

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

подпись

«26» мая 2023 г.



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.ДВ.02.01 КОМПЬЮТЕРНАЯ АЛГЕБРА И
КРИПТОГРАФИЯ

Направление подготовки 01.03.01 Математика

Направленность (профиль) Математическое моделирование

Форма обучения очная

Квалификация бакалавр

Краснодар 2023

Рабочая программа дисциплины Компьютерная алгебра и криптография составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 01.03.01 Математика

Программу составил(и):

А.В. Рожков, профессор, д.ф.-м.н., профессор



Рабочая программа дисциплины Компьютерная алгебра и криптография утверждена на заседании кафедры функционального анализа и алгебры, протокол № 8 «18» апреля 2023 г.

Заведующий кафедрой Барсукова В.Ю.



Утверждена на заседании учебно-методической комиссии факультета математики и компьютерных наук протокол № 3 «20» апреля 2023 г.

Председатель УМК факультета/института Шмалько С.П.



Рецензенты:

Ганижева Л.Л. к.т.н., доцент кафедры наземного транспорта и механики КубГТУ

Иванисова О. В., кандидат физ.-мат. наук, доцент кафедры вычислительной математики и информатики КубГУ

1 Цели и задачи изучения дисциплины (модуля).

1.1 Цель освоения дисциплины.

Цель освоения дисциплины – рассматривает задачи информатизации и 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 «Компьютерная алгебра и криптография»: получение базовых теоретических и исторических сведений о структуре и алгоритмах функционирования криптоалгоритмов. 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:

- о нормативных требованиях по административно-правовому регулированию в области криптографической защиты информации;
- об основных задачах и понятиях криптографии;
- 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;
- о методах криптозащиты компьютерных систем и сетей.

1.3 Место дисциплины (модуля) в структуре образовательной программы.

Дисциплина «Компьютерная алгебра и криптография» относится к части, формируемой участниками образовательных отношений Блока 1 "Дисциплины (модули)" учебного плана.

Данная дисциплина, как математическая основа теории защищенных информационных систем, призвана содействовать фундаментализации образования, укреплению правосознания и развитию системного мышления студентов.

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 решать актуальные и важные задачи фундаментальной и прикладной математики	
ПК-1.1 Знает основные понятия, идеи и методы фундаментальных математических дисциплин для решения базовых задач ПК-1.2 Умеет передавать результаты проведенных теоретических и прикладных исследований в виде конкретных предметных рекомендаций в терминах предметной области	Знать: О компьютерной реализации информационных объектов. Связи компьютерной алгебры и численного анализа Уметь: Применять основные математические методы, используемые в анализе типовых алгоритмов Владеть навыками: использования библиотеки алгоритмов и пакетов расширения;

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине (знает, умеет, владеет (навыки и/или опыт деятельности))
ПК-1.4 Имеет навыки решения математических задач, соответствующих квалификации, возникающих при проведении научных и прикладных исследований	поиска и использования современной научно-технической литературой в области символьных вычислений.
ПК-4 Способен разрабатывать программное обеспечение для решения прикладных задач в сфере профессиональной деятельности	
ПК-4.1 Имеет навыки использования современных языков программирования для разработки программного обеспечения ПК-4.4 Ориентируется в современных алгоритмах компьютерной математики и имеет практический опыт разработки программных модулей на основе математических моделей	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)			
		5			
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)	6	6			
Промежуточная аттестация (ИКР)	0,3	0,3			
				-	-
Самостоятельная работа, в том числе:	50	50			
Проработка учебного (теоретического) материала	18	18	-	-	-

Выполнение индивидуальных заданий (подготовка сообщений, презентаций)	10	10	-	-	-
Реферат	10	10	-	-	-
Подготовка к текущему контролю	12	12	-	-	-
Контроль:					
Подготовка к экзамену	35,7	35,7			
Общая трудоемкость	час.	144	144	-	-
	в том числе контактная работа	58,3	58,3		
	зач. ед	4	4		

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 5 семестре (очная форма)

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	
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.	22	4		8	10
4	Поточные шифры. Синхронизированные и самосинхронизирующиеся. Надежность шифров.	36	6		10	20
	<i>Итого по разделам дисциплины:</i>	102	18		34	50
	Контроль самостоятельной работы (КСР)	6				
	Промежуточная аттестация (ИКР)	0,3				
	Подготовка к текущему контролю	35,7				
	Общая трудоемкость по дисциплине	144				

