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
_____ Иванов А.Г.
«01» июля 2016 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.09.02 ТЕОРЕТИКО-ГРУППОВЫЕ МОДЕЛИ В КОДИРОВАНИИ И ЗАЩИТЕ ИНФОРМАЦИИ

Направление подготовки 02.03.01 Математика и компьютерные науки

Направленность (профиль): Алгебра, теория чисел и дискретный анализ

Программа подготовки академическая

Форма обучения очная

Квалификация (степень) выпускника бакалавр

Краснодар 2016

Рабочая программа дисциплины Теоретико-групповые модели в кодировании и защите информации составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 02.03.01 Математика и компьютерные науки

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

Рабочая программа дисциплины Теоретико-групповые модели в кодировании и защите информации утверждена на заседании кафедры функционального анализа и алгебры
протокол № 14 « 7 » июня 2016 г.
Заведующий кафедрой (разработчика) Барсукова В.Ю.

Рабочая программа обсуждена на заседании кафедры (выпускающей) функционального анализа и алгебры
протокол № 14 «7» июня 2016 г.
Заведующий кафедрой (выпускающей) Барсукова В.Ю.

Утверждена на заседании учебно-методической комиссии факультета математики и компьютерных наук
протокол № 3 « 20 » июня 2016 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 – дальнейшее формирование у студентов приобретенных на первых трех курсах знаний по фундаментальной алгебре и математическим проблемам защиты информации

1.2 Задачи дисциплины.

Задачи освоения дисциплины «Теоретико-групповые модели в кодировании и защите информации»: получение базовых теоретических сведений по алгебраическим системам и теории чисел, в том числе по теории групп; развитие познавательной деятельности и приобретение практических навыков работы с алгебраическими и общематематическими понятиями.

При освоении дисциплины вырабатывается общематематическая культура: умение логически мыслить, проводить доказательства основных утверждений, устанавливать логические связи между понятиями, применять полученные знания для решения задач в области теории групп, теории чисел, математического моделирования информационных процессов. Получаемые знания лежат в основе математического образования и необходимы для понимания и освоения всех курсов математики, а также для продолжения обучения в магистратуре по соответствующему направлению подготовки.

1.3 Место дисциплины (модуля) в структуре образовательной программы.

Дисциплина «Теоретико-групповые модели в кодировании и защите информации» относится к вариативной части Блока 1 "Дисциплины (модули)" учебного плана Б1.В.ДВ.09.02.

Курс «Теоретико-групповые модели в кодировании и защите информации» продолжает начатое на первых трех курсах алгебраическое образование студентов соответствующего направления подготовки. Знания, полученные в этом курсе, могут быть использованы в дискретной математике, теории чисел, методах оптимизации и др. Слушатели должны владеть математическими знаниями в рамках программы курса «Фундаментальная и компьютерная алгебра».

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 (ОПК/ПК) ОПК-2, ПК-4, ПК-4

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
1.	ОПК-2	Способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопас-	О компьютерной реализации информационных объектов. Связи компьютерной алгебры и численного анализа.	Определять структуры данных в компьютерной алгебре. использовать технику символьных вычислений.	навыками использования основных типов шифров и криптографических алгоритмов; методами криптоанализа простейших шифров: навыками мате-

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	**уметь**	**владеть**
		ности	Элементы теории сложности алгоритмов. об основных задачах и понятиях криптографии об этапах развития криптографии	Требования к шифрам и основные характеристики шифров; принципы построения современных шифрсистем.	матического моделирования в криптографии; современной научно-технической литературой в области криптографической защиты.
2.	ОПК-4	Способностью находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем			
3	ПК-4	способностью публично представлять собственные и известные научные результаты			

В результате освоения данной дисциплины обучающийся должен:
Знать:
о компьютерной реализации информационных объектов;
связи компьютерной алгебры и численного анализа;
элементы теории сложности алгоритмов;
об основных задачах и понятиях криптографии
Уметь:
классифицировать модели информационных систем, использовать в научной работе приобретенные знания, реализовывать на компьютере некоторые алгоритмы, предложенные в курсе «Теоретико-групповые модели в кодировании и защите информации»
Владеть:
методами исследований, используемыми в комбинаторных теориях алгебраических систем, моделирующих информационные процессы.

2. Структура и содержание дисциплины.

2.1 Распределение трудоёмкости дисциплины по видам работ.

Общая трудоёмкость дисциплины составляет 3 зач. ед. (108 часа), их распределение по видам работ представлено в таблице.

