ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ОРЕНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»

Методические рекомендации для самостоятельной работы обучающихся по дисциплине

Б1.Б.1.09 ДИСКРЕТНАЯ МАТЕМАТИКА

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация Информационная безопасность автоматизированных систем критически важных объектов

Форма обучения очная

СОДЕРЖАНИЕ

1. ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

1.1. Организационно-методические данные дисциплины

№ п.п.	Наименование темы	Общий объем часов по видам самостоятельной работы				
		Промежуточная аттестация	подготовка реферата/ эссе	индивидуальные домашние задания (ИДЗ)	самостоятельное изучение вопросов (СИВ)	подготовка к занятиям (ПкЗ)
1	2	3	4	5	6	7
1	**Тема 4** Эквивалентные множества. Мощность множеств.	×	×	×	5	4
2	**Тема 6** Кольца и поля. Кольцо классов вычетов целых чисел.	×	×	×	5	2
3	**Тема 7** Правила комбинаторики. Комбинаторные формулы.	×	×	×	4	2
4	**Тема 8** Биномиальные коэффициенты и их свойства. Метод включений и исключений. Метод рекуррентных соотношений. Производящие функции.	×	×	×	8	6
5	**Тема 9** Простые числа.	×	×	×	4	2
6	**Тема 10** Уравнения в кольце вычетов. Сравнения первой степени с одним неизвестным. Решение сравнений первой степени. Порядок числа и класса вычетов по модулю. Первообразные корни. Индексы по простому модулю и их приложения. Математические	×	×	×	8	12

	основы криптографии: приложения модульной арифметики в алгоритме RSA.					
	Тема 16 Орграфы и сети. Прикладные задачи и алгоритмы анализа графов и сетей, задачи оптимизации на графах и сетях. ИТ - технологии анализа графов и сетей.				5	4
	Тема 18 Нечёткие отношения и соответствия. Экспертные системы.				5	2
6	**Итого: 120**	**8**	×	×	**44**	**68**

2. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО САМОСТОЯТЕЛЬНОМУ ИЗУЧЕНИЮ ВОПРОСОВ

2.1 Наименование вопроса. Эквивалентные множества. Мощность множеств. (5 ч).

При изучении вопроса необходимо обратить внимание на следующие особенности.

- Мощность множеств. .

2.2 Наименование вопроса. Кольца и поля. Кольцо классов вычетов целых чисел. (5 ч).

При изучении вопроса необходимо обратить внимание на следующие особенности.

- Кольца и поля.
- Кольцо классов вычетов целых чисел..

2.3 Наименование вопроса. Группоид и полугруппа. Группы. Подстановки на множестве. (1 ч).

При изучении вопроса необходимо обратить внимание на следующие особенности.

- Группоид и полугруппа.
- Группы. Подстановки на множестве.

2.3 Наименование вопроса. Правила комбинаторики. Комбинаторные формулы. (4 ч).

При изучении вопроса необходимо обратить внимание на следующие особенности.

- Правила комбинаторики.
- Комбинаторные формулы

2.4 Наименование вопроса. Метод рекуррентных соотношений. Производящие функции (8 ч).

При изучении вопроса необходимо обратить внимание на следующие особенности.

- Рекурсивный способ задания функций целочисленных аргументов является очень важным в математике и приложениях;
- используется при формализации понятия алгоритма (рекурсивный алгоритм).

2.5 Наименование вопроса. Простые числа. (4 ч).

При изучении вопроса необходимо обратить внимание на следующие особенности.

- Простые числа.

2.6 Наименование вопроса. Уравнения в кольце вычетов. Сравнения первой степени с одним неизвестным. Решение сравнений первой степени. Порядок числа и класса вычетов по модулю. Первообразные корни. Индексы по простому модулю и их приложения. Математические основы криптографии: приложения модульной арифметики в алгоритме RSA. (8 ч).

При изучении вопроса необходимо обратить внимание на следующие особенности.

- Первообразные корни. Индексы по простому модулю и их приложения.
- Математические основы криптографии: приложения модульной арифметики в алгоритме RSA.

2.7 Наименование вопроса. Орграфы и сети. Прикладные задачи и алгоритмы анализа графов и сетей, задачи оптимизации на графах и сетях. ИТ - технологии анализа графов и сетей. (5 ч).

При изучении вопроса необходимо обратить внимание на следующие особенности.

