Аннотация к рабочей программы дисциплины

Б1.В.ДВ.03.01 Линейные регистры сдвига с обратной связью

(код и наименование дисциплины)

Объем трудоемкости: 2 зачетные единицы

Цель дисциплины: задачи алгебраических основ математических методов защиты информации. Изучение этой дисциплины является важной составной частью современного математического образования и образования в области компьютерных наук.

Задачи дисциплины: 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.

Место дисциплины в структуре образовательной программы

Дисциплина Линейные регистры сдвига с обратной связью относится к части, формируемой участниками образовательных отношений Блока 1 "Дисциплины (модули)" учебного плана и является дисциплиной по выбору Б1.В.ДВ.03.01.

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

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
ПК-1 Способен формулировать и решать актуальные и значимые задачи фундаментальной и прикладной математики	
ПК-1.1 Знает основные понятия, идеи и методы фундаментальных математических дисциплин для решения базовых задач ПК-1.2 Умеет передавать результаты проведенных теоретических и прикладных исследований в виде конкретных предметных рекомендаций в терминах предметной области ПК-1.3 Самостоятельно и корректно решает стандартные задачи фундаментальной и прикладной математики ПК-1.4 Имеет навыки решения математических задач, соответствующих квалификации, возникающих при проведении научных и прикладных исследований	Знать: об основных задачах и понятиях теории кодирования и криптографии; о структуре полей Галуа; о матричных характеристиках регистров сдвигов с обратной связью; о методах применения регистров сдвигов в криптографии; о методах работы с характеристическими многочленами регистров сдвигов; Уметь использовать: Методы вычислений в полях Галуа; пакеты компьютерной алгебры на открытом коде; основные математические методы, используемые в анализе псевдослучайных последовательностей. Владеть: Терминологией и приемами работы с дискретными объектами и полями Галуа; криптографической терминологией; навыками математического моделирования в криптографии и теории кодирования; современной научно-технической литературой в области компьютерной алгебры.

Содержание дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1.	Линейные рекуррентные последовательности. Свойства периодичности	14	2		4	8
2.	Регистры сдвига с обратной связью. Производящие функции.	16	4		2	10
3.	Семейства линейных рекуррентных последовательностей.	16	2		4	10
4.	Приложения конечных полей Линейные коды. Циклические коды. Поточные шифры.	25.8	4		4	17,8
5.	***Итого по дисциплине:***		**12**		**14**	**45,8**
	Контроль самостоятельной работы (КСР)	-				
	Промежуточная аттестация (ИКР)	0,2				
	Подготовка к текущему контролю	16,8				
	Общая трудоемкость по дисциплине	72				

Курсовые работы: не предусмотрены
Форма проведения аттестации по дисциплине: зачет

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