Вид учебной работы	Всего часов	Семестры (часы)			
		6			
Контактная работа, в том числе:					
Аудиторные занятия (всего):	**64**	**64**			
Занятия лекционного типа	32	32	-	-	-
Лабораторные занятия	32	32	-	-	-
Занятия семинарского типа (семинары, практические занятия)			-	-	-
	-	-	-	-	-

Иная контактная работа:						
Контроль самостоятельной работы (КСР)		4	4			
Промежуточная аттестация (ИКР)		0,2	0,2			
Курсовая работа		7	7	-	-	-
Самостоятельная работа, в том числе:						
Проработка учебного (теоретического) материала		8	8	-	-	-
Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		8	8	-	-	-
Реферат				-	-	-
Подготовка к текущему контролю		16,8	16,8	-	-	-
Контроль:						
Подготовка к экзамену		-	-			
Общая трудоемкость	**час.**	**108**	**108**	**-**	**-**	**-**
	в том числе контактная работа	**75,2**	**75,2**			
	зач. ед	**3**	**3**			

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 6 семестре *(очная форма)*

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1	Теоретико-числовые конструкции в теории защиты информации и теории кодов	26	8		8	10
2	Основы алгебраической теории кодов	28	8		8	12
3	Теоретико-числовые модели защищенных информационных систем	28	8		8	12
4	Поточные шифры. Синронизированные и самосинхронизующиеся. Надежность шифров.	18,8	8		8	8,8
	Итого по дисциплине:		32		32	32,8

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

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа.

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1	Теоретико-числовые	Определение и основные свойства колец. Евкли-	Р

	конструкции в теории защиты информации и теории кодов	довы кольца. Кольца многочленов. Фактор кольца. Кольца вычетов. Многочлены над кольцами вычетов. Простейшие модели псевдослучайных последовательностей, как рекуррентные последовательности над конечными кольцами. Малая теорема Ферма. Первообразные корни. Структура мультипликативной группы кольца вычетов. Функция Эйлера, китайская теорема об остатках. Дискретное логарифмирование. Поля Галуа. Однонаправленные функции. Разложение на множители. Алгоритм шифрования RSA. Алгоритмы, основанные на извлечении квадратного корня в кольце вычетов.	
2	Основы алгебраической теории кодов	Определение кода. Расстояние Хэмминга. Основные двоичные коды. Разложение многочленов над конечными полями. Основной алгоритм. Определение периода многочлена. Трехчлены над GF(2). Полное разложение многочлена $x^n - 1$. Квадратичный закон взаимности. Коды с повторением. Коды с одной проверкой на четность. Линейные коды. Циклические коды. Групповые коды. Коды Хэмминга. Коды Боуза-Чоудхури-Хоквингемы (БЧХ-коды). Двоичные циклические коды. Двоичные БЧХ-коды, исправляющие многократные ошибки. Недвоичное кодирование. Схемы модуляции. Весовые функции. Нециклические коды для метрики Ли.	Р
3	Теоретико-числовые модели защищенных информационных систем	Основы теории обыкновенных, ориентированных и нагруженных графов. Конечные автоматы. Структура и классификация автоматизированных систем. Модели организации данных. Иерархическая и сетевая модели представления данных. Реляционная модель организации данных. Распределенные модели данных. Управляющие системы. Теоретико-числовые модели безопасности данных и информационных систем. Модель матрицы доступа HRU. Модель рапространения прав доступа TAKE-GRANT. Модель системы безопасности БЕЛЛА-ЛАПАДУЛА.	Э
4	Поточные шифры. Синронизированные и самосинхронизующиеся. Надежность шифров.	Табличное и модульное гаммирование. Случайные и псевдослучайные гаммы. Криптограммы, полученные при повторном использовании ключа. Анализ криптограмм, полученных применением неравновероятной гаммы. Криптографическая стойкость шифров. Ненадежность ключей и сообщений. Совершенные шифры. Характеризация со-	Р

		вершенных шифров с минимальным числом ключей. Безусловно стойкие и вычислительно стойкие шифры.	

2.3.2 Занятия семинарского типа.

Не предусмотрены

2.3.3 Лабораторные занятия.

