Министерство образования и науки 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
_____ Хагуров Т.А.
«27» апреля 2018 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

Программа подготовки академическая

Форма обучения очная

Квалификация (степень) выпускника магистр

Краснодар 2018

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 составил(и):
А.В. Рожков, профессор, д.ф.-м.н., профессор

Рабочая программа дисциплины Линейные регистры сдвига с обратной связью утверждена на заседании кафедры функционального анализа и алгебры, протокол № 10 от «10» апреля 2018 г.

Заведующий кафедрой Барсукова В.Ю.

Утверждена на заседании учебно-методической комиссии факультета математики и компьютерных наук, протокол № 2 от «17» апреля 2018 г.
Председатель УМК факультета Титов Г.Н

Рецензенты:

Крамаренко Т.А. к.п.н. доцент кафедры системного анализа и обработки информации КубГАУ

Дроботенко М.И. к.ф.-м.н., зав. кафедрой математических и компьютерных методов КубГУ

1 Цели и задачи изучения дисциплины (модуля).

1.1 Цель освоения дисциплины.

Цель освоения дисциплины – рассматривает задачи 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 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:

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 вариативной части Блока 1 "Дисциплины (модули)" учебного плана 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.

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 общекультурных/общепрофессиональных/профессиональных компетенций (ОК/ОПК/ПК)

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1.	ПК-4	Способностью к применению методов математического и алгоритмического моделирования при решении теоретических и прикладных задач	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.

В результате освоения данной дисциплины обучающийся должен:

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.

2. Структура и содержание дисциплины.

2.1 Распределение трудоёмкости дисциплины по видам работ.

Общая трудоёмкость дисциплины составляет 4 зач. ед. (144 часа), их распределение по видам работ представлено в таблице.

Вид учебной работы		Всего часов	Семестры (часы)			
			2			
Контактная работа, в том числе:						
Аудиторные занятия (всего):		**46**	**46**			
Занятия лекционного типа		16	16	-	-	-
Лабораторные занятия		-	-	-	-	-
Занятия семинарского типа (семинары, практические занятия)		30	30	-	-	-
		-	-	-	-	-
Иная контактная работа:						
Контроль самостоятельной работы (КСР)						
Промежуточная аттестация (ИКР)		0,2	0,2			
Самостоятельная работа, в том числе:						
Курсовая работа		-	-	-	-	-
Проработка учебного (теоретического) материала		40	40	-	-	-
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		35	35	-	-	-
Реферат		6	6	-	-	-
Подготовка к текущему контролю		16,8	16,8	-	-	-
Контроль:						
Подготовка к экзамену		-	-			
Общая трудоемкость	**час.**	**144**	**144**	**-**	**-**	**-**
	в том числе контактная работа	**46,2**	**46,2**			
	зач. ед	**4**	**4**			

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 2 семестре *(очная форма)*

№	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	34	4	6		24
2	Регистры сдвига с обратной связью. Производящие функции.	32	4	8		24
3	Семейства линейных рекуррентных последовательностей.	38	4	8		26
4	Приложения конечных полей Линейные коды Циклические коды. Поточные шифры.	32,8	4	8		24,8
	Итого по дисциплине:		16	30		97,8

Примечание: Л – лекции, ПЗ – практические занятия / семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа магистра

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа.

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
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.	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 многочленов 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.	Т
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.	Р

2.3.2 Занятия семинарского типа.

Не предусмотрены

№	Наименование раздела	Тематика практических занятий (семинаров)	Форма текущего контроля
1	2	3	4
1.			
2.			

2.3.3 Практические занятия.

№	Наименование практических работ	Форма текущего контроля
1	3	4
1	Характеристический многочлен. Минимальный период однородной линейной рекуррентной последовательности над конечным полем.	РГЗ
2	Связь порядка характеристического многочлена и минимального периода импульсной функции.	Р
3	Явная формула n-го члена рекуррентной последовательности. Связь со следом элемента алгебраического расширения поля.	Э
4	Минимальный период последовательности и порядок ее матрицы, как элемента общей линейной группы.	РГЗ
5	Линейные коды. Расстояние Хэмминга.Вес Хэмминга.	Р
6	Расстояние Хэмминга является метрикой. Коды исправляющие	РГЗ

	ошибки.	
7	Декодирование линейных кодов. Циклические коды. Поточный шифры.	Р
8	Шифр А5. Шифрование трафика мобильной связи	РГЗ

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

2.3.4 Примерная тематика курсовых работ (проектов)

Курсовые работы не предусмотрены.

