Аннотация к рабочей программы дисциплины

ФТД.01. Экспериментальная теория чисел

(код и наименование дисциплины)

Объем трудоемкости: 2 зачетные единицы

Цель дисциплины: задачи информатизации и научного программирования. 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 символьных математических вычислений. Прежде всего алгебраических, связанных с вычислительными и числовыми вопросами алгебры и криптографии. Применение этих знаний на практике, при рассмотрении перспектив развития математических и компьютерных наук, месте и роли вычислительных приемов и методов, при решении вопросов защиты информации. А также при анализе структур информационных систем и математических методов построения защищенных информационных систем.

Место дисциплины в структуре образовательной программы

Дисциплина экспериментальная теория чисел относится к факультативной части учебного плана ФТД.01.

Данная дисциплина, как алгоритмическая основа криптографии, криптоанализа, теории защищенных информационных систем, призвана содействовать фундаментализации образования, укреплению правосознания и развитию системного мышления магистров. 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-4 Способен ориентироваться в современных алгоритмах компьютерной математики; обладать способностями к эффективному применению и реализации математически сложных алгоритмов в современных программных комплексах	
ПК-4.1 Умеет применять и реализовывать математически сложные алгоритмы в современных программных комплексах ПК-4.2 Применяет в профессиональной деятельности методику исследования и создания новых моделей, методов и технологий в математике и естественных науках ПК-4.3 Демонстрирует умение отбора среди существующих методов наиболее подходящие для решения конкретной прикладной задачи	Знать: 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; 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: типовые поточные и блочные шифры, системы шифрования с открытыми ключами, криптографические протоколы; постановки задач криптоанализа и подходы к их решению; Владеть: криптографической терминологией; навыками использования основных типов шифров и криптографических алгоритмов; методами криптоанализа простейших шифров: навыками математического моделирования в криптографии; современной научно-технической литературой в области криптографической защиты.

Содержание дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1.	Понятие о компьютерной алгебре. Пакеты компьютерной алгебры. Пакеты на открытом коде.	14	4	4		6
2.	Структуры данных в компьютерной алгебре. Техника символьных вычислений.	18	4	4		10
3.	LISP-машины. Целочисленная арифметика. Полиномиальная арифметика.	18	4	4		10
4.	Редукция алгебраических выражений. Метод критических пар. Алгоритм Евклида. Простые числа. Тесты простоты. Разложение чисел на простые числа.	21,8	4	4		13,8
5.	***Итого по дисциплине:***		**16**	**16**		**39,8**
	Контроль самостоятельной работы (КСР)	-				
	Промежуточная аттестация (ИКР)	0,2				
	Подготовка к текущему контролю	10,8				
	Общая трудоемкость по дисциплине	72				

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

Автор А.В. Рожков, профессор, д.ф.-м.н.