МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет математики и компьютерных наук

УТВЕРЖДАЮ:
Проректор по учебной работе,
качеству образования – первый
проректор
_____ Т.А. Хагуров
подпись
«26» мая 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.03.01 ЛИНЕЙНЫЕ РЕГИСТРЫ СДВИГА С ОБРАТНОЙ СВЯЗЬЮ

Направление подготовки 01.04.01 Математика

Направленность (профиль) Алгебраические методы защиты информации,

Форма обучения очная

Квалификация магистр

Краснодар 2023

Рабочая программа дисциплины Линейные регистры сдвига с обратной связью составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 01.04.01 Математика

Программу составили:
Н.А. Наумова, докт.техн. наук, доцент _____
подпись

Рабочая программа дисциплины «Линейные регистры сдвига с обратной связью» утверждена на заседании кафедры (разработчика) функционального анализа и алгебры
протокол № 8 «18» апреля 2023 г.

Заведующий кафедрой (разработчика) Барсукова В.Ю. _____
фамилия, инициалы подпись

Утверждена на заседании учебно-методической комиссии факультета
протокол № 3 « 20 » апреля 2023 г.
Председатель УМК факультета Шмалько С.П. _____
фамилия, инициалы подпись

Рецензенты:

Пригодина А.Г., кандидат педагогическиз наук, доцент кафедры высшей математики КубГТУ
Марковский А.Н., кандидат физико-математических наук, доцент кафедры математического моделирования КубГУ

1 Цели и задачи изучения дисциплины

1.1 Цель освоения дисциплины

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

1.2 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 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.

1.3 Место дисциплины (модуля) 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».

1.4 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

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 дисциплины для решения задач фундаментальной и прикладной математики
	В результате изучения учебной дисциплины обучаю-

	щийся 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

Результаты обучения по дисциплине достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

2 Структура и содержание дисциплины

2.1 Распределение трудоемкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 2 зачетные единицы (72 часа), их распределение по видам работ представлено в таблице

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, подго-	15	15

товка к лабораторным и практическим занятиям, коллоквиумам и т.д.)			
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**

2.2 Содержание дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
Разделы (темы) дисциплины, изучаемые во **втором** семестре:

.

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛЗ	СРС
1.	Линейные рекуррентные последовательности. Свойства периодичности	15	2		3	10
2.	Регистры сдвига с обратной связью. Производящие функции	18	4		4	10
3.	Семейства линейных рекуррентных последовательностей	15	2		3	10
4.	Приложения конечных полей Линейные коды Циклические коды. Поточные шифры	18	4		4	10
	ИТОГО по разделам дисциплины	66	12		14	40
	Контроль самостоятельной работы (КСР)					
	Промежуточная аттестация (ИКР)	0,2				
	Подготовка к текущему контролю	5,8				
	Общая трудоемкость по дисциплине	72				

2.3 Содержание разделов (тем) дисциплины

2.3.1 Занятия лекционного типа

№	Наименование раздела (темы)	Содержание раздела (темы)	Форма текущего контроля
1	Линейные рекуррентные последовательности. Свойства периодичности	Импульсная функция. Характеристический многочлен. Минимальный период однородной линейной рекуррентной последовательности над конечным полем. Минимальный период последовательности и порядок ее матрицы, как элемента общей линейной группы. Характеристический многочлен. Явная формула n□го члена рекуррентной последовательности. Связь со следом элемента алгебраического расширения поля. Связь порядка характеристического многочлена и минимального периода импульсной функции.	К, Р
2	Регистры сдвига с обратной связью. Производящие функции.	Определение производящей функции. Использование алгебраического аппарата формальных степенных рядов. Формальные степенные ряды над конечным полем. Кольцо формальных рядов, как кольцо без делителей нуля, Э содержащее кольцо много-	К, Р

