Аннотация к рабочей программы дисциплины
«Б1.В.ДВ.02.01 КОМПЬЮТЕРНАЯ АЛГЕБРА И КРИПТОГРАФИЯ»

Объем трудоемкости: 4 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 «Компьютерная алгебра и криптография»: 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 «Компьютерная алгебра и криптография» относится к части, формируемой участниками образовательных отношений Блока 1 "Дисциплины (модули)" учебного плана.

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 решать актуальные и важные 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-1.4 Имеет навыки решения математических задач, соответствующих квалификации, возникающих при проведении научных и прикладных исследований	Знать: О компьютерной реализации информационных объектов. Связи компьютерной алгебры и численного анализа Уметь: Применять основные математические методы, используемые в анализе типовых алгоритмов Владеть навыками: использования библиотеки алгоритмов и пакетов расширения; поиска и использования современной научно-технической литературой в области символьных вычислений.
ПК-4 Способен разрабатывать программное обеспечение для решения прикладных задач в сфере профессиональной деятельности	
ПК-4.1 Имеет навыки использования современных языков программирования для разработки программного обеспечения ПК-4.4 Ориентируется в современных алгоритмах компьютерной математики и имеет практический опыт разработки программных модулей на основе математических моделей	Знать: О компьютерной реализации информационных объектов. Связи компьютерной алгебры и численного анализа. 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; Уметь: Определять структуры данных в

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
	компьютерной алгебре. использовать технику символьных вычислений. требования к шифрам и основные характеристики шифров; принципы построения современных шифрсистем. Владеть: классификации систем компьютерной алгебры; ориентироваться в типовых архитектурах вычислительных процессов; использования библиотеки алгоритмов и пакетов расширения; криптографической терминологией

Содержание дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1	Понятие о компьютерной алгебре. Пакеты компьютерной алгебры. Пакеты на открытом коде.	22	4		8	10
2	Структуры данных в компьютерной алгебре. Техника символьных вычислений.	22	4		8	10
3	Модели шифров. Блочные и поточные шифры. Понятие криптосистемы.	22	4		8	10
4	Поточные шифры. Синронизированные и самосинхронизующиеся. Надежность шифров.	38	4		10	24
	Итого по разделам дисциплины:	104	16		34	54
	Контроль самостоятельной работы (КСР)	4				
	Промежуточная аттестация (ИКР)	0,3				
	Подготовка к текущему контролю	35,7				
	Общая трудоемкость по дисциплине	144				

Курсовые работы: не предусмотрена

Форма проведения аттестации по дисциплине: экзамен

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