УТВЕРЖДЕНО

решением Ученого совета факультета математики,
информационных и авиационных технологий
от «21» 05 2024г., протокол № 5/24
Председатель _____ Волков М.А.
«21» 05 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина	**Вычислительные методы в алгебре и теории чисел**
Факультет	Факультет математики, информационных и авиационных технологий
Кафедра	Кафедра информационной безопасности и теории управления
Курс	2

Направление (специальность): 10.05.03 Информационная безопасность автоматизированных систем
Направленность (профиль/специализация): Безопасность открытых информационных систем
Форма обучения: очная
Дата введения в учебный процесс УлГУ: 01.09.2024 г.
Программа актуализирована на заседании кафедры: протокол № 10 от 15.04 2024 г.
Программа актуализирована на заседании кафедры: протокол №_____ от _____ 20___г.
Программа актуализирована на заседании кафедры: протокол №_____ от _____ 20___г.

Сведения о разработчиках:

ФИО	КАФЕДРА	Должность, ученая степень, звание
Рацеев Сергей Михайлович	Кафедра информационной безопасности и теории управления	Профессор,Доктор физико-математических наук, Доцент

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины:

- обеспечение подготовки в одной из важных областей, находящихся на границе теории чисел, алгебры, информатики и криптографии;
- освоение основных методов разработки алгоритмов для решения задач, возникающих как в самой теории чисел и таких приложениях, как криптография.

Задачи освоения дисциплины:

- овладение основными вычислительными методами классической и современной теории чисел;
- овладение методами теоретико-числового характера;
- выявление различных приложений теории чисел.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Вычислительные методы в алгебре и теории чисел» относится к числу дисциплин блока Б1.О.1, предназначенного для студентов, обучающихся по направлению: 10.05.03 Информационная безопасность автоматизированных систем.

В процессе изучения дисциплины формируются компетенции: ОПК-3.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: Теория кодирования, сжатия и восстановления информации, Методы и средства криптографической защиты информации, Теория псевдослучайных генераторов, Вычислительные методы в алгебре и теории чисел, Математическая логика и теория алгоритмов, Дифференциальные уравнения, Алгебра и геометрия, Теория вероятностей, Математический анализ, Научно-исследовательская работа, Численные методы, Ознакомительная практика, Методы алгебраической геометрии в криптографии, Избранные вопросы математического анализа, Проектная деятельность, Подготовка к сдаче и сдача государственного экзамена.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
ОПК-3 Способен использовать математические методы, необходимые для решения задач профессиональной деятельности;	**знать**: основные методы решения алгоритмических проблем, возникающих в теории чисел и в их приложениях к решению практических задач; формировать алгоритмическое мировоззрение, творческое мышление и навыки в проведении самостоятельных научных исследований **уметь**:

Код и наименование реализуемой компетенции	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций
	применять изученные математические методы при решении профессиональных задач и задач с практическим содержанием **владеть**: математическим аппаратом, изученным в данном курсе

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

4.1. Объем дисциплины в зачетных единицах (всего): 7 ЗЕТ

4.2. Объем дисциплины по видам учебной работы (в часах): 252 часа

Форма обучения: очная

Вид учебной работы	Количество часов (форма обучения очная)		
	Всего по плану	В т.ч. по семестрам	
		3	4
1	2	3	4
Контактная работа обучающихся с преподавателем в соответствии с УП	134	54	80
Аудиторные занятия:	134	54	80
Лекции	50	18	32
Семинары и практические занятия	52	36	16
Лабораторные работы, практикумы	32	-	32
Самостоятельная работа	82	54	28
Форма текущего контроля знаний и контроля самостоятельной работы: тестирование, контр. работа, коллоквиум, реферат и др. (не менее 2 видов)	Тестирование, Проверка решения задачи (выполнения задания), контрольные работы, Оценивание выполнения задания	Тестирование, Проверка решения задачи (выполнения задания), контрольные работы, Оценивание выполнения задания	
Курсовая работа	-	-	-
Виды промежуточной аттестации (экзамен, зачет)	Зачет, Экзамен (24)	Зачет	Экзамен
Всего часов по дисциплине	252	108	144

