Аннотация к рабочей программы дисциплины

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

Объем трудоемкости: 2 зачетных единицы
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 «Эллиптическая кривая и электронная подпись»: 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, формируемой участниками образовательных отношений Блока 1 "Дисциплины (модули)" учебного плана В соответствии с рабочим учебным планом дисциплина изучается на 5 курсе по очной форме обучения. Вид промежуточной аттестации: зачет (9 семестр).

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 ПК-2.3 Владеет навыками математической обработки результатов экспериментальных исследований составленных математических моделей	Знать: об основных задачах и понятиях криптографии; о классификации шифров; о методах криптографического синтеза и анализа; о применениях криптографии в решении задач аутентификации, построения систем цифровой подписи; Уметь использовать: типовые шифры замены и перестановки; частотные характеристики языков и их использование в криптоанализе; требования к шифрам и основные характеристики шифров; принципы построения современных шифрсистем: Владеть: криптографической терминологией; навыками использования основных типов шифров и криптографических алгоритмов; методами криптоанализа простейших шифров:

Содержание дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
Разделы (темы) дисциплины, изучаемые в 9семестре (очная форма обучения*)*

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
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.	23,8	4		8	11,8
	ИТОГО по разделам дисциплины		10	-	20	37,8
	Контроль самостоятельной работы (КСР)	4	-	-	-	-
	Промежуточная аттестация (ИКР)	0.2	-	-	=	-
	Подготовка к промежуточному контролю		-	-	-	-
	Общая трудоемкость по дисциплине (3 семестр)	72	10	-	20	37,8

Курсовые работы: не предусмотрены.
Форма проведения аттестации по дисциплине: зачет (9 семестр)

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