АННОТАЦИЯ рабочей программы дисциплины
«Б1.В.ДВ.02.02 Криптография и основы защиты информации»

Направление подготовки/специальность 01.03.01 Математика, «Математическое моделирование»

Объем трудоемкости: 4 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 систем кодирования и криптосистем. 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: коды исправляющие ошибки, коды сжатия информации как текстовой, так и мультимедийной. Математические и теоретико-числовые основы теории кодирования и криптологии.
Обучение системному подходу к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения кодирующих и криптографических средств.

Место дисциплины в структуре ООП ВО
Дисциплина «Теория кодирования и защита информации» относится к части, формируемой участниками образовательных отношений блока Б1, и является дисциплиной по выбору. Курс «Теория кодирования и защита информации» продолжает начатое ранее обучение студентов по направлению математика и компьютерные науки. Знания, полученные в этом курсе, могут быть использованы в курсах защита операционных систем и баз данных, криптография, организационно-правовые методы защиты информации и др. Слушатели должны владеть знаниями в рамках программы курсов «Алгебра», «Дискретная математика», «Математический анализ».

Требования к уровню освоения дисциплины
Процесс изучения дисциплины направлен на формирование следующих компетенций: ПК-1, ПК-4.

Основные разделы дисциплины:
Понятие о компьютерной алгебре. Пакеты компьютерной алгебры. Пакеты на открытом коде. Структуры данных в компьютерной алгебре. Техника символьных вычислений. Модели шифров. Блочные и поточные шифры. Понятие криптосистемы. Поточные шифры. Синронизированные и самосинхронизующиеся. Надежность шифров.

Курсовые работы: не предусмотрены.

Форма проведения аттестации по дисциплине: экзамен

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