4.3. Содержание дисциплины. Распределение часов по темам и видам учебной работы

Форма обучения: очная

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
Раздел 1. Алгебраические структуры							
Тема 1.1. Группы	48	8	16	0	0	24	Вопросы к Экзамену, Проверка решения задачи (выполнения задания), Оценивание выполнения задания
Тема 1.2. Кольца.	36	6	12	0	0	18	Вопросы к Экзамену, Проверка решения задачи (выполнения задания), Оценивание выполнения задания
Тема 1.3. Поля.	24	4	8	0	0	12	Вопросы к Экзамену, Проверка решения задачи (выполнения задания), Оценивание выполнения задания
Раздел 2. Теория чисел							
Тема 2.1. Разложение по модулю.	18	4	2	8	8	4	Вопросы к Экзамену, Тестирование, Контрольные работы

Название разделов и тем	Всего	Виды учебных занятий					Форма текущего контроля знаний
		Аудиторные занятия			Занятия в интерактивной форме	Самостоятельная работа	
		Лекции	Практические занятия, семинары	Лабораторные работы, практикумы			
1	2	3	4	5	6	7	8
Тема 2.2. Диофантовы уравнения первой степени.	18	4	2	8	0	4	Вопросы к Экзамену, Тестирование, Контрольные работы
Тема 2.3. Простые числа. Факторизация.	10	4	2	0	0	4	Вопросы к Экзамену, Тестирование
Тема 2.4. Цепные дроби.	18	4	2	8	0	4	Вопросы к Экзамену, Тестирование, Контрольные работы
Тема 2.5. Бесконечные цепные дроби.	10	4	2	0	0	4	Вопросы к Экзамену, Оценивание выполнения задания
Тема 2.6. Мультипликативные функции.	10	4	2	0	0	4	Вопросы к Экзамену, Тестирование
Тема 2.7. Сравнения.	16	4	2	8	4	2	Вопросы к Экзамену, Тестирование
Тема 2.8. Сравнения первой степени.	8	4	2	0	0	2	Вопросы к Экзамену, Тестирование
Итого подлежит изучению	216	50	52	32	12	82	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Алгебраические структуры

Тема 1.1. Группы

Алгебраические операции. Группы. Основные свойства группы. Подгруппы. Эквивалентные условия подгруппы. Циклическая группа. Свойства циклических групп. Смежные классы. Индекс подгруппы. Теорема Лагранжа. Нормальная подгруппа. Эквивалентные условия нормальной подгруппы. Фактор-группа. Морфизмы групп. Ядро и образ гомоморфизма. Теорема о гомоморфизме групп.

Тема 1.2. Кольца.

Кольца. Мультипликативная группа кольца. Подкольца. Критерий подкольца. Идеал кольца. Фактор-кольцо. Кольца вычетов. Морфизмы колец. Ядро и образ гомоморфизма. Теорема о гомоморфизме колец. Кольца главных идеалов. Китайская теорема об остатках для идеалов колец. Разложение кольца вычетов в прямую сумму примарных колец.

Тема 1.3. Поля.

Поле. Подполе. Простое поле. Характеристика поля. Простые идеалы. Поле частных. Расширение поля. Теорема о башне расширений. Конечные расширения. Алгебраические и трансцендентные элементы. Минимальный многочлен алгебраического элемента, некоторые его свойства. Строение расширения поля, полученное присоединением алгебраического элемента. Поля разложения многочлена. Конечные поля.

Раздел 2. Теория чисел

Тема 2.1. Разложение по модулю.

Теорема о разложении одного целого числа по модулю другого (основная теорема делимости целых чисел). q-ичные системы счисления (представление и единственность). Отношение делимости в кольце целых чисел и его свойства. Наибольший общий делитель и его свойства. Алгоритм Евклида. Обобщенный алгоритм Евклида. Взаимно простые числа и их свойства.