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	Понятие о компьютерной алгебре. Пакеты компьютерной алгебры. Пакеты на открытом коде.	Компьютерная алгебра и численный анализ. Точная, целочисленная и полиномиальная арифметика. Системы компьютерной алгебры. Функциональное назначение. Тип архитектуры. Средства реализации. Область применения. Интегральные оценки качества. Пакеты компьютерной алгебры Maple 2017, PARI/GT 2.9, GAP4r8p8, Sage 8.1. Обзор их возможностей и сравнение функционала. Расширение состава встроенных и программируемых типов математических объектов. Интеграция	Р

		СКА с другими компьютерными системами. Унификация и объектная ориентация интерфейса пользователя. Программирование символьных вычислений произвольной сложности. Ускорение работы СКА.	
2	Структуры данных в компьютерной алгебре. Техника символьных вычислений.	Базовые структуры данных в Sage Списки (list), динамические массивы. Перечисления (tuples). Словарь или ассоциативный массив (dictionary). Функции и Функции языка Python. Условные операторы, циклы, символьные выражения, алгебраические структуры, матрицы, векторные пространства. Структуры данных в GAP. Константы и операторы, Переменные и присваивания, Функции, Списки, Тожественность и равенство списков, Множества, Векторы и матрицы, Записи, Арифметические прогрессии, Использование циклов.	Р
3	Модели шифров. Блочные и поточные шифры. Понятие криптосистемы.	Ручные и машинные шифры. Ключевая система шифра. Основные требования к шифрам. Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты. Криптоанализ шифров перестановки. Одно алфавитные и многоалфавитные замены. Вопросы криптоанализа простейших шифров замены. Стандартные алгоритмы криптографической защиты данных.	Э
4	Поточные шифры. Синхронизированные и самосинхронизирующиеся. 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 совершенных шифров с минимальным числом ключей. Безусловно стойкие и вычислительно стойкие шифры.	Р

2.3.3 Лабораторные занятия.

№	Наименование лабораторных работ	Форма текущего контроля
1	3	4
1	Интегральные оценки качества. Пакеты компьютерной алгебры Maple 2017, PARI/GT 2.9, GAP4r8p8, Sage 8.1. Обзор их возможностей и сравнение функционала.	Р
2	Расширение состава встроенных и программируемых типов математических объектов. Интеграция СКА с другими компьютерными	Р

	системами. Унификация и объектная ориентация интерфейса пользователя	
3	Базовые структуры данных в Sage Списки (list), динамические массивы. Перечисления (tuples). Словарь или ассоциативный массив (dictionary). Функции и Функции языка Python.	Э
4	Структуры данных в GAP. Константы и операторы, Переменные и присваивания, Функции, Списки, Тожественность и равенство списков, Множества, Векторы и матрицы, Записи, Арифметические прогрессии, Использование циклов.	Р
5	Ручные и машинные шифры. Ключевая система шифра. Основные требования к шифрам. Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты.	Р
6	Криптоанализ шифров перестановки. Одно алфавитные и многоалфавитные замены. Вопросы криптоанализа простейших шифров замены.	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	Методические указания по выполнению самостоятельной работы обучающихся. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 3 от 20 апреля 2023 г.
2	Самостоятельное освоение теории	Методические указания по выполнению лабораторных работ. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 3 от 20 апреля 2023 г.
3	Решение задач	Методические указания по выполнению самостоятельной работы обучающихся. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 3 от 20 апреля 2023 г.
4	Решение задач	Методические указания по выполнению самостоятельной работы обучающихся. Утверждены на заседании Совета факультета математики и компьютерных наук ФГБОУ ВО «КубГУ». Протокол № 3 от 20 апреля 2023 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, 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 «Компьютерная алгебра и криптография» 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).

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

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «Компьютерная алгебра и криптография».

Структура оценочных средств для текущей и промежуточной аттестации

№ п/п	Код и наименование индикатора (в соответствии с п. 1.4)	Результаты обучения (в соответствии с п. 1.4)	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1	ИПК-1.1 Знает основные понятия, идеи и методы фундаментальных математических дисциплин для решения базовых задач ИПК-1.2 Умеет передавать результаты проведенных теоретических и прикладных исследований в виде конкретных предметных рекомендаций в терминах предметной области	Знать: О компьютерной реализации информационных объектов.	Доклад	Вопросы к экзамену
		Связи компьютерной алгебры и численного анализа	контрольная работа	Вопросы к экзамену
		Уметь: Применять основные математические методы, используемые в анализе типовых алгоритмов	Доклад	Вопросы к экзамену

