Аннотация дисциплины

Б1.В.02 Теоретико-числовые методы криптографии

(код и наименование дисциплины)

Объем трудоемкости: 3 зачетные единицы.

Цель дисциплины – рассматривает задачи защиты информации математическими методами. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук.

Задачи дисциплины теоретико-числовые методы криптографии: 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: числовые функции, основные теоремы о евклидовых кольцах, алгоритмы решения линейных и квадратных уравнений в конечных полях, кольцах вычетов, алгоритмы нахождения наибольших общих делителей, алгоритмов проверки простоты чисел;

системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов; алгебраических и теоретико-числовых принципов синтеза и анализа шифров; математических методов, используемых в криптоанализе и криптографии.

Место дисциплины в структуре образовательной программы

Дисциплина Теоретико-числовые методы криптографии относится к части, формируемой участниками образовательных отношений дополнительной части Блока 1 "Дисциплины (модули)" учебного плана Б1.В.02.

Знания, полученные в этом курсе, могут быть использованы в ходе практик, в других компьютерных дисциплинах. Слушатели должны владеть знаниями в рамках программы курсов «Алгебра», «Математический анализ», «Технология программирования и работа на электронно-вычислительной машине (ЭВМ)».

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

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	Знать: о целях, задачах, принципах и основных направлениях обеспечения информационной безопасности государства; о методологии создания систем защиты информации; Уметь: выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; Владеть: анализом информационной инфраструктуры государства; формальной постановкой и решением задачи обеспечения информационной безопасности компьютерных систем.

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
исследований	
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; о нормативно-правовых основах защиты информации; Уметь использовать: типовые шифры замены и перестановки; принципы построения современных шифрсистем: основные математические методы, используемые в анализе типовых криптографических алгоритмов. Владеть: криптографической терминологией; навыками использования основных типов шифров и криптографических алгоритмов; методами криптоанализа простейших шифров: навыками математического моделирования в криптографии

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.	Виды информации и основные методы ее защиты. Национальные интересы РФ в информационной сфере и их обеспечение. Виды угроз ИБ РФ.	24	4		8	12
2.	Организационно-правовые методы защиты информации	28	4		6	18
3.	Программно-аппаратные методы защиты информации	24	4		10	10
4.	Электронная Россия, электронный документооборот, универсальная электронная карта	27.8	6		10	11,8
	ИТОГО по разделам дисциплины		18		34	51,8
	Контроль самостоятельной работы (КСР)	4				
	Промежуточная аттестация (ИКР)	0,2				
	Подготовка к текущему контролю					
	Общая трудоемкость по дисциплине	108				

Курсовые работы: не предусмотрены

Форма проведения аттестации по дисциплине: зачет

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