Тема 2.2. Диофантовы уравнения первой степени.

Линейные диофантовы уравнения первой степени. Критерий существования решения. Формула общего решения. Наименьшее общее кратное и его свойства. Формула для наименьшего общего кратного пары целых чисел.

Тема 2.3. Простые числа. Факторизация.

Простые числа и их свойства. Теорема Евклида. Простейшие проверки целого числа на простоту. Решето Эратосфена. Основная теорема арифметики (о разложении целых чисел в произведение простых). Каноническое разложение целого числа. Формулы для наибольшего общего делителя и для наименьшего общего кратного набора целых чисел на основе их канонических разложений. Факторизация числа n!.

Тема 2.4. Цепные дроби.

Конечные цепные дроби. Представление рационального числа конечной цепной дробью. Подходящие дроби, их вычисление и основные свойства.

Тема 2.5. Бесконечные цепные дроби.

Бесконечные цепные дроби. Представление действительных чисел бесконечными цепными дробями.

Тема 2.6. Мультипликативные функции.

Мультипликативные функции и их свойства. Примеры мультипликативных функций. Леммы о мультипликативных функциях. Формулы для количества и суммы делителей целого числа. Функция Мебиуса и ее свойства. Функция Эйлера и формула для ее вычисления.

Тема 2.7. Сравнения.

Отношение сравнимости в кольце целых чисел и его свойства. Полная и приведенная системы вычетов и их свойства. Теорема Эйлера. Теорема Ферма (малая).

Тема 2.8. Сравнения первой степени.

Сравнения первой степени $ax \equiv b \pmod m$, случай $(a, m)=1$. Сравнения первой степени $ax \equiv b \pmod m$, случай $(a, m)>1$. Системы сравнений первой степени. Системы сравнений первой степени и методы их решения. Китайская теорема об остатках. Схема разделения секрета на основе китайской теоремы об остатках.

6. ТЕМЫ ПРАКТИЧЕСКИХ И СЕМИНАРСКИХ ЗАНЯТИЙ

Раздел 1. Алгебраические структуры

Тема 1.1. Группы

Вопросы к теме:

Очная форма

Алгебраические операции. Группы. Основные свойства группы. Подгруппы. Эквива-лентные условия подгруппы. Циклическая группа. Свойства циклических групп. Смежные классы. Индекс подгруппы. Теорема Лагранжа. Нормальная подгруппа. Эквивалентные условия нормальной подгруппы. Фактор-группа. Морфизмы групп. Ядро и образ гомоморфизма. Теорема о гомоморфизме групп.

Тема 1.2. Кольца.

Вопросы к теме:

Очная форма

Кольца. Мультипликативная группа кольца. Подкольца. Критерий подкольца. Идеал кольца. Фактор-кольцо. Кольца вычетов. Морфизмы колец. Ядро и образ гомоморфизма. Теорема о гомоморфизме колец. Кольца главных идеалов. Китайская теорема об остатках для идеалов колец. Разложение кольца вычетов в прямую сумму примарных колец.

Тема 1.3. Поля.

Вопросы к теме:

Очная форма

Поле. Подполе. Простое поле. Характеристика поля. Простые идеалы. Поле частных. Расширение поля. Теорема о башне расширений. Конечные расширения. Алгебраические и трансцендентные элементы. Минимальный многочлен алгебраического элемента, некоторые его свойства. Строение расширения поля, полученное присоединением алгебраического элемента. Поля разложения многочлена. Конечные поля.

Раздел 2. Теория чисел

Тема 2.1. Разложение по модулю.

Вопросы к теме:

Очная форма

q-ичные системы счисления (представление и единственность). Отношение делимости в кольце целых чисел и его свойства. Наибольший общий делитель и его свойства. Алгоритм Евклида. Обобщенный алгоритм Евклида. Взаимно простые числа и их свойства.

Тема 2.2. Диофантовы уравнения первой степени.

