

АННОТАЦИЯ рабочей программы дисциплины «Б1.О.32.02 Теоретико-числовые методы криптографии»

Направление подготовки/специальность 01.05.01 Фундаментальные математика и механика

Объем трудоемкости: 3 зач. ед.

Цель освоения дисциплины:

Цель освоения дисциплины – рассматривает задачи защиты информации математическими методами. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук.

Задачи дисциплины:

Задачи освоения дисциплины «Теоретико-числовые методы криптографии»: 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.

Место дисциплины в структуре ООП ВО:

Дисциплина «Теоретико-числовые методы криптографии» относится к обязательной части Блока 1 "Дисциплины (модули)" учебного плана и является одной из основных дисциплин в освоении математических знаний. Дисциплина «Теоретико-числовые методы криптографии» читается в 6 семестре.

Требования к уровню освоения дисциплины

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций: ОПК-1, ОПК-3.

Основные разделы дисциплины:

Разделы дисциплины, изучаемые в 6 семестре: Модели шифров; Мультипликативные функции; Табличное и модульное гаммирование; Построение больших простых чисел.

Курсовые работы: предусмотрена

Форма проведения аттестации по дисциплине: зачет

Автор доктор физ.-мат.наук, профессор Рожков А.В.