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

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Подготовка рефератов и научных сообщений	Рожков А.В. «Темы исследовательских работ и методические указания по их написанию», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 30 августа 2017 г.
2	Самостоятельное освоение теории	Рожков А.В. «Алгебра и теория чисел. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 30 августа 2017 г.
3	Решение задач	Рожков А.В. «Решебник типовых задач по криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 30 августа 2017 г
4	Самостоятельное освоение теории	Рожков А.В. «Комментарии к лекциям по криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 30 августа 2017 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 с 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,

Перечень

электронных документов, которые могут быть представлены
в печатной форме с увеличенным шрифтом

1. Рожков А.В. «Темы исследовательских работ и методические указания по их написанию», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 30 августа 2017 г.
2. Рожков А.В. «Решебник типовых задач по криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 30 августа 2017 г.
3. Рожков А.В. «Алгебра и теория чисел. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 30 августа 2017 г.
4. Рожков А.В. «Комментарии к лекциям по криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 30 августа 2017 г.

3. Образовательные технологии.

Активные и интерактивные формы, лекции, контрольные работы, реферативные доклады (по некоторым темам в виде презентации) и зачет. В течение семестра магистры решают задачи, указанные преподавателем, к каждому лабораторному занятию. Каждый магистр готовит реферативный доклад по одной из ниже научных тем. Зачет выставляется после выполнения определенного количества (практических и теоретических) заданий контрольных работ и отчета по реферативному докладу. В случае невыполнения какого-то из приведенных требований, магистру для сдачи зачета предлагаются по усмотрению преподавателя некоторые практические и теоретические задания, подобные предложенным ниже.

К образовательным технологиям также относятся интерактивные методы обучения. Интерактивность подачи материала по дисциплине «Линейные регистры сдвига с обратной связью» предполагает не только взаимодействия вида «преподаватель - магистр» и «магистр - преподаватель», но и «магистр - магистр». Все эти виды взаимодействия хорошо достигаются при изложении материала на занятиях в ходе дискуссий, а также на лабораторных занятиях в ходе изложения магистрами реферативных докладов (возможно в виде презентации).

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации.

4.1 Фонд оценочных средств для проведения текущего контроля.

Список теоретических вопросов (для подготовки 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

4.2 Фонд оценочных средств для проведения промежуточной аттестации. Список типовых алгоритмов (для самостоятельных занятий и зачета)

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 $S_{n+k} = a_{k-1}S_{n+k-1} + a_{k-2}S_{n+k-2} + ... + a_1S_{n+1} + a_0S_n + a, n = 0,1,2,...$
8. Характеристический многочлен регистра сдвига $x^k = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + ... + a_1x + a_0$
9. Нахождение явного вида значений регистра сдвига $S_n = \beta_1\alpha_1{}^n + \beta_2\alpha_2{}^n + ... + \beta_k\alpha_k{}^n, n = 0,1,2,...$, где $\alpha_1, \alpha_2, ..., \alpha_k$ - корни характеристического многочлена, коэффициенты $\beta_1, \beta_2, ..., \beta_k \in P$ являются решениями системы $\begin{cases} \beta_1\alpha_1{}^0 + \beta_2\alpha_2{}^0 + ... + \beta_k\alpha_k{}^0 = S_0 \\ \beta_1\alpha_1{}^1 + \beta_2\alpha_2{}^1 + ... + \beta_k\alpha_k{}^1 = S_1 \\ ... \\ \beta_1\alpha_1{}^{k-1} + \beta_2\alpha_2{}^{k-1} + ... + \beta_k\alpha_k{}^{k-1} = S_{k-1} \end{cases}$.
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 $GF(2^8)$, нахождение обратных элементов.
26. Фактор кольцо $GF(2^8)[x] / ид((x+1)^4)$, 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.

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля).

5.1 Основная литература:

1. Рябко Б.Я, Фионов А.Н. Криптографические методы защиты информации, 2-е изд. [Электронный ресурс]. – М.: Горячая линия-Телеком, 2012. - URL: http://e.lanbook.com/view/book/5193/
2. Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра, 2-е изд. [Электронный ресурс]. - СПб.: Лань, 2015. - URL: http://e.lanbook.com/view/book/67458/

5.2 Дополнительная литература:

1. 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.
2. Торстейнсон П., Ганеш Г.А. Криптография и безопасность в технологии .NET. 3-е изд. [Электронный ресурс]. – М.: Лаборатория знаний, 2015. – URL: http://e.lanbook.com/view/book/70724/

1.3. Периодические издания:

Не предусмотрены

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

1. Пакет компьютерной алгебры Sage 8.2. Официальный сайт http://sagemath.org/
2. Пакет компьютерной алгебры Gap4r9p1. Официальный сайт http://www.gap-system.org/

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

Согласно учебному плану дисциплины «Линейные регистры сдвига с обратной связью» итоговой формой контроля является зачет. Для сдачи зачета магистр должен научиться на лабораторных занятиях решать практические задания по темам разделов 1-3, выполнять домашние задания. Типы практических заданий на зачет соответствуют заданиям. Также на зачете магистрам предлагаются и теоретические задания, состоящие в письменном ответе на один из вопросов. Количество практических и теоретических заданий зависит от активности и результативности работы магистра в течение семестра.

