МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Компьютерная безопасность

Направление подготовки: 01.03.02 – Прикладная математика и информатика

Направленность (профиль): Математические модели в экономике и технике

Форма обучения: Очная

Общие сведения о дисциплине (модуле).

В курсе «Компьютерная безопасность» изучаются основные математические методы криптографии. Цель преподавания дисциплины – обеспечить студентам знания в области теоретической криптографии и ее прикладных методов, необходимые для профессиональной деятельности специалистов по компьютерной и информационной безопасности. Компетенции, приобретаемые студентами, применяются для научно-исследовательской деятельности.

Дисциплина предназначена для получения знаний при решении следующих профессиональных задач: алгебраические и теоретико-числовые основы криптографии, криптосистемы RSA, Эль-Гамаля, Рабина, а также криптопротоколы Диффи-Хеллмана, Шнорра, Блюма и некоторые другие. использование частотных характеристик открытых текстов для анализа простейших шифров замены и перестановки, применение стандартов в области криптографических методов информационной безопасности для проектирования, разработки и анализа защищенности информационных

систем, изучение современной литературе по криптографии. В результате освоения дисциплины студент будет владеть криптографическими понятиями, стандартными криптографическими алгоритмами и протоколами, реализуемыми на компьютерах, приёмами математического моделирования в шифровании. владеть знаниями и опытом, связанным с теорией алгебраических чисел (символ Лежандра, символ Якоби, квадратичный закон взаимности Гаусса).

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