МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Алгебра

Специальность:	10.05.01 – Компьютерная безопасность
Специализация:	Информационная безопасность объектов информатизации на базе компьютерных систем
Форма обучения:	Очная

Общие сведения о дисциплине (модуле).

Целями освоения учебной дисциплины (модуля) «Алгебра» являются:

- закладка математического фундамента как средства изучения окружающего мира для успешного освоения дисциплин естественнонаучного и профессионального циклов;

- получение студентами основ теоретических знаний и прикладных навыков применения математических методов и моделей;

- подготовка к использованию этих методов для разработки и принятия эффективных организационных и управленческих решений;

- развитие логического мышления и повышение общего уровня культуры студентов.

Задачами освоения учебной дисциплины "Алгебра" являются:

-формирование прочной теоретической базы в области абстрактной и линейной алгебры, необходимой для понимания математических основ криптографии, теории кодирования и защиты информации.

- освоение фундаментальных алгебраических структур, таких как группы, кольца, поля, векторные пространства и конечные поля (поля Галуа), которые лежат в основе современных криптографических алгоритмов и протоколов.

- развитие навыков работы с матрицами, определителями, системами линейных уравнений, что необходимо при анализе и построении линейных кодов, шифров и методов защиты данных.

- изучение методов решения алгебраических задач, включая задачи факторизации, нахождения обратных элементов, вычисления дискретных логарифмов и работы с полиномами над конечными полями — ключевых компонентов асимметричной криптографии.

- подготовка к изучению специальных дисциплин, таких как криптография, теория чисел, теория информации, дискретная математика и безопасность компьютерных систем, где алгебраические методы играют центральную роль.

- формирование строгого логического и абстрактного мышления, позволяющего анализировать и проектировать надежные криптографические примитивы и протоколы обеспечения безопасности.

- освоение математического аппарата для анализа устойчивости криптосистем к атакам, включая алгебраические атаки на симметричные и асимметричные шифры.

- развитие навыков формального доказательства и строгого обоснования алгоритмов, что критически важно при верификации корректности и безопасности программных и аппаратных реализаций криптографических систем.

Общая трудоемкость дисциплины (модуля) составляет 9 з.е. (324 академических часа(ов).