Аннотация к рабочей программе дисциплины
«Б1.В.ДВ.03.01 ЛИНЕЙНЫЕ РЕГИСТРЫ СДВИГА
С ОБРАТНОЙ СВЯЗЬЮ»
(код и наименование дисциплины)

Объем трудоемкости: _2__ зачетные единицы

Цель дисциплины:_ изучение 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 полученных 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 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 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. Курс «Линейные регистры сдвига с обратной связью» продолжает алгебраическое образование студентов, начатое в дисциплинах «Теоретико-числовые методы криптографии», «Алгоритмические проблемы алгебры», «Компьютерная алгебра». Полученные знания необходимы для освоения дисциплин «Помехоустойчивое кодирование», « Алгебраическая теория кодов».

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
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	В результате изучения учебной дисциплины обучающийся знает основные понятия, идеи и методы изучаемой дисциплины, применяемые для решения задач фундаментальной и прикладной математики
	В результате изучения учебной дисциплины обучающийся умеет применять основные понятия, идеи и методы изучаемой

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине
	дисциплины для решения задач фундаментальной и прикладной математики
	В результате изучения учебной дисциплины обучающийся владеет методами решения актуальных и важных задач фундаментальной и прикладной математики
ПК-1.2. Умеет передавать результаты проведенных теоретических и прикладных исследований в виде конкретных предметных рекомендаций в терминах предметной области	В результате изучения учебной дисциплины обучающийся знает методы анализа и обработки проведенных теоретических и прикладных исследований в виде конкретных предметных рекомендаций в терминах предметной области
	В результате изучения учебной дисциплины обучающийся умеет передавать результаты проведенных теоретических и прикладных исследований в виде конкретных предметных рекомендаций в терминах предметной области
	В результате изучения учебной дисциплины обучающийся владеет методами анализа и обработки проведенных теоретических и прикладных исследований в виде конкретных предметных рекомендаций в терминах предметной области

Содержание дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины:

Виды работ	Всего часов	Форма обучения
		очная
		II семестр (часы)
Контактная работа, в том числе:	**26,2**	**26,2**
Аудиторные занятия (всего):	**26**	**26**
занятия лекционного типа	12	12
лабораторные занятия	14	14
практические занятия		
семинарские занятия		
Иная контактная работа:		
Контроль самостоятельной работы (КСР)		
Промежуточная аттестация (ИКР)	0,2	0,2
Самостоятельная работа, в том числе:	**45,8**	**45,8**
Курсовая работа/проект (КР/КП) (подготовка)		
Контрольная работа	15	15

Расчётно-графическая работа (РГР) (подготовка)			
Реферат/эссе (подготовка)		10	10
Самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиумам и т.д.)		15	15
Подготовка к текущему контролю		5,8	5,8
Контроль:			
Подготовка к экзамену			
Общая трудоемкость	**час.**	**72**	**72**
	в том числе контактная работа	**26,,2**	**26,,2**
	зач. ед	**2**	**2**

Курсовые работы: не предусмотрены

Форма проведения аттестации по дисциплине: зачет

Автор Н.А. Наумова, докт.техн. наук, доцент