№	Наименование лабораторных работ	Форма текущего контроля
1	3	4
1	Многочлены над кольцами вычетов. Простейшие модели псевдослучайных последовательностей, как рекуррентные последовательности над конечными кольцами. Малая теорема Ферма.	Р
2	Первообразные корни. Структура мультипликативной группы кольца вычетов. Функция Эйлера, китайская теорема об остатках. Дискретное логарифмирование. Поля Галуа.	Р
3	Определение кода. Расстояние Хэмминга. Основные двоичные коды. Разложение многочленов над конечными полями. Основной алгоритм. Определение периода многочлена. Трехчлены над GF(2). Полное разложение многочлена $x^n - 1$.	Э
4	Квадратичный закон взаимности. Коды с повторением. Коды с одной проверкой на четность. Линейные коды. Циклические коды. Групповые коды. Коды Хэмминга. Коды Боуза-Чоудхури-Хоквингемы (БЧХ-коды). Двоичные циклические коды.	Р
5	Структура и классификация автоматизированных систем. Модели организации данных. Иерархическая и сетевая модели представления данных. Реляционная модель организации данных. Распределенные модели данных. Управляющие системы.	Р
6	Теоретико-числовые модели безопасности данных и информационных систем. Модель матрицы доступа HRU. Модель рапространения прав доступа TAKE-GRANT. Модель системы безопасности БЕЛЛА-ЛАПАДУЛА.	Э
7	Табличное и модульное гаммирование. Случайные и псевдослучайные гаммы. Криптограммы, полученные при повторном использовании ключа. Анализ криптограмм, полученных применением неравновероятной гаммы.	Р
8	Криптографическая стойкость шифров. Ненадежность ключей и сообщений.	Р

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

2.4 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 31 августа 2017 г.
2	Самостоятельное освоение теории	Рожков А.В. «Комментарии к лекциям по криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 31 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 31 августа 2017 г.
4	Решение задач	Рожков А.В. «Алгебраические методы криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 31 августа 2017.

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 31 августа 2017 г.
2. Рожков А.В. «Перечень электронных источников информации для самостоятельных работ по циклу дисциплин Информационная безопасность магистерской программы АМЗИ и рекомендации по его использованию». Методические указания, утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 31 августа 2017.

3. Образовательные технологии.

Активные и интерактивные формы, лекции, контрольные работы, реферативные доклады (по некоторым темам в виде презентации) и зачет. В течение семестра студенты решают задачи, указанные преподавателем, к каждому лабораторному занятию. Каждый студент 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, студенту 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 «Теоретико-групповые модели в кодировании и защите информации» предполагает не только взаимодействия вида «преподаватель - студент» и «студент - преподаватель», но и «студент - студент». Все эти виды взаимодействия хорошо достигаются при изложении материала на занятиях в ходе дискуссий, а также на лабораторных занятиях в ходе изложения студентами реферативных докладов (возможно в виде презентации).

Вид занятия	**Используемые интерактивные образовательные технологии**
ЛЗ	Мультимедийная беседа: «Ручные и машинные шифры..
ЛЗ	Дискуссия на тему: «Ключевая система шифра. с докладами-презентациями
ЛЗ	Круглый стол на тему: «Основные требования к шифрам..» с докладами-презентациями

Семестр	**Вид занятия**	**Используемые интерактивные образовательные технологии**	**Количество часов**
6	Лабораторные занятия	Тема Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты	2
		Тема Криптоанализ шифров перестановки.	2
		Тема Одно алфавитные и многоалфавитные замены.	2
		Тема Вычисления средствами системы GAP4.	2
	Лабораторные занятия	Дискуссия на тему: «.Вопросы криптоанализа простейших шифров замены. с докладами-презентациями	2
		Круглый стол на тему: «Разложение АТ-групп в прямое произведение. и.» с докладами-презентациями	2
		Стандартные алгоритмы криптографической зашиты данных.	2
		Компьютерная симуляция: Нерешенные проблемы. Варианты обобщения конструкции.	2
Итого:			16

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций со студентом при помощи электронной информационно-образовательной среды ВУЗа.

Компьютерная симуляция – это максимально приближенная к реальности имитация различных процессов и (или) деятельности с использованием программного обеспечения образовательного назначения.