Вопросы к теме:

Очная форма

Линейные диофантовы уравнения первой степени. Формула общего решения. Наименьшее общее кратное и его свойства. Формула для наименьшего общего кратного пары целых чисел.

Тема 2.3. Простые числа. Факторизация.

Вопросы к теме:

Очная форма

Простые числа и их свойства. Простейшие проверки целого числа на простоту. Решето Эратосфена. Каноническое разложение целого числа. Формулы для наибольшего общего делителя и для наименьшего общего кратного набора целых чисел на основе их канонических разложений. Факторизация числа n!.

Тема 2.4. Цепные дроби.

Вопросы к теме:

Очная форма

Конечные цепные дроби. Представление рационального числа конечной цепной дробью. Подходящие дроби, их вычисление.

Тема 2.5. Бесконечные цепные дроби.

Вопросы к теме:

Очная форма

Бесконечные цепные дроби. Представление действительных чисел бесконечными цепными дробями.

Тема 2.6. Мультипликативные функции.

Вопросы к теме:

Очная форма

Мультипликативные функции и их свойства. Примеры мультипликативных функций. Леммы о мультипликативных функциях. Формулы для количества и суммы делителей целого числа. Функция Мебиуса и ее свойства. Функция Эйлера и формула для ее вычисления.

Тема 2.7. Сравнения.

Вопросы к теме:

Очная форма

Отношение сравнимости в кольце целых чисел и его свойства. Полная и приведенная системы вычетов и их свойства. Теорема Эйлера. Теорема Ферма (малая).

Тема 2.8. Сравнения первой степени.

Вопросы к теме:

Очная форма

Сравнения первой степени ax ≡ b (mod m), случай (a, m)=1. Сравнения первой степени ax ≡ b (mod m), случай (a, m)>1. Системы сравнений первой степени. Системы сравнений первой степени и методы их решения. Китайская теорема об остатках. Схема разделения секрета на основе китайской теоремы об остатках.

7. ЛАБОРАТОРНЫЕ РАБОТЫ, ПРАКТИКУМЫ

Диофантовы уравнения первой степени
Цели: Целью работы является освоение обобщенного алгоритма Евклида.
Содержание: Требуется составить программу, которая для любых целых чисел a и b, одновременно не равных нулю, находит частное решение уравнения ax+by=(a,b).
Результаты: Основное внимание должно быть уделено освоению обобщенного алгоритма Евклида.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/270
Конечные цепные дроби
Цели: Целью работы является освоение представлений рациональных чисел конечными цепными дробями и представление конечных цепных дробей рациональными числами.
Содержание: Требуется составить программу, которая для любых целых чисел a и b, причем b не равно нулю, представляет рациональное число a/b в виде конечной цепной дроби. И обратно, представить конечную цепную дробь в виде рационального числа вида a/b.
Результаты: Основное внимание должно быть уделено освоению методов представлений рациональных чисел конечными цепными дробями.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/270
Сравнения первой степени
Цели: Целью работы является освоение методов решений сравнений первой степени.
Содержание: Требуется составить программу, которая для любых целых чисел a, b и m, m>0, находит все решения сравнения ax ≡ b (mod m).
Результаты: Основное внимание должно быть уделено освоению методов решений сравнений первой степени.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/270
Системы сравнений первой степени
Цели: Целью работы является освоение методов решений систем сравнений первой степени.
Содержание: Требуется составить программу, которая находит решение системы сравнений первой степени с помощью китайской теоремы об остатках.
Результаты: Основное внимание должно быть уделено освоению методов решений систем сравнений первой степени.
Ссылка: http://lib.ulsu.ru/MegaPro/Download/MObject/270

8. ТЕМАТИКА КУРСОВЫХ, КОНТРОЛЬНЫХ РАБОТ, РЕФЕРАТОВ

Контрольные работы
Тема 1. Найти все решения диофантова уравнения 16x - 42y = 2.
Тема 2. Найти множество общих делителей чисел 36, 90, 240.a = 198; b = 306; c = 550. Найти (a, b, c), [a, b, c].

