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
_____ Г.А. Хагуров
подпись
«31» мая 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.ДВ.04.02 ТЕОРЕТИКО-ГРУППОВЫЕ МОДЕЛИ В КОДИРОВАНИИ И ЗАЩИТЕ ИНФОРМАЦИИ

Направление подготовки 02.03.01 Математика и компьютерные науки

Направленность (профиль) Современная алгебра и криптография

Форма обучения очная

Квалификация бакалавр

Краснодар 2024

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
(Алгебра, теория чисел и дискретный анализ)

код и наименование направления подготовки

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 № 12 «07» мая 2024 г.
Заведующий кафедрой функционального анализа и алгебры

Барсукова В.Ю. 

Утверждена на заседании учебно-методической комиссии факультета математики и компьютерных наук
протокол № 3 «14» мая 2024 г.

Председатель УМК факультета/института Шмалько С.П. 

Рецензенты:
Крамаренко Т.А. к.п.н. доцент кафедры системного анализа и обработки информации КубГАУ
Лежнев А. В. 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, формируемой участниками образовательных отношений Блока 1 "Дисциплины (модули)" учебного плана дисциплина по выбору Б1.В.ДВ.04.02.

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 профессиональных компетенций (ПК)

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
ПК-1 Способен демонстрировать базовые знания математических и естественных наук, основ программирования и информационных технологий	
ПК-1.1 Способен решать актуальные и важные задачи фундаментальной и прикладной математики ПК-1.2 Демонстрирует навыки программирования подготовленных алгоритмов решения вычислительных задач, разработки структуры и программирования реляционных баз данных, а также экспертных систем ПК-1.4 Собирает и анализирует научно- техническую информацию с учетом базовых представлений, полученных в области	Знать: О компьютерной реализации информационных объектов. Связи компьютерной алгебры и численного анализа Уметь: Применять основные математиче-ские методы, используемые в анализе типовых алгоритмов Владеть навыками: использования библиотеки алгоритмов и пакетов расширения; поиска и использования современной научно-технической литературой в области символьных вычислений.

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
фундаментальной математики, механики, естественных наук, программирования и информационных технологий	
ПК-5 Способен использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования	
ПК-5.1 Анализирует поставленные задачи и выбирает эффективные математические методы при создании алгоритмов и вычислительных программ для решения современных задач математики и механики ПК-5.2 Описывает математические модели, формулирует, теоретически обосновывает и реализует программно численные методы для решения поставленных задач ПК-5.3 Применяет в профессиональной деятельности методику исследования и создания новых моделей, методов и технологий в математике, механике и естественных науках	Знать: О компьютерной реализации информационных объектов. Связи компьютерной алгебры и численного анализа. об этапах развития криптографии; о видах информации, подлежащей шифрованию; о классификации шифров; о методах криптографического синтеза и анализа; о применениях криптографии в решении задач аутентификации, построения систем цифровой подписи; Уметь: Определять структуры данных в компьютерной алгебре. использовать технику символьных вычислений. требования к шифрам и основные характеристики шифров; принципы построения современных шифрсистем. Владеть: классификации систем компьютерной алгебры; ориентироваться в типовых архитектурах вычислительных процессов; использования библиотеки алгоритмов и пакетов расширения; криптографической терминологией

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)			
		6			
Контактная работа, в том числе:					
Аудиторные занятия (всего):	**52**	**52**			
Занятия лекционного типа	18	18	-	-	-
Лабораторные занятия	34	34	-	-	-
Занятия семинарского типа (семинары, практические занятия)			-	-	-
Иная контактная работа:					
Контроль самостоятельной работы (КСР)	14	14			
Промежуточная аттестация (ИКР)	0,3	0,3			
Курсовая работа	7	7	-	-	-
Самостоятельная работа, в том числе:	**51**	**51**			
Проработка учебного (теоретического) материала	12	12	-	-	-

