

АННОТАЦИЯ рабочей программы дисциплины «Б1.В.ДВ.02.01 Компьютерная алгебра и криптография»

Направление подготовки/специальность 01.03.01 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:

Задачи освоения дисциплины «Компьютерная алгебра и криптография»: 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 и получение сведений:

- о компьютерной реализации информационных объектов;
- связи компьютерной алгебры и численного анализа;
- элементы теории сложности алгоритмов;
- об основных задачах и понятиях криптографии;
- об этапах развития криптографии;
- о видах информации, подлежащей шифрованию;
- о классификации шифров;
- о методах криптографического синтеза и анализа;
- о применениях криптографии в решении задач аутентификации, построения систем цифровой подписи;
- о методах криптозащиты компьютерных систем и сетей.

Место дисциплины в структуре ООП ВО

Дисциплина «Компьютерная алгебра и криптография» относится к части, формируемой участниками образовательных отношений блока Б1 и является дисциплиной по выбору.

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. Синхронизированные и самосинхронизирующиеся. Надежность шифров.

Курсовые работы: не предусмотрена

Форма проведения аттестации по дисциплине: экзамен

Автор РПД

Рожков А.В., д-р физ.-мат. наук, профессор.