		членов как подкольцо. Мультипликативная группа кольца формальных рядов. Характеристический многочлен регистра. Возвратный характеристический многочлен регистра сдвига и их связь с производящей функцией регистра	
3	Семейства линейных рекуррентных последовательностей	Методы получения случайных и псевдослучайных последовательностей. Регистры сдвига с обратной связью. Линейный конгруэнтный метод. Мультиплексорные последовательности. Вопросы периодичности и распределения элементов в псевдослучайных последовательностях. Связь между качеством последовательностей, полученных с помощью нелинейных регистров сдвига и характеристиками функции усложнения. Применения дискретных функций для усложнения последовательностей	К, Р
4	Приложения конечных полей Линейные коды Циклические коды. Поточные шифры.	Линейные коды. Расстояние Хэмминга.Вес Хэмминга. Расстояние Хэмминга является метрикой. Коды исправляющие ошибки. Декодирование линейных кодов. Циклические коды. Поточный шифры. Шифр А5. Шифрование трафика мобильной связи.	К, Р

2.3.2 Занятия семинарского типа (практические / семинарские занятия/ лабораторные работы)

№	Наименование раздела (темы)	Тематика занятий/работ	Форма текущего контроля
1	Линейные рекуррентные последовательности. Свойства периодичности	Характеристический многочлен. Минимальный период однородной линейной рекуррентной последовательности над конечным полем.	Проверка домашнего задания
2	Линейные рекуррентные последовательности. Свойства периодичности	Связь порядка характеристического многочлена и минимального периода импульсной функции	Проверка домашнего задания
3	Линейные рекуррентные последовательности. Свойства периодичности	Явная формула n-го члена рекуррентной последовательности. Связь со следом элемента алгебраического расширения поля	Проверка домашнего задания. Контрольная работа
4	Регистры сдвига с обратной связью. Производящие функции.	Кольцо формальных рядов, как кольцо без делителей нуля, Э содержащее кольцо многочленов как подкольцо. Мультипликативная группа кольца формальных рядов. Характеристический многочлен регистра. Возвратный характеристический многочлен регистра сдвига и их связь с производящей функцией регистра	Проверка домашнего задания
5	Семейства линейных рекуррентных последовательностей	Методы получения случайных и псевдослучайных последовательностей. Регистры сдвига с обратной связью. Линейный конгруэнтный метод. Мультиплексорные последовательности. Вопросы периодичности и распределения элементов в псевдослучайных последовательностях.	Проверка домашнего задания. Контрольная работа
6	Приложения конечных полей Линейные коды Циклические коды. Поточные шифры.	Линейные коды. Расстояние Хэмминга.Вес Хэмминга. Расстояние Хэмминга является метрикой. Коды исправляющие ошибки. Декодирование линейных кодов. Циклические коды	Проверка домашнего задания
7	Приложения конечных полей Линейные	Поточный шифры. Шифр А5. Шифрование трафика мобильной связи.	Проверка домашнего задания. Контрольная

	коды Циклические коды. Поточные шифры.		работа

Защита лабораторной работы (ЛР), выполнение курсового проекта (КП), курсовой работы (КР), расчетно-графического задания (РГЗ), написание реферата (Р), эссе (Э), коллоквиум (К), тестирование (Т) и т.д.

2.3.2 Примерная тематика курсовых работ (проектов)

Курсовые работы не предусмотрены.

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

№	Вид самостоятельной работы	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	**2**	**3**
1.	Подготовка к текущему контролю	1. Методические указания для подготовки к занятиям лекционного и семинарского типа. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г. 2. Методические указания по выполнению самостоятельной работы обучающихся. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г. 3. Методические указания по использованию интерактивных методов обучения. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5т от 05 мая 2022 г. 4. Методические указания по подготовке эссе, рефератов, курсовых работ. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5т от 05 мая 2022 г.
2.	Выполнение лабораторных работ и расчетно-графических заданий	1. Методические указания по выполнению лабораторных работ. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г. 2. Методические указания по выполнению расчетно-графических заданий. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г.
4.	Подготовка и оформление отчетов по практике	Методические указания по подготовке и оформлению отчета по практике. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г.
5.	Выполнение и защита выпускной квалификационной	Методические указания по выполнению и защите выпускной квалификационной работы (бакалавриат, магистратура, специалитет). Утверждены на заседании Совета факультета ма-

	работы	тематики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 5 от 05 мая 2022 г.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа,

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа,

3. Образовательные технологии, применяемые при освоении дисциплины (модуля)

В ходе изучения дисциплины предусмотрено использование следующих образовательных технологий: лекции, лабораторные занятия, проблемное обучение, модульная технология, подготовка письменных аналитических работ, самостоятельная работа студентов.