	ИПК-1.4 Имеет навыки решения математических задач, соответствующих квалификации, возникающих при проведении научных и прикладных исследований			
2	ПК-4.1 Имеет навыки использования современных языков программирования для разработки программного обеспечения ПК-4.4 Ориентируется в современных алгоритмах компьютерной математики и имеет практический опыт разработки программных модулей на основе математических моделей	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;	Доклад, контрольная работа	Вопросы к экзамену
		Уметь: Определять структуры данных в компьютерной алгебре. использовать технику символьных вычислений. требования к шифрам и основные характеристики шифров; принципы построения современных шифрсистем.	Доклад	Вопросы к экзамену
		Владеть: классификации систем компьютерной алгебры; ориентироваться в типовых архитектурах вычислительных процессов; использования библиотеки алгоритмов и пакетов расширения; криптографической терминологией	Доклад	Вопросы к экзамену

4.1 Фонд оценочных средств для проведения текущего контроля.

Список теоретических вопросов (для подготовки к экзамену)

1. Константы и операторы в GAP и Sage.
2. Переменные и присваивания.
3. Функции.
4. Списки - тождественность и равенство списков.
5. Множества, Векторы и матрицы.
6. Записи.
7. Использование циклов.
8. Алгоритм пополнения.
9. Теорема Кнута – Бендикса.
10. Защита персональных данных.
11. История криптографии; классические шифры, шифры гаммирования.
12. Принципы построения криптографических алгоритмов.

13. Различие между программными и аппаратными реализациями шифров.
14. Функция Эйлера и Мебиуса.
15. Группы обратимых элементов в кольцах.
16. Структура мультипликативной группы кольца вычетов.
17. Обратимые элементы.
18. Примитивные элементы.
19. Особенности использования вычислительной техники в криптографии вопросы организации сетей засекреченной связи.
20. Криптографические хеш-функции.
21. Электронная подпись.
22. Криптографические протоколы.
23. Предмет и задачи программно-аппаратной защиты информации.
24. Идентификация субъекта, понятие протокола идентификации.
25. Пароли и ключи, организация хранения ключей.

2.3.4 Примерная тематика курсовых работ (проектов)

1. Освоение процессов зашифрования и расшифрования для простейших шифров.
2. Свойства простейших шифров.
3. Расчет мощности ключевой системы различных шифров.
4. Оценка расстояния единственности для простейших шифров.
5. Криптоанализ шифра Виженера.
6. Расчет характеристик метода перебора ключей.
7. Вычисление характеристик двоичных функций.
8. Анализ схемы DES при небольшом числе итераций.
9. Вычисление характеристик датчиков псевдослучайных чисел.
10. Применение тестов на простоту целых чисел.
11. Изучение свойств алгоритма RSA.
12. Анализ некоторых алгоритмов выработки хэш-функций.
13. Методы и средства хранения ключевой информации
14. Протоколы аутентификации PAP и CHAP.
15. Система аутентификации и авторизации Kerberos.

4.2 Фонд оценочных средств для проведения промежуточной аттестации.

Список типовых алгоритмов (для самостоятельных и лабораторных занятий)

1. Применения и разработки шифровальных средств.
2. Применения электронной подписи.
3. Криптографические методы обеспечения информационной безопасности.
4. Алгоритмы проверки на простоту.
5. Эллиптические кривые над конечными полями
6. Алгоритмы вычисления в конечных полях.
7. Электронная подпись по схеме Эль Гамала.
8. Электронная подпись на основе RSA.
9. Случайные и псевдослучайные гаммы.
10. Регистры сдвига с обратной связью.
11. Схема Файстеля.
12. Подсчет количества точек на эллиптической кривой.
13. Операция сложения на эллиптической кривой.
14. Схема алгоритма RSA.
15. Криптограммы, полученные при повторном использовании ключа.
16. Нахождение примитивного элемента конечного поля.
17. Построение таблицы логарифма Якоби конечного поля.
18. Решение систем линейных уравнений над конечным полем.

