АННОТАЦИЯ
дисциплины «ЭЛЛИПТИЧЕСКАЯ КРИВАЯ И ЭЛЕКТРОННАЯ ПОДПИСЬ»

Объем трудоемкости: 3 зачетные единицы (108 часов, из них – 60,2 часа контактной работы (28 часа лекций, 28 часа лабораторных занятий, 4 часа КСР, 0,2 часа ИКР); 47,8 часа самостоятельной работы).

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 «Эллиптическая кривая 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 вариативной части Блока 1 «Дисциплины (модули)» учебного плана 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:

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1.	ОПК-4	способность находить, анализировать, реализовывать программно и использовать на' практике математические алгоритмы, в том числе с применением современных вычислительных систем	содержание основных понятий по правовому обеспечению информационной безопасности; правовые способы	отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законода-	использования библиотеки алгоритмов и пакетов расширения; поиска и использования современной

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
2	ПК-3	Способностью создавать и исследовать новые математические модели явлений реального мира, сред, тел и конструкций	защиты государственной тайны	тельства, в том числе с помощью систем правовой информации	научно-технической литературой в области символьных вычислений.

Основные разделы дисциплины:

№	Наименование раздела	Содержание раздела
1	2	3
1	Об основных задачах и понятиях криптографии; о нормативно-правовых основах защиты информации.	Линейные рекуррентные последовательности ЛРП над полем. Характеристический многочлен и начальный вектор ЛРП. о нормативно-правовых основах защиты информации. О методах криптографического синтеза и анализа; о применениях криптографии в решении задач аутентификации, о методах криптографического синтеза и анализа. о классификации шифров; построения систем цифровой подписи.
2	Эллиптические кривые над конечными полями и алгоритмы вычисления на них.	Приведение кривой к каноническому виду. Вычисления числа точек на эллиптической кривой. Сложение точек. Нахождение порядков точек. Нахождение порождающих точек эллиптической кривой.
3	Табличное и модульное гаммирование.	Случайные и псевдослучайные гаммы. Регистры сдвига с обратной связью Криптограммы, полученные при повторном использовании ключа. Анализ криптограмм, полученных применением неравновероятной гаммы.
4	Построение больших простых чисел.	Алгоритмы проверки на простоту. Эллиптические кривые над конечными полями и алгоритмы вычисления на них. Электронная подпись.

Курсовые работы: не предусмотрены.
Форма проведения аттестации по дисциплине: зачет
Основная литература:

1. Рябко Б.Я, Фионов А.Н. Криптографические методы защиты информации [Электронный ресурс]. – М.: Горячая линия-Телеком, 2012. - URL: https://e.lanbook.com/book/5193
2. Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В. Введение в теоретико-числовые методы криптографии. [Электронный ресурс]. - СПб.: Лань, 2011. - URL: https://e.lanbook.com/book/68466

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