Компетентностный подход в рамках преподавания дисциплины реализуется в использовании интерактивных технологий и активных методов (проектных методик, мозгового штурма, разбора конкретных ситуаций, анализа педагогических задач, педагогического эксперимента, иных форм) в сочетании с внеаудиторной работой.

Информационные технологии, применяемые при изучении дисциплины: использование информационных ресурсов, доступных в информационно-телекоммуникационной сети Интернет.

Адаптивные образовательные технологии, применяемые при изучении дисциплины – для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «*Алгебра*».

Оценочные средства включает контрольные материалы для проведения **текущего контроля** в форме разноуровневых заданий для контрольных работ, теоретических вопросов к коллоквиуму, доклада-презентации по проблемным вопросам и **промежуточной аттестации** в форме вопросов и заданий к экзамену.

Структура оценочных средств для текущей и промежуточной аттестации

№ п/п	Код и наименование индикатора (в соответствии с п. 1.4)	Результаты обучения (в соответствии с п. 1.4)	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1	ПК-1.1. Знает основные понятия, идеи и методы фундаментальных математических дисциплин для решения базовых	В результате изучения учебной дисциплины обучающийся знает основные понятия, идеи и методы изучаемой дисциплины,	Контрольная работа	Вопрос на зачете 1-20

	задач	применяемые для решения задач фундаментальной и прикладной математики		
		В результате изучения учебной дисциплины обучающийся умеет применять основные понятия, идеи и методы изучаемой 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		
2	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	Контрольная работа	Вопрос на зачете 1-20
		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		

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерный перечень вопросов и заданий

1. Нахождение примитивного элемента конечного поля.
2. Построение таблицы логарифма Якоби конечного поля.
3. Решение систем линейных уравнений над конечным полем.
4. Алгоритм быстрого возведения в степень.

5. Нахождение обратных элементов в конечном поле.
6. Расширения конечных полей.
7. Линейный регистр сдвига с обратной связью
$S_{n+k} = a_{k-1}S_{nn+k-1} + a_{k-2}S_{n+k-2}... + a_0 S_n + a\,,\ n = 0,1,2$
8. Характеристический многочлен регистра сдвига
$x^k = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + ... + a_1 x + a_0$
9. Нахождение явного вида значений регистра сдвига
10. Методы получения случайных и псевдослучайных последовательностей.
11. Регистры сдвига с обратной связью.
12. Линейный конгруэнтный метод.
13. Мультиплексорные последовательности.
14. Вопросы периодичности и распределения элементов в псевдослучайных последовательностях.
15. Связь между качеством последовательностей, полученных с помощью нелинейных регистров сдвига и характеристиками функции усложнения.
16. Применения дискретных функций для усложнения последовательностей.
17. Случайные и псевдослучайные гаммы.
18. Регистры сдвига с обратной связью.
19. Нахождение примитивного элемента конечного поля.
20. Построение таблицы логарифма Якоби конечного поля.
21. Решение систем линейных уравнений над конечным полем.
22. Алгоритм быстрого возведения в степень.
23. Нахождение обратных элементов в конечном поле.
24. Расширения конечных полей.
25. Структура поля $GF\left(2^8\right)$, нахождение обратных элементов.
26. Фактор кольцо $GF\left(2^8\right)[x]/\left((x+1)^4\right)$, преобразование столбцов.
27. Линейное преобразование, собственные значения матрицы.

Примерные темы реферативных докладов

1. Освоение процессов зашифрования и расшифрования для простейших шифров.
2. Линейные коды.
3. Расстояние Хэмминга.
4. Вес Хэмминга.
5. Расстояние Хэмминга является метрикой.
6. Коды исправляющие ошибки.
7. Декодирование линейных кодов.
8. Циклические коды.
9. Поточный шифры.
10. Шифр А5.
11. Шифрование трафика мобильной связи

Контрольная работа

1. Используя криптосистему RSA и естественную оцифровку русского алфавита, зашифруйте слово ВЕНЕРА, предварительно оцифровав его и разбив на биграммы, если n = 59 · 61 и

ключ зашифрования $e = 17$. Найдите секретный ключ d и расшифруйте полученный шифртекст.