19. Алгоритм быстрого возведения в степень.
20. Нахождение обратных элементов в конечном поле.
21. Расширения конечных полей.
22. Алгоритм шифрования AES: структура поля $GF(2^8)$, нахождение обратных элементов.
23. Алгоритм шифрования AES: фактор кольцо $GF(2^8)[x]/\text{ид}((x+1)^4)$, преобразование столбцов.
24. Алгоритм шифрования AES: Линейное преобразование, собственные значения матрицы.
25. Алгоритм RSA – выбор секретных параметров p, q, d , вычисление открытого ключа n, e .
26. Рюкзачная система шифрования. Быстрорастущий вектор. Соккрытие быстрорастущего вектора после преобразования умножения по модулю.
27. Решение систем линейных уравнений по разным модулям.
28. Решение систем линейных уравнений в кольце целых чисел.
29. Линейный регистр сдвига с обратной связью

$$S_{n+k} = a_{k-1}S_{n+k-1} + a_{k-2}S_{n+k-2} + \dots + a_1S_{n+1} + a_0S_n + a, n = 0, 1, 2, \dots$$
30. Характеристический многочлен регистра сдвига $x^k = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \dots + a_1x + a_0$
31. Матрица линейного регистра сдвига ее собственные значения и жорданова форма.
32. Квадратичный закон взаимности. Вычисление квадратичных вычетов и невычетов.
33. Извлечение квадратных корней по простому модулю $p \equiv 3 \pmod{4} \Rightarrow p = 4k + 3$.
34. Извлечение квадратных корней по простому модулю $p \equiv 1 \pmod{4} \Rightarrow p = 4k + 1$.
35. Криптоанализ шифра однобуквенной простой замены.
36. Криптоанализ системы шифрования RSA при неправильном выборе модуля.
37. Вскрытие шифра Вернама при повторном использовании ключа.

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 уровень «3» (удовлетворительно)	оценку «удовлетворительно» заслуживает студент, частично с 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»	оценку «неудовлетворительно» заслуживает студент, не освоивший знания, умения, компетенции и теоретический материал, учебные задания не выполнил, практические навыки не сформированы.

(неудовлетворительно)	
-----------------------	--

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. Торстейнсон П., Ганеш Г.А. Криптография и безопасность в технологии .NET. 4-е изд. [Электронный ресурс]. – М.: Лаборатория знаний, 2020. – URL: <https://e.lanbook.com/reader/book/151552>
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. Столов Е.Л. Цифровая обработка сигналов. Водяные знаки в аудиофайлах [Электронный ресурс]. - СПб.: Лань, 2021. - URL: <https://e.lanbook.com/reader/book/169170>
2. Конова Е.А., Поллак Г.А. Алгоритмы и программы. Язык C++, 3-е изд. [электронный ресурс] – М.: Издательство "Лань", 2018. – URL: <https://e.lanbook.com/reader/book/103905>

5.3 Периодические издания:

Не предусмотрены

5.4. 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.uceba.com/>;
14. Законопроект "Об образовании в Российской Федерации". Вопросы и ответы http://xn--273--84d1f.xn--p1ai/voprosy_i_otvety

Собственные электронные образовательные и информационные ресурсы

КубГУ:

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

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

Согласно учебному плану дисциплины «Компьютерная алгебра и криптография» 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.

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

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

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения
Учебные аудитории для проведения занятий лекционного типа	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер	Microsoft Windows 8, 10 Microsoft Office Professional Plus Kaspersky Endpoint Security для бизнеса
Учебные аудитории для проведения занятий семинарского типа, групповых и	Мебель: учебная мебель Технические средства обучения:	Microsoft Windows 8, 10 Microsoft Office Professional Plus

индивидуальных консультаций, текущего контроля и промежуточной аттестации	экран, проектор, компьютер	Kaspersky Endpoint Security для бизнеса
Учебные аудитории для проведения лабораторных работ.	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер	Microsoft Windows 8, 10 Microsoft Office Professional Plus Kaspersky Endpoint Security для бизнеса
Учебные аудитории для выполнения курсовых работ	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютер	Microsoft Windows 8, 10 Microsoft Office Professional Plus Kaspersky Endpoint Security для бизнеса MATLAB Wavelet Toolbox WolframResearch Mathematica MapleSoft Maple 18 PTC Mathcad

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

Наименование помещений для самостоятельной работы обучающихся	Оснащенность помещений для самостоятельной работы обучающихся	Перечень лицензионного программного обеспечения
Помещение для самостоятельной работы обучающихся (читальный зал Научной библиотеки)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	Microsoft Windows 8, 10 Microsoft Office Professional Plus Kaspersky Endpoint Security для бизнеса
Помещение для самостоятельной работы обучающихся (ауд.314)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-	Microsoft Windows 8, 10 Microsoft Office Professional Plus Kaspersky Endpoint Security для бизнеса MATLAB Wavelet Toolbox

	коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	WolframResearch Mathematica MapleSoft Maple 18 PTC Mathcad
--	--	--