Выполнение индивидуальных заданий (подготовка сообщений, презентаций)		12	12	-	-	-
Реферат				-	-	-
Интер часы		16	16			
Подготовка к текущему контролю		11	11	-	-	-
Контроль:						
Подготовка к зачету		-	-			
Общая трудоемкость	**час.**	**108**	**108**	**-**	**-**	**-**
	в том числе контактная работа	**66,3**	**66,3**			
	зач. ед	**4**	**4**			

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	Понятие о компьютерной алгебре. Пакеты компьютерной алгебры. Пакеты на открытом коде.	22	4		8	10
2	Структуры данных в компьютерной алгебре. Техника символьных вычислений.	22	4		8	10
3	Модели шифров. Блочные и поточные шифры. Понятие криптосистемы.	29	4		8	17
4	Поточные шифры. Синронизированные и самосинхронизующиеся. Надежность шифров.	30	6		10	14
	Итого по дисциплине:		18		34	51

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 конструкции в теории защиты информации и	Определение и основные свойства колец. Евклидовы кольца. Кольца многочленов. Фактор кольца. Кольца вычетов. Многочлены над	Р

	теории кодов	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.	Р

		Характеризация совершенных 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 распространения 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).

2.3.4 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

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 № 9 от 18 мая 2024 г.
2	Самостоятельное освоение теории	Рожков А.В. «Комментарии к лекциям по криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 9 от 18 мая 2024
3	Решение задач	Рожков А.В. «Решебник типовых задач по криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 9 от 18 мая 2024
4	Решение задач	Рожков А.В. «Алгебраические методы криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 9 от 18 мая 2024

1. Методические указания для подготовки к занятиям лекционного и семинарского типа. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 9 от 18 мая 2024 г.

2. Методические указания по выполнению самостоятельной работы обучающихся. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 9 от 18 мая 2024 г.

3. Методические указания по использованию интерактивных методов обучения. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 9 от 18 мая 2024 г.

4. Методические указания по подготовке эссе, рефератов, курсовых работ. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 9 от 18 мая 2024 г.

5. Методические указания по выполнению лабораторных работ. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 9 от 18 мая 2024 г.

6. Методические указания по выполнению расчетно-графических заданий. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ

ВО «КубГУ». Протокол № 9 от 18 мая 2024 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,

3. Образовательные технологии.

Активные и интерактивные формы лекционных занятий, практических занятий, контрольных работ, тестовых заданий, типовых расчетов, докладов, сдача экзамена.

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
3	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.

В рамках реализации компетентностного подхода предусматриваются следующие основные виды активных и интерактивных форм проведения учебных занятий, которые указываются в рабочих программах дисциплин, профессиональных модулей, практик в рамках которых они реализуются:

– применение электронных образовательных ресурсов;

– компьютерные симуляции;

– анализ производственных ситуаций;

Практические занятия с запланированными ошибками. После объявления темы преподаватель сообщает, что в ней будет сделано определенное количество ошибок различного типа: содержательные, методические, поведенческие и т. д. Студенты в конце лекции должны назвать ошибки.

Визуализация. В данном типе занятий передача преподавателем информации студентам сопровождается показом различных рисунков, структурно-логических схем, опорных конспектов, диаграмм и т. п. с помощью ТСО и ЭВМ (слайды, видеозапись, дисплеи, интерактивная доска и т. д.).

Разбором конкретных ситуаций по форме организации похожа на дискуссию, в которой вопросы для обсуждения заменены конкретной ситуацией, предлагаемой обучающимся для анализа в устной или письменной форме. Обсуждение конкретной ситуации может служить прелюдией к дальнейшей традиционной лекции и использоваться для акцентирования внимания аудитории на изучаемом материале.

Коллоквиум – вид учебных занятий, представляющий собой обсуждение под руководством преподавателя широкого круга проблем, например, относительно самостоятельного большого раздела лекционного курса или отдельных частей какой-либо конкретной темы. Он может включать вопросы и темы из изучаемой дисциплины, не включенные в темы практических и семинарских занятий. Коллоквиум может проводиться в форме индивидуальной беседы преподавателя со студентом или как групповое обсуждение.