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. Бинарная алгебраическая операция, свойства, терминология.
2. Определение кольца.
3. Примеры колец.
4. Конечные кольца.
5. Евклидовы кольца.
6. Кольца вычетов.
7. Функция Эйлера.
8. Функция Мебиуса.
9. Теорема Ферма.
10. Китайская теорема об остатках.
11. Однонаправленные функции.
12. Сложность разложения на множители.
13. Алгоритм RSA.
14. Конечные поля.
15. Алгоритм извлечения квадратных корней в конечном поле.
16. Неприводимые многочлены над полями Галуа.
17. Период многочлена.
18. Решение систем линейных уравнений по разным модулям.
19. Генераторы псевдослучайных последовательностей.
20. Определение кода, исправляющего ошибки.
21. Расстояние Хэмминга.
22. Коды Хэмминга.
23. Линейные коды.
24. Циклические коды.
25. Групповые коды.
26. Матричные модели доступа.
27. Обыкновенные графы.
28. Ориентированные графы.
29. Графы с петлями и мультиграфы.
30. Нагруженные графы.
31. Реляционная алгебра.
32. Реляционных базы данных.
33. Распределенные базы данных.
34. Коды Боуза-Чоудхури-Хоквингемы (БЧХ-коды).
35. Двоичные БЧХ-коды, исправляющие многократные ошибки.
36. Недвоичное кодирование.
37. Схемы модуляции.
38. Весовые функции.
39. Нециклические коды для метрики Ли.
40. Модель матрицы доступа HRU.
41. Модель распространения прав доступа TAKE-GRANT.
42. Модель системы безопасности БЕЛЛА-ЛАПАДУЛА.

4.2 Фонд оценочных средств для проведения промежуточной аттестации.

Список типовых алгоритмов (для самостоятельных и лабораторных занятий)

1. Сколько различных бинарных операций можно задать на множестве из 4 элементов? Сколько из этих операций коммутативных?

2. Решить в кольце $M_2(\mathbb{Z}_{12})$ линейное уравнение.
3. Сколько элементов содержит кольцо $M_2(\mathbb{Z}_{12})$.
4. Перечислить идеалы кольца $M_2(\mathbb{Z}_4)$
5. Найти НОД двух многочленов в кольце $\mathbb{Z}_{11}[\mathrm{x}]$.
6. Найти группу обратимых элементов в кольце $\mathbb{Z}_{24}$.
7. Найти примитивные элементы в поле $GF(2^3)$.
8. Пример вычислений в системе RSA для $n = pq, p = 17, q = 23$.
9. Проверить неприводимость конкретного многочлена над полем $GF(3)$.
10. Привести пример системы, к которой применима китайская теорема об остатках и решить ее.
11. Привести три примера кандидатов в однонаправленные функции.
12. Написать на GAP программу, вычисляющую все простые числа из промежутка [m, n].
13. Пример ручного применения алгоритма извлечения квадратного корня по простому модулю.
14. Вычисление корней в конечных полях с использованием пакета GAP и Maple 17.
15. Найти все неприводимые многочлены степени 3 над полем Галуа $GF(3)$.
16. Найти период последовательности, заданной формулой $s_{n+1} = 2s_n + 1(\mathrm{mod}11)$.
17. Решить систему линейных уравнений по разным модулям
$$\begin{cases} 2x = 3(\mathrm{mod}11) \\ 2x = 5(\mathrm{mod}13) \\ x = 2(\mathrm{mod}22) \end{cases}.$$
18. Привести пример регистра сдвига с обратной связью. Записать регистр в матричной форме. Нарисовать электронную схему регистра.
19. Привести пример кода, исправляющего 3 ошибки.
20. Найти расстояние Хэмминга между конкретными кодирующими словами.
21. Найти расстояние Хэмминга между конкретными множествами кодирующих слов.
22. Закодировать кодом Хэмминга данный набор объектов (например, слов в алфавите $\{\mathrm{a}, \mathrm{b}, \mathrm{c}\}$).
23. Привести пример линейного кода.
24. Привести пример циклического кода.
25. Привести пример кода являющего групповым и кода групповым не являющегося.
26. На примере системы с тремя ресурсами и тремя пользователями привести пример матрицы доступа.
27. Матрицы доступа, реализованные в операционных системах семейства Linux.
28. Привести пример графа частично упорядоченного множества.
29. Привести пример графа с петлями.
30. Привести пример мультиграфа.
31. Матричная запись нагруженного графа.
32. Пример конечной реляционной алгебры.
33. Примеры операций в реляционной алгебре.
34. Привести примеры коммерческих реляционных баз данных.
35. Перечислить признаки распределенных баз данных.