- Алгоритмы отыскания кратчайшего пути в графе имеют важное прикладное значение для разработки маршрутизаторов;
- алгоритмы отыскания максимального потока решают одну из важных задач оптимизации на графах и сетях;
-алгоритмы отыскания остова минимального веса используются для решения важных прикладных оптимизационных задач на графах и сетях;
- сетевое планирование является одной из важных задач оптимизации на сетях.

2.8 Наименование вопроса. Нечёткие отношения и соответствия. Экспертные системы. (5 ч).

При изучении вопроса необходимо обратить внимание на следующие особенности.

- Нечёткие отношения и соответствия.

Экспертные системы.;

3. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПОДГОТОВКЕ К ЗАНЯТИЯМ

3.1 Вид и наименование темы занятия

Практические занятия № ПЗ-1- ПЗ-8 Раздела 1: Бинарные отношения.

Практическое занятие 1. (2 ч). Множества и операции над ними.

Практическое занятие 2. (2 ч). Алгебра Буля.

Практическое занятие 3. (2 ч). Бинарные отношения и их свойства, способы задания отношений (в инт. форме).

Практическое занятие 4. (2 ч). Отношения эквивалентности.

Практическое занятие 5. (2 ч). Отношения частичного порядка. Отношения Парето. Принятие решений при многих критериях.

Практическое занятие 6. (2 ч). Функции. Виды функций.

Практическое занятие 7. (2 ч). Эквивалентные множества. Понятие мощности множеств, сравнение мощностей.

Практическое занятие 8. (2 ч). Счётные множества. Множества мощности континуум

При подготовки к занятию необходимо обратить внимание на следующие моменты.

1. Множества и операции над ними.
2. Мощность конечных множеств.
3. Эквивалентные множества.
4. Счётные множества.
5. Множества мощности континуум.
6. Бинарные отношения.
7. Свойства бинарных отношений.
8. Виды бинарных отношений.
9. Отношения эквивалентности.
10. Отношения порядка.

3.2 Вид и наименование темы занятия

Практические занятия №ПЗ-9-ПЗ-13 Раздела 2 «Основные алгебраические структуры», раздела 4 «Элементы теории чисел».

Практическое занятие 9. (2 ч). Бинарные операции. Группы. Подстановки на множестве.

Практическое занятие 10. (2 ч). Кольца и поля. Кольцо классов вычетов целых чисел Z_n.

Практическое занятие 15. (2 ч). Простые числа.

Практическое занятие 16-17. (4 ч). Уравнения в кольце вычетов. Сравнения первой степени с одним неизвестным. Решение сравнений первой степени.

Практическое занятие 18-19. (4 ч). Порядок числа и класса вычетов по модулю. Первообразные корни. Индексы по простому модулю и их приложения.

Практическое занятие 20-21. (4 ч). Математические основы криптографии: приложения модульной арифметики в алгоритме RSA.

Практическое занятие 11. (2 ч). Уравнения в кольце вычетов. Сравнения первой степени с одним неизвестным Решение сравнений первой степени.

При подготовке к занятию необходимо обратить внимание на следующие моменты.

1. Понятие алгебраической структуры.
2. Понятие группоида, основные свойства и примеры.
3. Понятие полугруппы, основные свойства и примеры.
4. Понятие группы, основные свойства и примеры.
5. Аддитивные и мультипликативные группы.
6. Абелевы группы.
7. Подгруппы, примеры.
8. Фактор группы.
9. Циклические группы.
10. Подстановки на множестве.
11. Кольца, кольца целостности. Поля.
12. Понятие о классах вычетов целых чисел по модулю. Бинарные операции сложения и умножения классов, таблицы сложения и умножения, замкнутость операций.
13. Кольцо Z_n классов вычетов целых чисел и его алгебраические свойства, мощность кольца.
14. Системы вычетов.
15. Обратимые элементы и делители нуля кольца Z_n, мультипликативная группа обратимых элементов кольца.
16. Необходимое и достаточное условие при котором Z_n становится полем, признаки обратимых классов и делителей нуля.
17. Отношение делимости и его свойства. Деление с остатком. НОД и алгоритм Евклида, взаимно простые числа, НОК.
18. Простые и составные числа, основная теорема арифметики. Разложение составных чисел на простые множители. Теоремы о свойствах простых чисел. Решето Эратосфена.
19. Вопрос о характере распределения простых чисел в натуральном ряду.
20. Тесты на простоту.
21. Понятие о числовых функциях, примеры: число $\tau(n)$ всех натуральных делителей n, сумма $\sigma(n)$ всех натуральных делителей n, функция Эйлера $\phi(n)$, $[x]$.Мультипликативные числовые функции.
22. Функция $[x]$, её свойства и применения в теории чисел.
23. Функция Эйлера $\phi(n)$.
24. Понятие сравнения целых чисел по модулю, различные признаки сравнимых чисел, примеры. Основные свойства сравнений. Простейшие приложения сравнений в теории делимости.
25. Вычеты целых чисел по модулю и их алгебраические свойства.
26. Приложения модульной арифметики в криптографии. Понятие о системе шифрования RSA, история вопроса.
27. Модульная арифметика как математическая основа системы RSA. Шифровка и дешифровка. Надёжность, выбор простых.
28. Проблема цифровой подписи.