Тема 3. Найти значение конечной цепной дроби [1;2,2,3,2,3].
Тема 4. Разложить в конечную цепную дробь 121/36.

9. ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ, ЗАЧЕТУ

Вопросы к экзамену

1. Бинарная операция. Полугруппа, моноид. Примеры.
2. Группа. Свойства групп. Примеры групп.
3. Циклические группы. Порядок элемента.
4. Смежные классы по подгруппе. Теорема Лагранжа.
5. Нормальная подгруппа. Факторгруппа. Примеры.
6. Кольцо. Свойства колец. Примеры колец.
7. Идеалы кольца. Факторкольцо.
8. Поле. Свойства полей. Примеры полей.
9. Изоморфизм групп, колец, полей. Свойства изоморфизма.
10. Подгруппа, подкольцо, подполе. Критерий подгруппы, подкольца, подполя.
11. Симметрические многочлены. Основная теорема о симметрических многочленах.
12. Теорема о делении с остатком.
13. q-ичные системы счисления (представление и единственность).
14. Отношение делимости в кольце целых чисел и его свойства.
15. Наибольший общий делитель и его свойства.
16. Алгоритм Евклида. Бинарный алгоритм Евклида.
17. Обобщенный алгоритм Евклида.
18. Взаимно простые числа и их свойства.
19. Наименьшее общее кратное и его свойства.
20. Диофантовы уравнения первой степени. Теорема о существовании решения для уравнений вида a1x1+…+ anxn=(a1,…, an).
21. Критерий существования решения диофантова уравнения первой степени.
22. Простые числа и их свойства.
23. Простейшие проверки целого числа на простоту. Решето Эратосфена.
24. Основная теорема арифметики. Каноническое разложение целого числа.
25. Вычисление н.о.д. и н.о.к. на основе канонического разложения чисел. Нахождение всех делителей целого числа при известном каноническом разложении.
26. Целая часть числа. Каноническое разложение числа n!.
27. Конечные цепные дроби. Представление рационального числа конечной цепной дробью.
28. Подходящие дроби и их вычисление с помощью рекуррентных последовательностей.
29. Бесконечные цепные дроби. Сходимость бесконечных цепных дробей.
30. Разложение действительных чисел в цепные дроби.
31. Мультипликативные функции и их свойства. Примеры мультипликативных функций.
32. Леммы о мультипликативных функциях.
33. Формула суммы и числа делителей целого числа.
34. Функция Мебиуса и ее свойства.
35. Функция Эйлера и ее вычисление.

36. Отношение сравнимости в кольце целых чисел и его свойства.
37. Полная система вычетов и ее свойства.
38. Приведенная система вычетов и ее свойства.
39. Теорема Эйлера. Теорема Ферма.
40. Сравнения первой степени ax ≡ b (mod m). Случай (a, m)=1.
41. Сравнения первой степени ax ≡ b (mod m). Случай (a, m)>1.
42. Системы сравнений 1-й степени и методы их решения. Китайская теорема об остатках.

Вопросы к зачету

1. Бинарная операция. Полугруппа, моноид. Примеры.

2. Группа. Свойства групп. Примеры групп.

3. Циклические группы. Порядок элемента.

4. Смежные классы по подгруппе. Теорема Лагранжа.

5. Нормальная подгруппа. Факторгруппа. Примеры.

6. Кольцо. Свойства колец. Примеры колец.

7. Идеалы кольца. Факторкольцо.

8. Поле. Свойства полей. Примеры полей.

9. Изоморфизм групп, колец, полей. Свойства изоморфизма.

10. Подгруппа, подкольцо, подполе. Критерий подгруппы, подкольца, подполя.

10. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩИХСЯ

Содержание, требования, условия и порядок организации самостоятельной работы обучающихся с учетом формы обучения определяются в соответствии с «Положением об организации самостоятельной работы обучающихся», утвержденным Ученым советом УлГУ (протокол №8/268 от 26.03.2019г.).

