Аннотация к рабочей программы дисциплины

Б1.В.ДВ.04.01. Теоретико-числовые методы криптографии

(код и наименование дисциплины)

Объем трудоемкости: 3 зачетные единицы

Цель дисциплины: задачи информатизации и защиты информации средствами классической криптографии и теории чисел. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук.

Задачи дисциплины: 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.

Место дисциплины в структуре образовательной программы

Дисциплина теоретико-числовые методы криптографии относится к части, формируемой участниками образовательных отношений Блока 1 "Дисциплины (модули)" учебного плана и является дисциплиной по выбору Б1.В.ДВ.04.01.

Данная дисциплина, как математическая основа криптографии, критоанализа, теории защищенных информационных систем, призвана содействовать фундаментализации образования, укреплению правосознания и развитию системного мышления магистров.

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-1 Способен формулировать и решать актуальные и значимые задачи фундаментальной и прикладной математики	
ПК-1.1 Знает основные понятия, идеи и методы фундаментальных математических дисциплин для решения базовых задач ПК-1.2 Умеет передавать результаты проведенных теоретических и прикладных исследований в виде конкретных предметных рекомендаций в терминах предметной области ПК-1.3 Самостоятельно и корректно решает стандартные задачи фундаментальной и прикладной математики ПК-1.4 Имеет навыки решения математических задач, соответствующих квалификации, возникающих при проведении научных и прикладных исследований	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;

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
	основные математические методы, используемые в анализе типовых криптографических алгоритмов. Владеть: криптографической терминологией; навыками использования основных типов шифров и криптографических алгоритмов; методами криптоанализа простейших шифров: современной научно-технической литературой в области криптографической защиты.
ПК-3 Способен публично представлять собственные и известные научные результаты	
ПК-3.1 Структурирует и представляет результаты научно-исследовательских работ ПК-3.2 Анализирует и обобщает результаты математических доказательств, сформулированных научных утверждений ПК-3.3 Осуществляет сбор научной информации, участвует в научных дискуссиях, готовит обзоры, составляет рефераты, отчеты, выступает с докладами и сообщениями	Знать: О компьютерной реализации информационных объектов. Связи компьютерной алгебры и численного анализа. Элементы теории сложности алгоритмов. Уметь: Определять структуры данных в компьютерной алгебре. Использовать технику символьных вычислений. Применять основные математические методы, используемые в анализе типовых криптографических алгоритмов. Владеть навыками: классификации систем компьютерной алгебры;

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.	Модели шифров.	28	4		4	20
2.	Мультипликативные функции.	37	4		4	29
3.	Табличное и модульное гаммирование.	23.8	4		4	15,8
4.	Построение больших простых чисел.	19	4		4	11
5.	*Итого по дисциплине:*		16		16	75,8
	Контроль самостоятельной работы (КСР)	-				
	Промежуточная аттестация (ИКР)	0,2				
	Подготовка к текущему контролю	12,8				
	Общая трудоемкость по дисциплине	72				

Курсовые работы: не предусмотрены

Форма проведения аттестации по дисциплине: зачет

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