АННОТАЦИЯ

дисциплины **Б1.В.ДВ.09.02 «Теоретико-групповые модели в кодировании и защите информации»**

Объем трудоемкости: 3 зачетные единицы (108 ч., из них 75,2 контактной работы: 64 ч. аудиторной нагрузки: лекционных 32 ч., лабораторные занятия 32 ч., 11 ч. КСР, 0,2 ИКР; 32,8 ч. 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 профессиональному циклу (Б1) к курсам естественно-научного содержания (Б1.В.ДВ.09.02).

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 библиографи-	О компью-терной реализации информационных объектов.	Определять структуры данных в компью-	навыками использования основных типов шифров и криптографических ал-

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
2.	ОПК-4	ческой культуры с применением информационно-коммуникационных 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	Связи компьютерной алгебры и численного анализа. Элементы теории сложности алгоритмов. об основных задачах и понятиях криптографии об этапах развития криптографии	терной алгебре. использовать технику символьных вычислений. требования к шифрам и основные характеристики шифров; принципы построения современных шифрсистем.	горитмов; методами криптоанализа простейших 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	СРС
1	2	3	4	5	6	7
1	Теоретико-числовые конструкции в теории защиты информации и теории кодов	26	8		8	11
2	Основы алгебраической теории кодов	28	8		8	6
3	Теоретико-числовые модели защищенных информационных систем	28	8		8	6
4	Поточные шифры. Синронизированные и самосинхронизующиеся. Надежность шифров.	26	8		8	10
	Итого по дисциплине:		32		32	33

Курсовые работы: предусмотрены.

Форма проведения аттестации по дисциплине: зачет

Основная литература:

1. Малышев И.А. Компьютерная алгебра. Курс лекций. [Электронный ресурс]. - СПб.:

СПбГПУ (НИУ), 2014. URL: http:// kspt.ftk.spbstu.ru/course/comp-algebra .
2. Нестеров С.А. Основы информационной безопасности, 3-е изд. [Электронный ресурс]. - СПб.: Лань, 2017. - https://e.lanbook.com/book/90153?category_pk=1537 ./
3. Рябко Б.Я, Фионов А.Н. Основы современной криптографии и стеганографии [Электронный ресурс]. – М.: Горячая линия-Телеком, 2011. - URL: http://e.lanbook.com/view/book/5192

Автор РПД Рожков А.В.