

ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА
10.05.03 – Информационная безопасность автоматизированных систем

Аннотация рабочей программы
дисциплины «Математика криптографии»

Общая трудоемкость дисциплины составляет 6 зач. единиц, 216 часов, форма промежуточной аттестации – экзамен.

Программой дисциплины предусмотрены следующие виды занятий: лекционные – 54 часа, практические – 18 часов, лабораторные – 36 часов, самостоятельная работа обучающегося составляет 108 часов.

Дисциплина подразумевает изучение следующих основных разделов:

Линейные пространства и подпространства. Базис пространства. Евклидовы пространства. Порождающая и проверочная матрица

Основы теории конечных полей. Арифметические операции в конечном поле.

Различные формы алгоритма Евклида и линейного представления наибольшего общего делителя двух чисел. Алгоритм Евклида в кольце Z_n . Вычисление обратного элемента. Решение сравнений. Кольцо многочленов над полем. Поле $Z(p^n)$. Арифметика поля.

Теоретико-числовые методы криптографии. Методы: проверки чисел на простоту; генерации простых чисел; факторизации чисел. Дискретный логарифм.

Методы генерации и тестирования псевдослучайных последовательностей.