36. Привести примеры кодов Боуза-Чоудхури-Хоквингемы (БЧХ-коды).
37. Привести пример двоичного БЧХ-коды, исправляющего 7 ошибок.
38. Привести примеры недвоичное кодирования.
39. Найти логарифмы Якоби в поле $GF(5^2)$.
40. Построить конечный автомат, проверяющий натуральные числа на четность.
41. Привести пример конечного автомата с 5 состояниями и двумя завершающими состояниями.
42. Перечислить свойства схемы БЕЛЛА-ЛАПАДУЛА. Ее основные недостатки.

4.3 Примерная тематика курсовых работ (проектов)

1. Построение полей разложений многочленов над конечными полями
2. Деревья и их автоморфизмы
3. Алгоритм извлечения квадратного корня по простому модулю
4. Линейные регистры сдвига с обратной связью
5. Коды Хэмминга и сжатие информации
6. Реляционные алгебры
7. Коммерческие продукт, реализующие модель распределенных баз данных
8. Решение квадратных уравнений в конечных полях с использованием логарифмов Якоби
9. Обзор популярных БЧХ-кодов
10. Недостатки модели Белла-ЛаПадула

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

5.1 Основная литература:

1. Нестеров С.А. Основы информационной безопасности, 4-е изд. [Электронный ресурс]. - СПб.: Лань, 2018. URL:- https://e.lanbook.com/reader/book/103908/#1
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/reader/book/70724/#1

5.2 Дополнительная литература:

1. Рябко Б.Я, Фионов А.Н. Криптографические методы защиты информации [Электронный ресурс]. – М.: Горячая линия-Телеком, 2012. - URL: https://e.lanbook.com/reader/book/5193/#1
2. Водяхо А.И., Выговский Л.С., Дубенецкий В.А., Цехановский В.В. Архитектурные решения информационных систем, 2-е изд. [Электронный ресурс]. – М.: Лань, 2017. – URL: https://e.lanbook.com/reader/book/96850/#1

1.3. Периодические издания:

Не предусмотрены

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

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

Согласно учебному плану дисциплины «Теоретико-групповые модели в кодировании и защите информации» итоговой формой контроля является зачет. Для сдачи зачета студент 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 студентам предлагаются и теоретические

задания, состоящие в письменном ответе на один из вопросов. Количество практических и теоретических заданий зависит от активности и результативности работы студента 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 студентам 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 студентов 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.

8.2 Перечень необходимого программного обеспечения.

а) перечень лицензионного программного обеспечения:

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

в) Перечень свободно распространяемого программного обеспечения

№	Перечень свободно распространяемого программного обеспечения
1.	Пакет компьютерной алгебры Sage 8.2. Официальный сайт http://sagemath.org/
2.	Пакет компьютерной алгебры Gap4r9p1. 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 9.4. 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 2018.2. https://www.kali.org/
15.	Офисная система Apache OpenOffice 4.1.5. Официальный сайт

	https://www.openoffice.org/ru/

8.3 Перечень информационных справочных систем:

1. Пакет компьютерной алгебры Sage 8.3. Официальный сайт http://sagemath.org/
2. Пакет компьютерной алгебры Gap4r9p3. Официальный сайт http://www.gap-system.org/
3. Пакет компьютерной алгебры PARI/GT 2.11. Официальный сайт http://pari.math.u-bordeaux.fr/
4. Пакет компьютерной алгебры Maple 2018. http://www.maplesoft.com
5. http://www.pravo.gov.ru – официальный портал правовой информации
6. http://www.government.ru - интернет-портал Правительства РФ
7. http://graph.document.kremlin.ru - раздел «Документы» портала Президента России
8. http://minsvyaz.ru/ru - сайт Минкомсвязи РФ
9. http://www.rsoc.ru - сайт Федеральной службы Роскомнадзор
10. http://www.scrf.gov.ru – сайт Совета безопасности РФ
11. http://base.consultant.ru – сайт правовой информации «Консультант+»
12. http://www.fstec.ru – официальный сайт ФСТЭК России
13. Электронная библиотечная система eLIBRARY.RU (http://www.elibrary.ru)/
14. 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 со- ответствующим программным обеспечением (ПО)
2.	Лабораторные занятия	Специальное помещение, оснащенное учебной мебелью, доской, маркерами и мелом
3.	Групповые (индивидуальные) консультации	Аудитория (кабинет) оснащенная учебной мебелью, дос- кой, маркерами и мелом
4.	Текущий контроль, промежуточная аттестация	Аудитория (кабинет) оснащенная учебной мебелью, дос- кой, маркерами и мелом
5.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный ком- пьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспе- ченный доступом в электронную информационно- образовательную среду университета.

