АННОТАЦИЯ
Дисциплины Б1.В.ДВ.04.01
«ЭЛЛИПТИЧЕСКАЯ КРИВАЯ И ЭЛЕКТРОННАЯ ПОДПИСЬ»

Объем трудоемкости: 3 зачетные единицы (108 ч., из них 70,2 контактных – лекционных 32 ч., лабораторные занятия 34 ч., 4 ч. КСР, 0,2 ИКР) 37,8 ч. самостоятельной работы.

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

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.	ПК-2	Способен активно участвовать в исследовании новых математических моделей в естественных	содержание основных понятий по правовому обеспечению информаци-	отыскивать необходимые нормативные правовые акты и информационно-правовые нормы	использования библиотеки алгоритмов и пакетов расширения; поиска и использования со-

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
		науках	онной безопасности; правовые способы защиты государственной тайны	в системе действующего законодательства, в том числе с помощью систем правовой информации	временной научно-технической литературой в области символьных вычислений.

Основные разделы дисциплины:

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1	Об основных задачах и понятиях криптографии; о классификации шифров; о нормативно-правовых основах защиты информации	24	6		8	10
2	Эллиптические кривые над конечными полями и алгоритмы вычисления на них.	26	8		8	10
3	Табличное и модульное гаммирование.	28	8		10	10
4	Построение больших простых чисел.	23,8	8		8	7,8
	Итого по дисциплине:		**32**		**34**	**37,8**

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/reader/book/5193/#1
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/reader/book/68466/#1

Автор РПД Рожков А.В.