АННОТАЦИЯ

дисциплины Б1.В.ДВ.01.02 криптография и защита информации

(код и наименование дисциплины)

Объем трудоемкости: 2 зачетные единицы

Цель освоения дисциплины.

Цель освоения дисциплины – рассмотрение задач информатизации и программно-аппаратных основ кодирования информации. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук.

Задачи дисциплины.

Задачи освоения дисциплины криптография и защита информации: Получение базовых теоретических и практических сведений и навыков о структуре и алгоритмах кодирования информации. Математических основ анализа каналов связи с шумом. Основ теории кодов, исправляющих ошибки. Основ теории информации. Прежде всего алгебраических, связанных с вычислительными и числовыми вопросами алгебры и криптографии. Применение этих знаний на практике, при рассмотрении перспектив развития математических и компьютерных наук, месте и роли вычислительных приемов и методов, при решении вопросов защиты информации.

Изучение теоретических основ предмета: Информационные объекты. Компьютерная алгебра и численный анализ информационных систем. Коды Хэмминга. Теория информации по Шеннону. Алгоритмы кодирования информации жестких и съемных дисков.

Место дисциплины (модуля) в структуре образовательной программы.

Дисциплина криптография и защита информации относится к части, определяемой участниками образовательных отношений Блока 1 "Дисциплины (модули)" учебного плана и является дисциплиной по выбору Б1.В.ДВ.01.02.

Данная дисциплина, как алгоритмическая основа криптографии, призвана содействовать фундаментализации образования, укреплению правосознания и развитию системного мышления студентов. А также развитию навыков применения современных компьютерных средств для решения естественно-научных проблем.

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-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-4.2 Знает стандартные решения, библиотеки программных модулей, шаблоны, классы объектов, используемые при разработке прикладного программного обеспечения. ПК-4.3 Применяет методы и средства проектирования программного обеспечения, структур данных, баз данных, программных интерфейсов ПК-4.4 Ориентируется в современных алгоритмах компьютерной математики и имеет практический опыт разработки программных модулей на основе механико-математических моделей	Знать: об основных задачах и понятиях криптографии; о видах информации, подлежащей кодированию; о классификации шифров; о методах защиты компьютерных систем и сетей. Уметь использовать: шифры; линейные коды; циклические коды; основные математические методы, используемые в анализе типовых алгоритмов. Владеть: алгоритмами решение систем линейных уравнений по разным модулям; методами построения генераторов псевдослучайных последовательностей; алгоритмами построения шифров

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
ПК-4.5 Способен внедрять результаты математических исследований и разработок прикладного программного обеспечения в соответствии с установленными требованиями	

Содержание дисциплины.

Распределение трудоёмкости дисциплины по видам работ.

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.	Основные понятия и определения теории кодирования.	16	4		4	8
2.	Свойства энтропии. Теорема Шеннона для кодирования в двоичном симметричном канале связи с шумом.	16	4		4	8
3.	Алгебраические методы в теории кодов.	16	4		4	8
4.	Теория кодов и криптография.	19.8	4		6	9.8
	ИТОГО по разделам дисциплины		16		18	33.8
	Контроль самостоятельной работы (КСР)	4				
	Промежуточная аттестация (ИКР)	0,2				
	Подготовка к текущему контролю	9,8				
	Общая трудоемкость по дисциплине	72				

Курсовые работы: не предусмотрены

Форма проведения аттестации по дисциплине: зачет

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