РЕЦЕНЗИЯ

на рабочую программу дисциплины
ТЕОРЕТИКО-ГРУППОВЫЕ МОДЕЛИ В КОДИРОВАНИИ И ЗАЩИТЕ ИНФОРМАЦИИ

Направление подготовки 02.03.01 Математика и компьютерные науки
Направленность Алгебра, теория чисел и дискретный анализ

Рабочая программа дисциплины Теоретико-групповые модели в кодировании и защите информации для студентов направленность Алгебра, теория чисел и дискретный анализ составлена доктором физико-математических наук, профессором кафедры функционального анализа и алгебры факультета математики и компьютерных наук Кубанского государственного университета Рожковым А.В.

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего профессионального образования (ФГОС ВО) по направлению подготовки 02.03.01 Математика и компьютерные науки. Программа одобрена на заседании кафедры функционального анализа и алгебры и на заседании учебно-методического совета факультета математики и компьютерных наук.

Содержание рабочей программы. Определение кода. Расстояние Хэмминга. Основные двоичные коды. Разложение многочленов над конечными полями. Основной алгоритм. Определение периода многочлена. Трехчлены над GF(2). Полное разложение многочлена $x^n - 1$. Квадратичный закон взаимности. Коды с повторением. Коды с одной проверкой на четность. Линейные коды. Циклические коды. Групповые коды. Коды Хэмминга. Коды Боуза-Чоудхури-Хоквингемы (БЧХ-коды). Двоичные циклические коды. Двоичные БЧХ-коды, исправляющие многократные ошибки. Недвоичное кодирование. Схемы модуляции.

Рабочая программа дисциплины Теоретико-групповые модели в кодировании и защите информации для студентов направленность Алгебра, теория чисел и дискретный анализ сочетает теоретическую и практические части. Получение базовых практических сведений и навыков о структуре и алгоритмах символьных математических вычислений.

Считаю, что рабочая программа дисциплины Теоретико-групповые модели в кодировании и защите информации для студентов направленность Алгебра, теория чисел и дискретный анализ может быть рекомендована для подготовки студентов направления подготовки 02.03.01 Математика и компьютерные науки.

Кандидат физ.-мат. наук,
заведующий кафедрой математических
и компьютерных методов ФГБОУ ВО «КубГУ»

М.И. Дроботенко

РЕЦЕНЗИЯ

на рабочую программу дисциплины

ТЕОРЕТИКО-ГРУППОВЫЕ МОДЕЛИ В КОДИРОВАНИИ И ЗАЩИТЕ ИНФОРМАЦИИ

Направление подготовки 02.03.01 Математика и компьютерные науки
Направленность Алгебра, теория чисел и дискретный анализ

Рабочая программа дисциплины Теоретико-групповые модели в кодировании и защите информации для студентов направленность Алгебра, теория чисел и дискретный анализ составлена доктором физико-математических наук, профессором кафедры функционального анализа и алгебры факультета математики и компьютерных наук Кубанского государственного университета Рожковым А.В.

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего профессионального образования (ФГОС ВО) по направлению подготовки 02.03.01 Математика и компьютерные науки. Программа одобрена на заседании кафедры функционального анализа и алгебры и на заседании учебно-методического совета факультета математики и компьютерных наук.

Студенты, освоившие дисциплину Теоретико-групповые модели в кодировании и защите информации должны знать: связи компьютерной алгебры и численного анализа; элементы теории сложности алгоритмов; об основных задачах и понятиях криптографии. Уметь: классифицировать модели информационных систем, использовать в научной работе приобретенные знания, реализовывать на компьютере прикладные алгоритмы.

Рабочая программа дисциплины Теоретико-групповые модели в кодировании и защите информации для студентов направленность Алгебра, теория чисел и дискретный анализ сочетает теоретическую и практические части, что способствует более глубокому усвоению материала. Предложенные задания научно-исследовательского плана направлены на развитие практических навыков решения задач по направлению защита информации.

Считаю, что рабочая программа дисциплины Теоретико-групповые модели в кодировании и защите информации для студентов направленность Алгебра, теория чисел и дискретный анализ может быть рекомендована для подготовки студентов направления подготовки 02.03.01 Математика и компьютерные науки.

Кандидат педагогических наук,
доцент кафедры системного анализа и обработки информации
ФГБОУ ВО «КубГАУ»

Т.А. Крамаренко

Личную подпись тов.
ЗАВЕРЯЮ: Т.А. Крамаренко
Специалист по кадрам
Мелихова