АННОТАЦИЯ рабочей программы дисциплины
«Б1.В.ДВ.04.01 Эллиптическая кривая и электронная подпись»

Направление подготовки/специальность 01.05.01 Фундаментальные математика и механика

Объем трудоемкости: 3 зач. ед.

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

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 «Эллиптическая кривая и электронная подпись» относится к части, формируемой участниками образовательных отношений Блока 1 "Дисциплины (модули)" учебного плана Б1.В.ДВ.04.01.
Курс «Эллиптическая кривая и электронная подпись» продолжает, начатое на трех курсах математическое образование и студентов соответствующего направления подготовки. 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», «Программирование», «Информатика», «Правоведение».

Требования к уровню освоения дисциплины
Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций: ПК-2.

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