

АННОТАЦИЯ

дисциплины Б1. В. ДВ. 01.02 КРИПТОГРАФИЯ И ЗАЩИТА ИНФОРМАЦИИ

для специальности 01.05.01 *Фундаментальные математика и механика*

Объем трудоемкости: 2 зачетные единицы (72 часа, из них 38,2 часа контактной работы (34 часа лабораторных занятий, 4 ч. КСР, 0,2 ч. ИКР); 33,8 часов самостоятельной работы).

Цель освоения дисциплины.

Целями освоения дисциплины «Криптография и защита информации» являются: использование компьютерных технологий (пакетов) при изучении алгебры, овладение аппаратом символического вычисления в алгебре и смежных дисциплинах и их дальнейших приложений.

Задачи дисциплины.

При освоении дисциплины «Криптография и защита информации» вырабатывается общематематическая культура: умение логически мыслить, проводить доказательства основных утверждений, устанавливать логические связи между понятиями, переводить задачи и их решения на язык символических вычислений. Записывать коды и получать решения задач на компьютере. Применять полученные знания для решения геометрических задач и задач, связанных с приложениями теоретико-числовых и алгебраических методов.

Место дисциплины 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

Требования к уровню освоения дисциплины

Изучение данной учебной дисциплины направлено на формирование у обучающихся компетенций ПК-4.

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	владеть
1.	ПК-4	Способен ориентироваться в современных алгоритмах компьютерной математики; обладать способностями к эффективному применению и реализации математически сложных алгоритмов в современных программных комплексах	О компьютерной реализации информационных объектов. Связи компьютерной алгебры и численного анализа.	Применять основные математические методы, используемые в анализе типовых алгоритмов.	использования библиотеки алгоритмов и пакетов расширения; поиска и использования современной научной технической литературы в области символических вычислений.

Основные разделы дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
Разделы дисциплины, изучаемые в 7 семестре (*очная форма*)

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1	Основные понятия и определения теории кодирования.	16			8	8
2	Свойства энтропии. Теорема Шеннона для кодирования в двоичном симметричном канале связи с шумом.	16			8	8
3	Алгебраические методы в теории кодов.	16			8	8
4	Теория кодов и криптография.	19.8			10	9.8
	<i>Итого по дисциплине:</i>				34	33.8

Курсовые работы: *не предусмотрены*

Форма проведения аттестации по дисциплине: *зачет*

Основная литература:

1. Нестеров С.А. Основы информационной безопасности, 4-е изд. [Электронный ресурс]. - СПб.: Лань, 2018. – URL. <https://e.lanbook.com/reader/book/103908/#1>
2. Торстейнсон П., Ганеш Г.А. Криптография и безопасность в технологии .NET. 3-е изд. [Электронный ресурс]. – М.: Лаборатория знаний, 2015. – URL: <https://e.lanbook.com/reader/book/70724/#1>

Автор РПД: профессор Рожков А. В.