Аннотация к рабочей программе дисциплины

« Алгебра и теория чисел»

Цель преподавания дисциплины

Цель преподавания дисциплины – формирование у студентов основных представлений о важнейших разделах алгебры и теории чисел, а также подготовка студентов к использованию полученных знаний в методах и алгоритмах криптографии и криптологии.

Задачи изучения дисциплины

Задачи преподавания дисциплины – ознакомление студентов с рядом методов, свойств и утверждений алгебры и теории чисел, которые лежат в основе некоторых разделов криптографии и криптологии.

Выпускник по направлению подготовки должен овладеть основными понятиями и методами:

- аксиоматического задания алгебраических объектов: групп, колец и полей,
- проверки соответствия данной структуры определенным требованиям,
- методами теории чисел,
- методами решения задач линейной алгебры,
- методами решения сравнений и систем сравнений в кольце целых чисел.

Компетенции, формируемые в результате освоения дисциплины

ОПК-2 способностью применять в профессиональной деятельности знания математических основ информатики.

Разделы дисциплины

1. Введение и предмет курса.
2. Теорема деления с остатком. Делимость и её свойства. Простые числа.
3. Каноническое представление целых чисел. НОД.

4. Взаимно простые числа и их свойства. НОК. Свойства НОК, НОД.

5. Сравнения и их свойства. Системы сравнений первой степени.

6. Сравнения второй степени. Непрерывные дроби.

7. Группы, кольца, поля. Их свойства.

8. Элементы теории многочленов.

9. Эллиптические кривые над полем. Точки эллиптической кривой и их свойства.

10. Эллиптические кривые над конечными полями. Действия над точками эллиптической кривой.