2. Проверить, является ли многочлен $f(x) = x^5 + x^3 + 1$ неприводимым над полем F_p, используя двучлен $x^{p^r} - x$

3. Вычислите последовательность из первых десяти чисел, генерируемую методом Фибоначчи с запаздыванием начиная с k_a при следующих значениях исходных данных;

$a = 3, b = 1, k_0 = 0{,}6 \quad k_1 = 0{,}3, \qquad k_2 = 0{,}5$

4. Построить генератор LFSR с ассоциированным двоичным многочленом $f(x) = x^8 + x^4 + x^3 + x^2 + 1$ (схема Фибоначчи и схема Галуа)

5. Найти LFSR, если нам известна последовательность битов, которая была им сгенерирована 100110101111000

Зачетно-экзаменационные материалы для промежуточной аттестации (экзамен/зачет)

Примерный перечень вопросов к зачету

1. Импульсная функция.
2. Характеристический многочлен.
3. Минимальный период однородной линейной рекуррентной последовательности над конечным полем.
4. Минимальный период последовательности и порядок ее матрицы, как элемента общей линейной группы.
5. Характеристический многочлен.
6. Явная формула n-го члена рекуррентной последовательности.
7. Функция Эйлера и Мебиуса.
8. Группы обратимых элементов в кольцах.
9. Структура мультипликативной группы кольца вычетов.
10. Обратимые элементы.
11. Примитивные элементы.
12. Определение производящей функции.
13. Использование алгебраического аппарата формальных степенных рядов.
14. Формальные степенные ряды над конечным полем.
15. Кольцо формальных рядов, как кольцо без делителей нуля, содержащее кольцо многочленов как подкольцо.
16. Мультипликативная группа кольца формальных рядов.
17. Характеристический многочлен регистра.
18. Возвратный характеристический многочлен регистра сдвига
19. Основная задача теории кодирования. Коды, исправляющие ошибки.
20. Циклические коды. Коды Хэмминга. Коды БЧХ.

Критерии оценивания результатов обучения

Критерии оценивания по зачету:

«зачтено»: студент владеет теоретическими знаниями по данному разделу, знает методы доказательства основных утверждений, устанавливает логические связи между понятиями, владеет навыками применения методов изучаемой дисциплины для решения базовых задач, допускает незначительные ошибки; студент умеет правильно объяснять теоретический материал, иллюстрируя его примерами.

«не зачтено»: материал не усвоен или усвоен частично, студент затрудняется привести примеры, иллюстрирующие теоретический материал, имеет довольно ограниченный объем знаний о базовых понятиях изучаемой дисциплины.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5. Перечень учебной литературы, информационных ресурсов и технологий

5.1 Учебная литература

1. Мартынов Л.М. Алгебра и теория чисел для криптографии: учебное пособие [Электронный ресурс]. - СПб.: Лань, 2020. - URL: https://e.lanbook.com/reader/book/140740

2. Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра, 3-е изд. [Электронный ресурс]. - СПб.: Лань, 2020. - URL: https://e.lanbook.com/reader/book/126718/

3. Аверченков В.И., Рытов М.Ю., Шпичак С.А. Криптографические методы защиты информации: учебное пособие, 2-е изд. [Электронный ресурс]. – М.: ФЛИНТА, 2017 https://e.lanbook.com/book/92914

4. Сергеев, Александр Эдуардович (КубГУ). Основы теории Галуа [Текст] : монография / А. Э. Сергеев, Э. А. Сергеев ; М-во образования и науки Рос. Федерации, Кубанский гос. ун-т. - Краснодар : [Кубанский государственный университет], 2014. - 334 с. - Библиогр.: с. 327-332. - ISBN 9785820910791.

