николаевич  
Должность: врио ректора  
Дата подписания: 17.10.2023 14:21:13  
Уникальный программный ключ:  
69e375c64f7e975d4e8830e7b4fcc2ad1bf35f08

Министерство науки и высшего образования Российской Федерации  
ФГБОУ ВО «Тверской государственный университет»

Утверждаю:  
Руководитель ООП  
Н.А. Семькина

« 4 » 09



Рабочая программа дисциплины (с аннотацией)

### Теоретико-числовые методы в криптографии

Специальность

**10.05.01 Компьютерная безопасность**

Специализация

**«Математические методы защиты информации»**

Для студентов очной формы обучения

СПЕЦИАЛИТЕТ

Для студентов 3 курса ОФО

Составитель:

Семькина Н. А.

Тверь 2023

## **I. Аннотация**

### **1. Цель и задачи дисциплины**

Цель освоения дисциплины - формирование базы для развития профессиональных компетенций, связанных с готовностью студента к деятельности в области проектирования и построения криптографических систем, предназначенных для решения различных профессиональных, исследовательских и прикладных задач.

**Задачами** освоения дисциплины являются:

- 1) получение базовых знаний и умений, связанных с основными понятиями в сфере теоретико-числовых методов в криптографии;
- 2) изучение общих принципов анализа и назначения различных алгоритмов;
- 3) освоение методологии решений прикладных задачах с помощью теоретико-числовых методов.

### **2. Место дисциплины в структуре ООП**

Данная дисциплина входит в обязательную часть учебного плана, связана с другими дисциплинами образовательной программы: «Алгебра», «Математическая логика и теория алгоритмов», «Языки программирования».

Дисциплины, для которых освоение данной дисциплины необходимо как предшествующее: «Научно-исследовательская работа», «Проектно-технологическая практика», «Преддипломная практика».

**3. Объем дисциплины:** 4 зачетные единицы, 144 академических часов, в том числе:

контактная аудиторная работа: лекции – 34 часов, в т.ч. практическая подготовка – 0 часов;

лабораторные занятия – 34 часов, в т.ч. практическая подготовка – 4 часа;

самостоятельная работа: 76 часа, в том числе контроль 27 часов.

### **4. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы**

Планируемые результаты освоения образовательной программы (формируемые компетенции)	Планируемые результаты обучения по дисциплине
<b>ОПК-8.</b> Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей	<b>ОПК-8.1</b> Применяет основы теории чисел в криптографии и других дисциплинах
<b>ОПК-9.</b> Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития методов защиты информации в	<b>ОПК-9.1</b> Использует криптографические алгоритмы на практике при решении задач криптографическими методами

<p>операционных системах, компьютерных сетях и системах управления базами данных, а также методов и средств защиты информации от утечки по техническим каналам, сетей и систем передачи информации</p>	
<p><b>ОПК-10.</b> Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности</p>	<p><b>ОПК-10.1.</b> Использует методы построения быстрых вычислительных алгоритмов алгебры и теории чисел</p>

**5. Форма промежуточной аттестации и семестр прохождения** – экзамен в 6 семестре.

**6. Язык преподавания** русский.