

**МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ**  
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ**  
**УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**  
**«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»**  
**(РУТ (МИИТ))**

**АННОТАЦИЯ К**  
**РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)**

**Теоретико-числовые методы в криптографии**

Специальность: 10.05.01 – Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе компьютерных систем

Форма обучения: Очная

**Общие сведения о дисциплине (модуле).**

Дисциплина «Теоретико-числовые методы в криптографии» реализует требования федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 100501 «Компьютерная безопасность». Дисциплина «Теоретико-числовые методы в криптографии» относится к числу профессиональных прикладных дисциплин в силу направленности материала по проблемам безопасности и его важности для подготовки специалиста. Целью преподавания дисциплины «Теоретико-числовые методы в криптографии» является изложение слушателям основных принципов и методов защиты информации, комплексного проектирования и анализа защищенных компьютерных систем КС.

Задачами изучения дисциплины являются: понятия и задачи решаемые в криптографии; видах информации, подлежащей шифрованию, о методах криптографического синтеза и анализа; применениях криптографии в решении задач аутентификации, построения систем цифровой подписи; о

методах криптозащиты компьютерных систем и сетей и основных подходах к изучению криптосистем. Основной целью изучения учебной дисциплины «Теоретико-числовые методы в криптографии» является формирование у обучающегося компетенций для научно-исследовательского вида деятельности. Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности): научно-исследовательская деятельность: анализ состояния и динамики объектов деятельности с использованием необходимых методов и средств анализа, моделирование исследуемых явлений или процессов с использованием современных вычислительных машин и систем, а также компьютерных программ; разработка программ и методик испытаний объектов защиты информации, разработка предложений по внедрению результатов научных исследований.

Общая трудоемкость дисциплины (модуля) составляет 4 з.е. (144 академических часа(ов)).