5.2. Периодическая литература

1. Журнал “Вестник Московского университета. Серия 01. Математика. Механика”/ - Издательство Московского университета. – ISSN 0579-9368. - https://dlib.eastview.com/browse/publication/9045

2. Журнал "Известия высших учебных заведений. Математика" ISSN 0021-3446 (Print), ISSN 2076-4626 (Online) . - Учредитель и издатель: Казанский (Приволжский) федеральный университет. - https://dlib.eastview.com/browse/publication/7087

5.3. Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Электронно-библиотечные системы (ЭБС):

1. ЭБС «ЮРАЙТ» https://urait.ru/
2. ЭБС «УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН» www.biblioclub.ru
3. ЭБС «BOOK.ru» https://www.book.ru
4. ЭБС «ZNANIUM.COM» www.znanium.com
5. ЭБС «ЛАНЬ» https://e.lanbook.com

Профессиональные базы данных:

1. Web of Science (WoS) http://webofscience.com/
2. Scopus http://www.scopus.com/
3. ScienceDirect www.sciencedirect.com
4. Журналы издательства Wiley https://onlinelibrary.wiley.com/
5. Научная электронная библиотека (НЭБ) http://www.elibrary.ru/
6. Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОН http://archive.neicon.ru
7. Национальная электронная библиотека (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) https://rusneb.ru/
8. Президентская библиотека им. Б.Н. Ельцина https://www.prlib.ru/
9. Электронная коллекция Оксфордского Российского Фонда https://ebookcentral.proquest.com/lib/kubanstate/home.action
10. Springer Journals https://link.springer.com/
11. Nature Journals https://www.nature.com/siteindex/index.html
12. Springer Nature Protocols and Methods https://experiments.springernature.com/sources/springer-protocols
13. Springer Materials http://materials.springer.com/
14. zbMath https://zbmath.org/
15. Nano Database https://nano.nature.com/
16. Springer eBooks: https://link.springer.com/
17. "Лекториум ТВ" http://www.lektorium.tv/
18. Университетская информационная система РОССИЯ http://uisrussia.msu.ru

Информационные справочные системы:

1. Консультант Плюс - справочная правовая система (доступ по локальной сети с компьютеров библиотеки)

Ресурсы свободного доступа:

1. Американская патентная база данных http://www.uspto.gov/patft/
2. Полные тексты канадских диссертаций http://www.nlc-bnc.ca/thesescanada/
3. КиберЛенинка (http://cyberleninka.ru/);
4. Министерство науки и высшего образования Российской Федерации https://www.minobrnauki.gov.ru/;
5. Федеральный портал "Российское образование" http://www.edu.ru/;
6. Информационная система "Единое окно доступа к образовательным ресурсам" http://window.edu.ru/;
7. Единая коллекция цифровых образовательных ресурсов http://school-collection.edu.ru/ .
8. Федеральный центр информационно-образовательных ресурсов (http://fcior.edu.ru/);

9. Проект Государственного института русского языка имени А.С. Пушкина "Образование на русском" https://pushkininstitute.ru/;
10. Справочно-информационный портал "Русский язык" http://gramota.ru/;
11. Служба тематических толковых словарей http://www.glossary.ru/;
12. Словари и энциклопедии http://dic.academic.ru/;
13. Образовательный портал "Учеба" http://www.ucheba.com/;
14. Законопроект "Об образовании в Российской Федерации". Вопросы и ответы http://xn--273--84d1f.xn--p1ai/voprosy_i_otvety

Собственные электронные образовательные и информационные ресурсы КубГУ:

1. Среда модульного динамического обучения http://moodle.kubsu.ru
2. База учебных планов, учебно-методических комплексов, публикаций и конференций http://mschool.kubsu.ru/
3. Библиотека информационных ресурсов кафедры информационных образовательных технологий http://mschool.kubsu.ru;
4. Электронный архив документов КубГУ http://docspace.kubsu.ru/
5. Электронные образовательные ресурсы кафедры информационных систем и технологий в образовании КубГУ и научно-методического журнала "ШКОЛЬНЫЕ ГОДЫ" http://icdau.kubsu.ru/

6. Методические указания для обучающихся по освоению дисциплины (модуля)

По курсу предусмотрено проведение лекционных занятий, на которых дается основной систематизированный материал, лабораторных занятий, в ходе которых студентами приобретаются и закрепляются основные практически навыки решения различных задач, в том числе с применением полученных теоретических знаний.