3.3 Вид и наименование темы занятия

Практические занятия №ПЗ-11-ПЗ-14 Раздела 3: Основы комбинаторики.

Практическое занятие 11. (2 ч). Правила комбинаторики. Комбинаторные формулы.

Практическое занятие 12. (2 ч). Бином Ньютона. Биномиальные коэффициенты и их свойства.

Практическое занятие 13-14. (4 ч). Метод включений и исключений. Метод рекуррентных соотношений. Производящие функции.

При подготовки к занятию необходимо обратить внимание на следующие моменты.

1. Бином Ньютона
2. Биномиальные коэффициенты и их свойства.
3. Метод включений и исключений
4. Метод рекуррентных соотношений.
5. Линейные однородные рекурсии.
6. Примеры знаменитых рекурсий.
7. Правила комбинаторики
8. Сочетания.
9. Размещения.
10. Перестановки.

3.4 Вид и наименование темы занятия

Практические занятия №ПЗ-18-ПЗ-21 Раздела 4: Нечёткие множества и отношения.

Практическое занятие ПЗ 33-34 (4 ч). Нечёткие множества и операции над ними.

Практическое занятие ПЗ 35-36(4 ч). Нечёткие отношения и соответствия. Экспертные системы.

При подготовки к занятию необходимо обратить внимание на следующие моменты.

1. Нечёткие множества
2. Операции над нечёткими множествами
3. Нечёткие отношения и соответствия.
4. Экспертные системы.

3.5 Вид и наименование темы занятия

Практическое занятие №ПЗ-22-36 Раздела 5: Основы теории графов.

Практическое занятие 22-23. (4 ч). Определение графов, основные понятия теории графов. Виды графов. Способы задания графов. Матрицы смежности и инцидентности графа. Матрица Кирхгофа. Числовые характеристики графов.

Практическое занятие 24. (2 ч). Свойства графов: маршруты, циклы, связность. Свойства регулярных, двудольных и связных графов. Метрические характеристики связных графов.

Практическое занятие 25-26. (4 ч). Деревья. Свойства деревьев.

Практическое занятие 27-28. (4 ч). Свойства эйлеровых и гамильтоновых графов.

Практическое занятие 29-30. (4 ч). Планарность и укладка графов. Раскраска графов. Хроматическое число

Практическое занятие 31-32 (4 ч). Орграфы и сети. Прикладные задачи и алгоритмы анализа графов и сетей, задачи оптимизации на графах и сетях. ИТ - технологии анализа графов и сетей. .

При подготовки к занятию необходимо обратить внимание на следующие моменты.

1. Основные понятия теории графов.
2. Операции над графами.
3. Способы задания графов.
4. Задание графов матрицами, матрицы весов
5. Компоненты связности.
6. Пути и циклы в ориентированных графах
7. Орграфы.
8. Упорядочение вершин и дуг орграфа.
9. Выявление путей с заданным количеством рёбер.
10. Определение экстремальных путей на графах
11. Сети и алгоритмы поиска кратчайшего пути, понятие об алгоритме Дейкстры
12. Маршрутизаторы.
13. Эйлеровы графы.
14. Гамильтоновы графы.
15. Понятие потока в сети.
16. Алгоритм отыскания максимального потока через минимальный разрез.
17. Деревья.
18. Бинарные деревья поиска.
19. Обход бинарных деревьев Обход бинарных деревьев.
20. Остовные деревья.
21. Минимальные остовные деревья.
22. Понятие изоморфизма графов.
23. Критерий изоморфизма в терминах матриц смежности.
24. Прикладные задачи и алгоритмы анализа графов.