По каждой форме обучения: очная/заочная/очно-заочная заполняется отдельная таблица

Форма обучения: очная

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
Раздел 1. Алгебраические структуры			
Тема 1.1. Группы	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	24	Оценивание выполнения задания
Тема 1.2. Кольца.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	18	Оценивание выполнения задания
Тема 1.3. Поля.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	12	Оценивание выполнения задания
Раздел 2. Теория чисел			
Тема 2.1. Разложение по модулю.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование
Тема 2.2. Диофантовы уравнения первой степени.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование
Тема 2.3. Простые числа. Факторизация.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование
Тема 2.4. Цепные дроби.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Тестирование
Тема 2.5. Бесконечные цепные дроби.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	4	Оценивание выполнения задания
Тема 2.6. Мультипликативные функции.	Проработка учебного материала с использованием ресурсов учебно-	4	Тестирование

Название разделов и тем	**Вид самостоятельной работы** ***(проработка учебного материала, решение задач, реферат, доклад, контрольная работа,подготовка к сдаче зачета, экзамена и др).***	**Объем в часах**	**Форма контроля** ***(проверка решения задач, реферата и др.)***
	методического и информационного обеспечения дисциплины.		
Тема 2.7. Сравнения.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование
Тема 2.8. Сравнения первой степени.	Проработка учебного материала с использованием ресурсов учебно-методического и информационного обеспечения дисциплины.	2	Тестирование

11. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) Список рекомендуемой литературы

основная

1. Курош Александр Геннадиевич. Курс высшей алгебры : учебник для вузов по спец. "Математика" / А.Г. Курош. - 17-е изд., стер. - Санкт-Петербург : Лань, 2008. - 432 с. : ил. - (Лучшие классические учебники) (Классическая учебная литература по математике) (Учебники для вузов) (Специальная литература). - Библиогр.: с. 425-426. - ISBN 978-5-8114-0521-3 (в пер.). / .— ISBN 1_176383

2. Рацеев Сергей Михайлович. Элементы высшей алгебры и теории кодирования : учебное пособие для вузов / С.М. Рацеев. - Санкт-Петербург : Лань, 2022. - 656 с. - (Высшее образование). - ISBN 978-5-507-47915-3 (в пер.). / .— ISBN 1_258338

3. Рацеев С. М. Теоретико-числовые методы в криптографии : учебное пособие. Часть 1 / С. М. Рацеев ; УлГУ, ФМИиАТ. - Ульяновск : УлГУ, 2020. - 92 с. / .— ISBN 1_255372

дополнительная

1. Рацеев Сергей Михайлович. Математические методы защиты информации и их основы. Сборник задач : учебное пособие для вузов / С.М. Рацеев. - Санкт-Петербург : Лань, 2023. - 136 с. - (Высшее образование). - Библиогр.: с. 135-136. - ISBN 978-5-507-45197-5 (в пер.). / .— ISBN 1_258183

2. Теория чисел в криптографии : учебное пособие / В.А. Орлов, Н.В. Медведев, Н.А. Шимко, А.Б. Домрачева ; Орлов В.А.; Медведев Н.В.; Шимко Н.А.; Домрачева А.Б. - Москва : МГТУ им. Н.Э. Баумана, 2011. - 223 с. - URL: https://www.studentlibrary.ru/book/ISBN9785703835203.html. - Режим доступа: ЭБС "Консультант студента"; по подписке. - ISBN 978-5-7038-3520-3. / .— ISBN 0_255338

учебно-методическая

1. Рацеев С. М. Методические указания для самостоятельной работы студентов по дисциплине «Вычислительные методы в алгебре и теории чисел» для студентов специальностей 10.05.01 «Компьютерная безопасность» и 10.05.03 «Информационная безопасность автоматизированных систем» / С. М. Рацеев. - 2022. - 8 с. - Неопубликованный ресурс. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/13328. - Режим доступа: ЭБС УлГУ. - Текст : электронный. / .— ISBN 0_475952.

