

АННОТАЦИЯ
дисциплины «Б1.В.ДВ.09.02 ТЕОРЕТИКО-ГРУППОВЫЕ МОДЕЛИ В КОДИРОВАНИИ
И ЗАЩИТЕ ИНФОРМАЦИИ»

Объем трудоемкости: 3 зачетные единицы (108 часа, из них – 68,2 часа контактной работы (32 часа лекций, 32 часа лабораторных занятий, 11 часов КСР, 0,2 часа ИКР); 32,8 часа самостоятельной работы).

Цель дисциплины: 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:

Задачи освоения дисциплины «Теоретико-групповые модели в кодировании и защите информации»: 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;

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 «Теоретико-групповые модели в кодировании и защите информации» относится к вариативной части блока Б1 Дисциплины и модули и является дисциплиной по выбору.

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

Требования к уровню освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	владеть
1.	ОПК-2	Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных	О компьютерной реализации информационных объектов. Связи компьютерной алгебры и	Определять структуру данных в компьютерной алгебре. использовать технику	навыками использования основных типов шифров и криптографических алгоритмов; методами криптоанализа простейших

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	владеть
2.	ОПК-4	технологий и с учетом основных требований информационной безопасности Способность находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем	численного анализа. Элементы теории сложности алгоритмов. об основных задачах и понятиях криптографии и об этапах развития криптографии и	символьных вычислений. требования к шифрам и основные характеристики шифров; принципы построения современных шифрсистем.	шифров: навыками математического моделирования в криптографии; современной научно-технической литературой в области криптографической защиты.
3	ПК-4	способностью публично представлять собственные и известные научные результаты			

Основные разделы дисциплины:

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	
1	2	3	4	5	6	7
1	Теоретико-числовые конструкции в теории защиты информации и теории кодов	26	8		8	10
2	Основы алгебраической теории кодов	22	8		8	6
3	Теоретико-числовые модели защищенных информационных систем	24	8		8	8
4	Поточные шифры. Синхронизированные и самосинхронизирующиеся. Надежность шифров.	18,8	8		8	8,8
	<i>Итого по дисциплине:</i>		32		32	32,8

Курсовые работы: предусмотрена.

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/book/103908>
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/book/70724/#1>

Автор РПД доктор физ.-мат. наук, профессор

Рожков А.В.