Важнейшим этапом курса является самостоятельная работа по дисциплине (модулю).

Для подготовки к ответам на теоретические вопросы в ходе контрольных работ и на зачете магистрам достаточно использовать материал лекций. Весь этот теоретический материал содержится в учебных пособиях из списка основной литературы. Для изучения теоретического материала, необходимого для подготовки реферативного доклада, кроме основных источников литературы возможно использование дополнительных источников и Интернет-ресурса. В случае затруднений, возникающих у магистров в процессе самостоятельного изучения теории, преподаватель разъясняет сложные моменты на консультациях.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю).

8.1 Перечень информационных технологий.

Вычисления в пакетах компьютерной алгебры на отрытом коде GAP4.8.10 и Sage 8.1

8.2 Перечень необходимого программного обеспечения.

а) перечень лицензионного программного обеспечения:

№	Перечень лицензионного программного обеспечения
1.	Maple Soft Maple 18
2.	Mathcad 3
3.	Mathcad 14
4.	Microsoft office
5.	MS Windows 10 (x64)
6.	MS Office 2013, MS

в) Перечень свободно распространяемого программного обеспечения

№	Перечень свободно распространяемого программного обеспечения
1.	Пакет компьютерной алгебры Sage 8.1. Официальный сайт http://sagemath.org/
2.	Пакет компьютерной алгебры Gap4r8p10. Официальный сайт http://www.gap-system.org/
3.	Пакет компьютерной алгебры PARI/GT 2.9. Официальный сайт http://pari.math.u-bordeaux.fr/
4.	Библиотека для работы с большими целыми числами GMP 6.1.2. Официальный сайт https://gmplib.org/
5.	Язык программирования Python. Официальный сайт https://www.python.org/
6.	Язык программирования Julia. Официальный сайт http://julialang.org/
7.	Язык программирования Cython. Официальный сайт http://cython.org/
8.	Компилятор PyPy, оптимизирующий код Python и Cython. Официальный сайт http://pypy.org/
9.	Python в облаке, интегрированная среда разработки Anaconda. Официальный сайт https://store.continuum.io/cshop/anaconda/
10.	Математические пакеты Python, проект SciPy. Официальный сайт http://www.scipy.org/
11.	Клиентская ОС Debian 9.3. Официальный сайт https://www.debian.org/index.ru.html
12.	Издательская система LaTeX/MiKTeX 2.9. Официальный сайт http://www.miktex.org/
13.	Утилиты Руссиновича https://technet.microsoft.com/ru-ru/library/bb545021.aspx
14.	Анализ защищенности сети Kali Linux 2018.1. https://www.kali.org/
15.	Анализ защищенности сети Snort 2.9.11. Официальный сайт https://www.snort.org/
16.	Серверная ОС CentOS – 7. Официальный сайт https://www.centos.org/
17.	Офисная система Apache OpenOffice 4.1.5. Официальный сайт https://www.openoffice.org/ru/

8.3 Перечень информационных справочных систем:

1. Справочно-правовая система «Консультант Плюс» (http://www.consultant.ru)
2. Электронная библиотечная система eLIBRARY.RU (http://www.elibrary.ru)/

3. Электронная библиотека http://gen.lib.rus.ec/

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю).

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Лекционные занятия	Лекционная аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) и соответствующим программным обеспечением (ПО) Программы, демонстрации видео материалов (проигрыватель «Windows Media Player»). Программы для демонстрации и создания презентаций («Microsoft Power Point»).
2	Практические занятия	Специальное помещение, оснащенное учебной мебелью, презентационной техникой (проектор, экран, ноутбук) и соответствующим программным обеспечением (ПО).
3	Групповые (индивидуальные) консультации	Помещение для проведения групповых (индивидуальных) консультаций, учебной мебелью, доской, маркером или мелом
4	Текущий контроль, промежуточная аттестация	Помещение для проведения текущей и промежуточной аттестации, оснащенное учебной мебелью.
5	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета