АННОТАЦИЯ рабочей программы дисциплины
«Б1.В.ДВ.04.01 Теоретико-числовые методы криптографии»

Направление подготовки/специальность 01.04.01 Математика

Объем трудоемкости: 3 зач. ед.

Цель дисциплины:
Цель освоения дисциплины – знакомство с задачами и методами защиты информации математическими методами. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук. Ее значение возрастает в свете ведущейся информационной войны против Российской Федерации.

Задачи дисциплины:
Получение базовых теоретических и исторических сведений о структуре и алгоритмах функционирования криптоалгоритмов. Применение этих знаний на практике, при рассмотрении перспектив развития математических и компьютерных наук, месте и роли защиты информации в структуре информатизации и математических методов построения защищенных информационных систем.
Изучение теоретических основ предмета: Числовые функции, основные теоремы о евклидовых кольцах, алгоритмы решения линейных и квадратных уравнений в конечных полях, кольцах вычетов, алгоритмы нахождения наибольших общих делителей, алгоритмов проверки простоты чисел.
Системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов;
Алгебраических и теоретико-числовых принципов синтеза и анализа шифров;
Математических методов, используемых в криптоанализе и криптографии.

Место дисциплины в структуре ООП ВО
Дисциплина «Теоретико-числовые методы криптографии» относится к вариативной части блока Б1 Дисциплины (модули) и является дисциплиной по выбору.
Данная дисциплина, как математическая основа криптографии, критоанализа, теории защищенных информационных систем, призвана содействовать фундаментализации образования, укреплению правосознания и развитию системного мышления магистров.

Требования к уровню освоения дисциплины
Процесс изучения дисциплины направлен на формирование следующих компетенций: ПК-1, ПК-3.

Основные разделы дисциплины:
Модели шифров.
Мультипликативные функции.
Табличное и модульное гаммирование.
Построение больших простых чисел.

Курсовые работы: не предусмотрены.

Форма проведения аттестации по дисциплине: зачет

Автор РПД, д.ф.-м.н., профессор Рожков А.В.