

АННОТАЦИЯ рабочей программы дисциплины «Б1.В.06 Криптографические методы защиты информации»

Направление подготовки/специальность 01.04.01 Математика

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:

Задачи освоения дисциплины «Криптографические методы защиты информации»: 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 нормативных требованиях по административно-правовому регулированию в области криптографической защиты информации;
- 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 «Криптографические методы защиты информации» относится к вариативной части блока Б1 Дисциплины (модули) и является обязательной дисциплиной.

Данная дисциплина, как математическая основа 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-4, ПК-5.

Основные разделы дисциплины:

Модели шифров. Блочные и поточные шифры. Понятие криптосистемы.
Поточные шифры. Синхронизированные и самосинхронизирующиеся. Надежность шифров.
Принципы построения криптографических алгоритмов с симметричными и несимметричными ключами
Системы шифрования с открытыми ключами

Курсовые работы: предусмотрена.

Форма проведения аттестации по дисциплине: зачет

Автор РПД

Рожков А.В.