

## Аннотация

### дисциплины Б1.В.ДВ.09.02 Теория кодирования и защиты информации

(код и наименование дисциплины)

**Объем трудоемкости:** 2 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 дисциплины** получение базовых теоретических и исторических сведений о структуре и алгоритмах функционирования систем кодирования и криптосистем. 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: коды исправляющие ошибки, коды сжатия информации как текстовой так и мультимедийной. Математические и теоретико-числовые основы теории кодирования и криптологии.

Обучение системному подходу к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения кодирующих и криптографических средств.

#### **Место дисциплины в структуре ООП ВО**

Дисциплина Теория кодирования и защита информации относится к вариативной части, формируемой участниками образовательных отношений Блока 1 "Дисциплины (модули)" учебного плана дисциплина по выбору Б1.В.ДВ.09.02.

Курс Теория кодирования и защита информации продолжает, начатое ранее обучение студентов по направлению математика и компьютерные науки. Знания, полученные в этом курсе, могут быть использованы в курсах защита операционных систем и баз данных, криптография, организационно-правовые методы защиты информации и др. Слушатели должны владеть знаниями в рамках программы курсов «Алгебра», «Дискретная математика», «Математический анализ».

#### **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 базовых представлений, полученных в области фундаментальной математики, механики, естественных наук, программирования и информационных технологий	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))
<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: об основных задачах и понятиях теории кодов; о видах информации, подлежащей кодированию; о классификации кодов; о методах защиты компьютерных систем и сетей.</p> <p>Уметь использовать: коды с одной проверкой на четность; линейные коды; циклические коды; групповые коды. Коды Хэмминга; коды Боуза-Чоудхури-Хоквингема; основные математические методы, используемые в анализе типовых алгоритмов.</p> <p>Владеть: алгоритмами решения систем линейных уравнений по разным модулям; методами построения генераторов псевдослучайных последовательностей; алгоритмами построения кодов, исправляющих ошибки;</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.	Основные понятия и определения теории кодирования.	16	2		4	10
2.	Свойства энтропии. Теорема Шеннона для кодирования в двоичном симметричном канале связи с шумом.	19	3		6	10
3.	Алгебраические методы в теории кодов.	16	2		4	10
4.	Теория кодов и криптография.	16,8	3		6	7,8
5.	<i>Итого по дисциплине:</i>		10		20	37,8
	Контроль самостоятельной работы (КСР)	4				
	Промежуточная аттестация (ИКР)	0,2				
	Подготовка к текущему контролю	16,8				
	Общая трудоемкость по дисциплине	72				

**Курсовые работы:** не предусмотрены

**Форма проведения аттестации по дисциплине:** зачет

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