АННОТАЦИЯ
дисциплины «Б1.В.ДВ.08.01 КОМПЬЮТЕРНАЯ АЛГЕБРА И КРИПТОГРАФИЯ»

Объем трудоемкости: 4 зачетные единицы (144 часа, из них – 74,3 часа контактной работы (36 часов лекций, 36 часов лабораторных занятий, 2 часа КСР, 0,3 часа ИКР); 34 час самостоятельной работы, 35,7 часа контроль).

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 «Компьютерная алгебра и криптография»: 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;

элементы теории сложности алгоритмов;

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 «Компьютерная алгебра и криптография» относится к вариативной части Блока 1 «Дисциплины (модули)» учебного плана и является дисциплиной по выбору (Б1.В.ДВ.08.01).

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

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. 2.	ОПК-3	способностью к самостоятельной научно-исследовательской работе.	О компьютерной реализации информационных объектов. Связи компьютерной ал-	Определять структуры данных в компьютерной алгебре. использовать технику символьных вычислений.	навыками использования основных типов шифров и криптографических алгоритмов; методами криптоанализа про-

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
3.	ПК-3 ПК-4	способностью строго доказать утверждение, сформулировать результат, увидеть следствия полученного результата Способностью публично представлять собственные и известные научные результаты	гебры и численного 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.	стейших шифров: навыками математического моделирования в криптографии; современной научно-технической литературой в области криптографической защиты..

Основные разделы дисциплины:

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1	Понятие о компьютерной алгебре. Пакеты компьютерной алгебры. Пакеты на открытом коде.	24	8		8	8
2	Структуры данных в компьютерной алгебре. Техника символьных вычислений.	28	10		10	8
3	Модели шифров. Блочные и поточные шифры. Понятие криптосистемы.	26	8		8	10
4	Поточные шифры. Синронизированные и самосинхронизующиеся. Надежность шифров.	27,7	10		10	7,7
	Итого по дисциплине:		36		36	35,7

Курсовые работы: не предусмотрены.

Форма проведения аттестации по дисциплине: экзамен

1. 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

2. Рябко Б.Я, Фионов А.Н. Основы современной криптографии и стеганографии, 2-е изд. [Электронный ресурс]. – М.: Горячая линия-Телеком, 2013. - URL: https://e.lanbook.com/book/63244

Автор РПД доктор физ.-мат. наук, профессор Рожков А.В.