б) Программное обеспечение

- Операционная система "Альт образование"
- Офисный пакет "Мой офис"
- Code::Blocks IDE

в) Профессиональные базы данных, информационно-справочные системы

1. Электронно-библиотечные системы:

1.1. Цифровой образовательный ресурс IPRsmart : электронно-библиотечная система : сайт / ООО Компания «Ай Пи Ар Медиа». - Саратов, [2024]. – URL: http://www.iprbookshop.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.2. Образовательная платформа ЮРАЙТ : образовательный ресурс, электронная библиотека : сайт / ООО Электронное издательство ЮРАЙТ. – Москва, [2024]. - URL: https://urait.ru. – Режим доступа: для зарегистрир. пользователей. - Текст : электронный.

1.3. База данных «Электронная библиотека технического ВУЗа (ЭБС «Консультант студента») : электронно-библиотечная система : сайт / ООО Политехресурс. – Москва, [2024]. – URL: https://www.studentlibrary.ru/cgi-bin/mb4x. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.4. Консультант врача. Электронная медицинская библиотека : база данных : сайт / ООО Высшая школа организации и управления здравоохранением-Комплексный медицинский консалтинг. – Москва, [2024]. – URL: https://www.rosmedlib.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.5. Большая медицинская библиотека : электронно-библиотечная система : сайт / ООО Букап. – Томск, [2024]. – URL: https://www.books-up.ru/ru/library/ . – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.6. ЭБС Лань : электронно-библиотечная система : сайт / ООО ЭБС Лань. – Санкт-Петербург, [2024]. – URL: https://e.lanbook.com. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

1.7. ЭБС **Znanium.com** : электронно-библиотечная система : сайт / ООО Знаниум. - Москва, [2024]. - URL: http://znanium.com . – Режим доступа : для зарегистрир. пользователей. - Текст : электронный.

2. КонсультантПлюс [Электронный ресурс]: справочная правовая система. /ООО «Консультант Плюс» - Электрон. дан. - Москва : КонсультантПлюс, [2024].

3. eLIBRARY.RU: научная электронная библиотека : сайт / ООО «Научная Электронная Библиотека». – Москва, [2024]. – URL: http://elibrary.ru. – Режим доступа : для авториз. пользователей. – Текст : электронный

4. Федеральная государственная информационная система «Национальная электронная библиотека» : электронная библиотека : сайт / ФГБУ РГБ. – Москва, [2024]. – URL: https://нэб.рф. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

5. Российское образование : федеральный портал / учредитель ФГАУ «ФИЦТО». – URL: http://www.edu.ru. – Текст : электронный.

6. Электронная библиотечная система УлГУ : модуль «Электронная библиотека» АБИС Мега-ПРО / ООО «Дата Экспресс». – URL: http://lib.ulsu.ru/MegaPro/Web. – Режим доступа : для пользователей научной библиотеки. – Текст : электронный.

12. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:

Аудитории для проведения лекций, семинарских занятий, для выполнения лабораторных работ и практикумов, для проведения текущего контроля и промежуточной аттестации, курсового проектирования, групповых и индивидуальных консультаций *(выбрать необходимое)*

Аудитории укомплектованы специализированной мебелью, учебной доской. Аудитории для проведения лекций оборудованы мультимедийным оборудованием для представления информации большой аудитории. Помещения для самостоятельной работы оснащены компьютерный техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде, электронно-библиотечной системе. Перечень оборудования, используемого в учебном процессе:

- Мультимедийное оборудование: компьютер/ноутбук, экран, проектор/телевизор
- Компьютерная техника

13. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ДЛЯ ОБУЧАЮЩИХСЯ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением

тифлосурдопереводчика; индивидуальные задания и консультации;

- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;

- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

В случае необходимости использования в учебном процессе частично/исключительно дистанционных образовательных технологий, организация работы ППС с обучающимися с ОВЗ и инвалидами предусматривается в электронной информационно-образовательной среде с учетом их индивидуальных психофизических особенностей.

Разработчик	Доктор физико-математических наук, Доцент	Рацеев Сергей Михайлович
	Должность, ученая степень, звание	ФИО