Аннотация к рабочей программы дисциплины
«Б1.В.ДВ.04.01 Эллиптическая кривая и электронная подпись»
(код и наименование дисциплины)

Объем трудоемкости: 2 зачетных единицы

Цель дисциплины: рассмотрение задач информатизации и программно-аппаратных основ кодирования информации. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук

Задачи дисциплины: Получение базовых теоретических и практических сведений и навыков о структуре и алгоритмах кодирования информации. Получение базовых теоретических и исторических сведений о структуре информатизации, ее развитии, применении этих знаний на практике, перспектив развития математических и компьютерных наук, месте и роли защиты информации в структуре информатизации.

Место дисциплины в структуре образовательной программы

Дисциплина «Эллиптическая кривая и электронная подпись» относится к части, определяемой участниками образовательных отношений Блока 1 "Дисциплины (модули)" учебного плана и является дисциплиной по выбору Б1.В.ДВ. 04.01.

Данная дисциплина, как алгоритмическая основа криптографии, призвана содействовать фундаментализации образования, укреплению правосознания и развитию системного мышления студентов. А также развитию навыков применения современных компьютерных средств для решения естественно-научных проблем.

Требования к уровню освоения дисциплины

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
ПК-2 Способен активно участвовать в исследовании новых математических моделей в естественных науках	
ПК-2.1 Умеет использовать математические модели и применять численные методы решения задач в естественных науках ПК-2.2 Разрабатывает новые математические модели в естественных науках	Знать: основные педагогические методы и идеи Уметь: выделять сущности и связи предметной области; Владеть навыками: работы с педагогической литературой и коллективом учащихся .

Содержание дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 7 семестре *(очная форма)*

№	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.	14	2		4	8
2	Эллиптические кривые над конечными полями и алгоритмы вычисления на них.	16	2		4	10

3	Табличное и модульное гаммирование.	14	2		4	8
4	Построение больших простых чисел.	22,8	4		6	12,8
	Итого по дисциплине:		10		18	39,8
	Контроль самостоятельной работы (КСР)	4				
	Промежуточная аттестация (ИКР)	0,2				
	Подготовка к текущему контролю					
	Общая трудоемкость по дисциплине	72				

Курсовые работы: не предусмотрена
Форма проведения аттестации по дисциплине: зачет

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