АННОТАЦИЯ рабочей программы дисциплины
«Б1.В.ДВ.09.01 Эллиптические кривые и электронная подпись»

Направление подготовки: 02.03.01 Математика и компьютерные науки

Объем трудоемкости: 2 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 «Эллиптические кривые и электронная подпись»: 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;
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 «Эллиптические кривые и электронная подпись» относится к части, формируемой участниками образовательных отношений блока Б1, и является дисциплиной по выбору.
Данная дисциплина, как математическая основа теории защищенных информационных систем, призвана содействовать фундаментализации образования, укреплению правосознания и развитию системного мышления студентов.

Требования к уровню освоения дисциплины
Процесс изучения дисциплины направлен на формирование следующих компетенций: ПК-1, ПК-5.

Основные разделы дисциплины:
Об основных задачах и понятиях криптографии; о классификации шифров; о нормативно-правовых основах защиты информации
Эллиптические кривые над конечными полями и алгоритмы вычисления на них.
Табличное и модульное гаммирование.
Построение больших простых чисел.

Курсовые работы: не предусмотрены.

Форма проведения аттестации по дисциплине: зачет

Автор РПД Рожков А.В.