

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): Математическое моделирование и системный анализ

Форма обучения: Очная

Общие сведения о дисциплине (модуле).

Целями освоения дисциплины (модуля) являются:

- обеспечить студентов знаниями в области теоретической криптографии и ее прикладных методов, необходимые для профессиональной деятельности специалистов по компьютерной и информационной безопасности;

- приобретение компетенций для научно-исследовательской деятельности.

Задачами дисциплины (модуля) являются:

- формирование личности студента, развитие его интеллекта и умения логически и алгоритмически мыслить, формирование умений и навыков, необходимых при практическом применении приемов математического моделирования;

- формирование навыков решения задач по нижеследующим темам: алгебраические и теоретико-числовые основы криптографии, криптосистемы RSA, Эль-Гамала, 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;

-формирование навыков составления стандартных криптографических алгоритмов и протоколов, реализуемых на компьютерах, приёмов математического моделирования в шифровании, владение 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)).