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 $M_2(\mathbf{Z}_{12})$ линейное уравнение.
3. Сколько элементов содержит кольцо $M_2(\mathbf{Z}_{12})$.
4. Перечислить идеалы кольца $M_2(\mathbf{Z}_4)$
5. Найти НОД двух многочленов в кольце $\mathbf{Z}_{11}[x]$.
6. Найти группу обратимых элементов в кольце $\mathbf{Z}_{24}$.
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 $\{a, b, c\}$).
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.

Критерии оценивания результатов обучения

Оценка	Критерии оценивания по экзамену
Высокий уровень «5» (отлично)	оценку «отлично» заслуживает студент, освоивший знания, умения, компетенции и теоретический материал без пробелов; выполнивший все задания, предусмотренные учебным планом на высоком качественном уровне; практические навыки профессионального применения освоенных знаний сформированы.
Средний уровень «4» (хорошо)	оценку «хорошо» заслуживает студент, практически полностью освоивший знания, умения, компетенции и теоретический материал, учебные задания не оценены максимальным числом баллов, в основном сформировал практические навыки.
Пороговый	оценку «удовлетворительно» заслуживает студент, частично с

уровень «3» (удовлетворительно)	пробелами освоивший знания, умения, компетенции и теоретический материал, многие учебные задания либо не выполнил, либо они оценены числом баллов близким к минимальному, некоторые практические навыки не сформированы.
Минимальный уровень «2» (неудовлетворительно)	оценку «неудовлетворительно» заслуживает студент, не освоивший знания, умения, компетенции и теоретический материал, учебные задания не выполнил, практические навыки не сформированы.

Критерии оценивания по зачету:

«зачтено»: студент владеет теоретическими знаниями по данному разделу, знает формы допускает незначительные ошибки; студент умеет правильно объяснять материал, иллюстрируя его примерами

«не зачтено»: материал не усвоен или усвоен частично, студент затрудняется привести примеры, довольно ограниченный объем знаний программного материала.

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.

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

5.1 Основная литература:

1. Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В. Введение в теоретико-числовые методы криптографии, 3-е изд. [Электронный ресурс]. - СПб.: Лань, 2024. - https://reader.lanbook.com/book/367010
2. Рябко Б.Я, Фионов А.Н. Криптографические методы защиты информации, 2-е изд. [Электронный ресурс]. – М.: Горячая линия-Телеком, 2017. - URL: https://e.lanbook.com/reader/book/111097

5.2 Дополнительная литература:

1. Мартынов Л.М. Алгебра и теория чисел для криптографии: учебное пособие, 3-е изд. [Электронный ресурс]. - СПб.: Лань, 2024. - URL: https://reader.lanbook.com/book/362942
2. Рацеев С.М. Математические методы защиты информации, 2-е изд. [Электронный ресурс]. - СПб.: Лань, 2023. - URL: https://reader.lanbook.com/book/ 326153
3. Рацеев С.М. Математические методы защиты информации и их основы. Сборник задач: Учебное пособие для вузов [Электронный ресурс]. - СПб.: Лань, 2024. - URL: https://reader.lanbook.com/book/292913

5.3 Периодические издания:

Не предусмотрены

6. 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/

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:

в) Перечень свободно распространяемого программного обеспечения

№	Перечень свободно распространяемого программного обеспечения
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.	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 9.5. 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 2018.3. https://www.kali.org/
15.	Анализ защищенности сети Snort 3.0. Официальный сайт https://www.snort.org/
16.	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 соответствующим программным обеспечением (ПО) Программы, демонстрации видео материалов (проигрыватель «Windows Media Player»). Программы для демонстрации и создания презентаций («Microsoft Power Point»).
2.	Семинарские занятия	Не предусмотрены
3.	Лабораторные занятия	Лаборатория, укомплектованная специализированной мебелью и техническими средствами обучения – компьютерами с предустановленными GAP и Sage
4.	Курсовое проектирование	Не предусмотрено
5.	Групповые (индивидуальные) консультации	Аудитория для групповых занятий
6.	Текущий контроль, промежуточная аттестация	Аудитория для групповых занятий
7.	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.