АННОТАЦИЯ
дисциплины «Б1.В.ДВ.03.01 ЛИНЕЙНЫЕ РЕГИСТРЫ СДВИГА
С ОБРАТНОЙ СВЯЗЬЮ»

Объем трудоемкости: 2 зачетные единицы (72 часа, из них – 40,2 часа контактной работы (26 часов лекций, 14 лабораторных занятий, 0,2 часа ИКР); 31,8 часов 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 «Линейные регистры сдвига с обратной связью»: получение базовых теоретических и исторических сведений о структуре и алгоритмах функционирования криптоалгоритмов, алгоритмов создания псевдослучайных последовательностей. 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:

Изучение теоретических основ предмета и получение сведений:

об основных задачах и понятиях теории кодирования;

об этапах развития теории кодирования информации;

о классификации псевдослучайных последовательностей;

об алгебраических методах построения псевдослучайных последовательностей;

теории полей Галуа;

неприводимых многочленах над полями Галуа;

характеристических многочленах линейных сдвигов с обратной связью.

Место дисциплины в структуре ООП ВО

Дисциплина «Линейные регистры сдвига с обратной связью» 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 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.	ПК-1	Способен формулировать и решать актуальные и значимые задачи фундаментальной и прикладной математики	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 научно-технической литературой в области символьных вычислений.

Основные разделы дисциплины:

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1	Линейные рекуррентные последовательности. Свойства периодичности		8		4	8
2	Регистры сдвига с обратной связью. Производящие функции.		8		4	8
3	Семейства линейных рекуррентных последовательностей.		6		4	8
4	Приложения конечных полей Линейные коды Циклические коды. Поточные шифры.		4		2	7,8
	Итого по дисциплине:		**26**		**14**	**31,8**

Курсовые работы: не предусмотрены.

Форма проведения аттестации по дисциплине: зачет

Основная литература:

1. 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
2. Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра, 2-е изд. [Электронный ресурс]. - СПб.: Лань, 2015. - URL: https://e.lanbook.com/book/67458

Дополнительная литература:

1. Смолин Ю.Н. Алгебра и теория чисел, 4-е изд. [Электронный ресурс]. – М.: ФЛИНТА, 2012. URL: https://e.lanbook.com/book/20243
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

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля).

1. Пакет компьютерной алгебры Sage 8.9 Официальный сайт http://sagemath.org/
2. Пакет компьютерной алгебры Gap4r10p2. Официальный сайт http://www.gap-system.org/

Автор РПД. д.ф.-м.н., профессор Рожков А.В.