АННОТАЦИЯ
дисциплины «Б1.В.ДВ.04.02 ТЕОРЕТИКО-ГРУППОВЫЕ МОДЕЛИ В КОДИРОВАНИИ И ЗАЩИТЕ ИНФОРМАЦИИ»

Объем трудоемкости: 3 зачетные единицы (108 часа, из них – 79,2 часа контактной работы (34 часа лекций, 34 часа лабораторных занятий, 11 часов КСР, 0,2 часа ИКР); 28,8 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 части, формируемой участниками образовательных отношений блока Б1 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.	ПК-1	Способен демонстрировать базовые знания математических и естественных наук, основ программирования и информацион-	О компьютерной реализации информационных объектов. Связи компьютерной алгебры и чис-	Определять структуры данных в компьютерной алгебре. использовать технику символьных вычислений.	навыками использования основных типов шифров и криптографических алгоритмов; методами криптоанализа простейших шифров:

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
		ных технологий	ленного анализа. Элементы теории сложности алгоритмов. об основных задачах и понятиях криптографии об этапах развития криптографии	требования к шифрам и основные характеристики шифров; принципы построения современных шифрсистем.	навыками математического моделирования в криптографии; современной научно-технической литературой в области криптографической защиты..
2.	ПК-5	Способен использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования			

Основные разделы дисциплины:

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1	Теоретико-числовые конструкции в теории защиты информации и теории кодов	24	8		8	8
2	Основы алгебраической теории кодов	24	8		10	6
3	Теоретико-числовые модели защищенных информационных систем	26	10		8	8
4	Поточные шифры. Синронизированные и самосинхронизующиеся. Надежность шифров.	22,8	8		8	6,8
	Итого по дисциплине:		**34**		**34**	**28,8**

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/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 Рожков А.В.