Важнейшим этапом курса является самостоятельная работа по дисциплине. Самостоятельная работа студентов является неотъемлемой частью процесса подготовки. Под самостоятельной работой понимается часть учебной планируемой работы, которая выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Самостоятельная работа направлена на усвоение системы научных и профессиональных знаний, формирования умений и навыков, приобретение опыта самостоятельной творческой деятельности. СРС помогает формировать культуру мышления студентов, расширять познавательную деятельность.

Виды самостоятельной работы по курсу:

а) по целям: подготовка к лекциям, к практическим занятиям, к контрольной работе, к коллоквиуму; подготовка научного доклада и выполнение заданий по НИР.

б) по характеру работы: изучение литературы, конспекта лекций; поиск литературы в библиотеке; конспектирование рекомендуемой для самостоятельного изучения научной литературы; решение задач, тестов; работа с обучающими и контролирующими программами.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

7. Материально-техническое обеспечение по дисциплине (модулю)

По всем видам учебной деятельности в рамках дисциплины используются аудитории, кабинеты и лаборатории, оснащенные необходимым специализированным и лабораторным оборудованием.

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения
Учебные аудитории для проведения занятий лекционного типа	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер	Microsoft Office; Программы для демонстрации и создания презентаций («Microsoft Power Point»)
Учебные аудитории для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер	Microsoft Office; Программы для демонстрации и создания презентаций («Microsoft Power Point»)

Для самостоятельной работы обучающихся предусмотрены помещения, укомплектованные специализированной мебелью, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Наименование помещений для самостоятельной работы обучающихся	Оснащенность помещений для самостоятельной работы обучающихся	Перечень лицензионного программного обеспечения
Помещение для самостоятельной работы обучающихся (читальный зал Научной библиотеки)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	
Помещение для самостоятельной работы обучающихся (ауд.302)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	

РЕЦЕНЗИЯ

на рабочую программу дисциплины

Линейные регистры сдвига с обратной связью

по направлению подготовки **01.04.01 Математика**

Рабочая программа дисциплины «Линейные регистры сдвига с обратной связью» рассчитана на изучение в течение одного семестра. Программа курса опирается на знания, умения и навыки, полученные при изучении курсов «Алгебра», «Теоретико-числовые методы криптографии», «Алгоритмические проблемы алгебры», «Компьютерная алгебра».

Представленная на рецензию рабочая программа описывает требования к уровню усвоения дисциплины, объем учебных часов и их распределение по формам занятий, требования к обязательному минимуму содержания программы, перечень литературы и пособий, формы контроля. Содержание теоретического материала дисциплины полно отражает необходимые знания для формирования компетенций по дисциплине. Материалы для самостоятельной учебной работы студентов содержат основные теоретические положения, необходимые для усвоения указанных тем. Критерии оценок по дисциплине отражают необходимые компетенции, которые должны быть сформированы у студентов.

В ходе изучения дисциплины студенты подробно изучают теоретические основы предмета и получают сведения об основных задачах и понятиях теории кодирования, неприводимых многочленах над полями Галуа; характеристических многочленах линейных сдвигов с обратной связью.

Учитывая вышеизложенное, считаю, что рабочая программа профессора Н.А. Наумовой, соответствует государственным требованиям к минимуму содержания и уровню подготовки выпускников по направлению подготовки 01.04.01 Математика, и может быть рекомендована для высших учебных заведений.

Рецензент
доцент кафедры высшей математики
ФГБОУ ВО «Кубанский государственный
технологический университет»,
кандидат педагогических наук, доцент Пригодина А.Г.

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ * «КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ» * УПРАВЛЕНИЕ КАДРОВ

Пригодиной А.Г.
Подпись _____ удостоверяю
Начальник отдела
кадров сотрудников
_____ Е.И. Руссу
«____» _____ 20____ г.