

Аннотация  
дисциплины Б1.В.ДВ.04.01 компьютерная алгебра и криптография  
(код и наименование дисциплины)

**Объем трудоемкости:** 4 зачетные единицы

**Цель освоения дисциплины** – знакомство с задачами и методами защиты информации математическими методами. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук. Ее значение возрастает в свете ведущейся информационной войны против Российской Федерации.

**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.

Изучение теоретических основ предмета и получение сведений:  
о компьютерной реализации информационных объектов;  
связи компьютерной алгебры и численного анализа;  
элементы теории сложности алгоритмов;  
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.

**Место дисциплины в структуре ООП ВО**

Дисциплина Компьютерная алгебра и криптография относится к вариативной части, формируемой участниками образовательных отношений Блока 1 "Дисциплины (модули)" учебного плана дисциплина по выбору Б1.В.ДВ.04.01.

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

**Требования к уровню освоения дисциплины**

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
<b>ПК-1</b> Способен демонстрировать базовые знания математических и естественных наук, основ программирования и информационных технологий	
ПК-1.1 Способен решать актуальные и важные задачи фундаментальной и прикладной математики ПК-1.2 Демонстрирует навыки программирования подготовленных алгоритмов решения вычислительных задач, разработки структуры и программирования реляционных баз данных, а также экспертных систем ПК-1.4 Собирает и анализирует научно-техническую информацию с учетом ба-	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.

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
зовых представлений, полученных в области фундаментальной математики, механики, естественных наук, программирования и информационных технологий	
<b>ПК-5</b> Способен использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования	
<p>ПК-5.1 Анализирует поставленные задачи и выбирает эффективные математические методы при создании алгоритмов и вычислительных программ для решения современных задач математики и механики</p> <p>ПК-5.2 Описывает математические модели, формулирует, теоретически обосновывает и реализует программно численные методы для решения поставленных задач</p> <p>ПК-5.3 Применяет в профессиональной деятельности методику исследования и создания новых моделей, методов и технологий в математике, механике и естественных науках</p>	<p>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;</p> <p>Уметь: Определять структуры данных в компьютерной алгебре. использовать технику символьных вычислений. требования к шифрам и основные характеристики шифров; принципы построения современных шифрсистем.</p> <p>Владеть: классификации систем компьютерной алгебры; ориентироваться в типовых архитектурах вычислительных процессов; использования библиотеки алгоритмов и пакетов расширения; криптографической терминологией</p>

### 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	
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.	29	4		8	17
4.	Поточные шифры. Синхронизированные и самосинхронизирующиеся. Надежность шифров.	30	6		10	14
5.	<i>Итого по дисциплине:</i>		18		34	51
	Контроль самостоятельной работы (КСР)	14				
	Промежуточная аттестация (ИКР)	0,2				
	Подготовка к текущему контролю	12,8				
	Общая трудоемкость по дисциплине	144				

**Курсовые работы:** предусмотрены

**Форма проведения аттестации по дисциплине:** зачет

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