Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Курганский государственный университет»
(КГУ)

Кафедра «Безопасность информационных и автоматизированных систем»

УТВЕРЖДАЮ:
Первый проректор
_____ Т.Р. Змызгова
«31» августа 2023 г.

Рабочая программа учебной дисциплины

ДИСКРЕТНАЯ МАТЕМАТИКА

образовательной программы высшего образования –
программы специалитета
10.05.03 Информационная безопасность автоматизированных систем
Специализация № 5: Безопасность открытых информационных систем

Форма обучения: очная

Курган 2023

Рабочая программа дисциплины «Дискретная математика» составлена в соответствии с учебным планом по программе специалитета «Информационная безопасность автоматизированных систем» (Безопасность открытых информационных систем), утвержденным для очной формы обучения «30» 06 2023 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» «31» августа 2023, протокол № 1.

Рабочую программу составил:
канд. тех. наук, доцент В.А. Стукало

Согласовано:

Заведующий кафедрой «БИАС»
канд. тех. наук, доцент Д.И. Дик

Специалист по учебно-методической
работе Учебно-методического отдела Г.В. Казанкова

Начальник Управления
образовательной деятельности И.В. Григоренко

1. ОБЪЕМ ДИСЦИПЛИНЫ

Всего: 10 зачетных единиц трудоемкости (360 академических часа)

Очная форма обучения

Вид учебной работы	На всю дисциплину	Семестр	
		2	3
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**168**	**84**	**84**
Лекции	68	34	34
Лабораторные работы	32	16	16
Практические занятия	68	34	34
Самостоятельная работа, всего часов в том числе:	192	96	96
Подготовка к зачету	18	18	-
Подготовка к экзамену	27	-	27
Другие виды самостоятельной работы (подготовка к практическим, лабораторным занятиям и рубежному контролю)	127	58	69
Контрольная работа	20	20	-
Вид промежуточной аттестации	**зачет, экзамен**	**зачет**	**экзамен**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**360**	**180**	**180**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Дискретная математика» относится к базовым дисциплинам Блока 1. Одним из наиболее эффективных результатов взаимодействия математики и техники явилось создание современных электронных вычислительных машин. Для разработки новых средств вычислительной техники, математического и программного обеспечения, для защиты хранимой и передаваемой информации, а также для их использования при построении различных автоматизированных систем, машинных комплексов и компьютерных сетей необходимо знание дискретной математики, основным предметом исследования которой являются совокупности объектов самого общего вида и различные отношения между ними.

Для многих систем дискретность является основным свойством функционирования, в то же время дискретные модели позволяют существенно упростить анализ и синтез систем за счет исключения из рассмотрения переходных процессов.

Изучение дисциплины «Дискретная математика» не требует предварительного изучения каких-либо других дисциплин. В то же время данная дисциплина является основой многих других дисциплин технического, экономического и даже гуманитарного циклов и практически всех дисциплин математического цикла. Некоторые разделы, изучаемые в курсе дискретной математики, такие как метод математической индукции и, отчасти, теория множеств изучаются в рамках таких дисциплин как математический анализ и линейная алгебра. Модели, методы и алгоритмы, рассматриваемые в рамках курса «Дискретная математика», используются при изложении материала следующих дисциплин: «Безопасность сетей ЭВМ», «Базы данных», «Безопасность систем баз данных», «Криптографические методы защиты информации». Знания и навыки, полученные при изучении дисциплины «Дискретная математика», широко используются обучаемыми при изучении общепрофессиональных и специальных дисциплин, таких как «Основы информационной безопасности», «Безопасность операционных систем», «Программно-аппаратные средства защиты информации», «Техническая защита информации», а также при выполнении курсовах работ и написании выпускной квалификационной работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Целью освоения дисциплины «Дискретная математика» является ознакомление студентов с важнейшими разделами дискретной математики и ее применением для решения практических задач, которые являются основой многих других дисциплин математического, технического и экономического циклов. Изучая математическую логику и теорию множеств, студенты, по сути, знакомятся с современным математическим языком, являющимся, как известно, языком любой науки.

Задачами освоения дисциплины «Дискретная математика» являются:

- ознакомление слушателей с основами комбинаторики, математической логики, теории алгоритмов, теории автоматов, теории графов и их приложения к задачам математической кибернетики;

- приобретение навыков свободного обращения с основными дискретными объектами.

Компетенции, формируемые в результате освоения дисциплины:

- способностью к самоорганизации и самообразованию (ОК-8);

- способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач (ОПК-1);

- способностью корректно применять при решении профессиональных задач соответствующий математический аппарат алгебры, геометрии, дискретной математики, математического анализа, теории вероятностей, математической статистики, математической логики, теории алгоритмов, теории информации, в том числе с использованием вычислительной техники (ОПК-2);

- способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах (ПСК-7.1).

В результате изучения дисциплины обучающийся должен:

знать:

- основные методы и алгоритмы теории отношений, связанные с моделированием и оптимизацией систем различной природы (для ОК-8, ОПК-1, ОПК-2);

- математический аппарат, в том числе с использованием вычислительной техники, для решения профессиональных задач (для ОПК-1, ОПК-2);

- модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах (для ПСК-7.1);

уметь:

- выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и применять соответствующий физико-математический аппарат для их формализации, анализа и выработки решения (для ОПК-1, ОПК-2);

- разрабатывать и исследовать модели информационно-технологических ресурсов в распределенных информационных системах (для ОК-8, ПСК-7.1);

владеть:

- современными методами исследования с использованием компьютерных технологий (для ОК-8);

- способностью выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности, и применять соответствующий физико-математический аппарат для их формализации, анализа и выработки решения (для ОПК-1, ОПК-2);

- криптографическими протоколами для передачи и хранения данных в распределенных информационных системах (для ПСК-7.1).

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-тематический план. Очная форма обучения

Рубеж	Номер темы	Наименование раздела, темы	Количество часов контактной работы с преподавателем		
			Лекции	Практич. занятия	Лаборатор. работы
семестр 2					
Рубеж 1	Тема 1	Введение в теорию множеств	4	2	4
	Тема 2	Комбинаторика	8	8	4
Рубеж 2	Тема 3	Алгебра логики	12	10	4
Рубеж 3	Тема 4	Теория графов	4	8	2
	Тема 5	Теория формальных языков и автоматов	6	6	2
		Всего за семестр:	**34**	**34**	**16**
семестр 3					
Рубеж 1	Тема 6	Арифметические операции в цифровых машинах	6	2	2
	Тема 7	Основы теории управляющих систем	8	10	4
Рубеж 2	Тема 8	Теория кодирования	12	14	6
Рубеж 3	Тема 9	Элементы теории чисел	8	8	4
		Всего за семестр:	**34**	**34**	**16**

4.2. Содержание лекционных занятий

ТЕМА 1. ***Введение в теорию множеств.***

Понятие множества, способы их задания. Подмножества, Операции над множествами. Алгебра множеств. Диаграммы Венна.

Отношения. Бинарные отношения, способы их задания. Свойства отношений. Разбиение и отношение эквивалентности. Отношение порядка. Соответствия, функции, отображения.

ТЕМА 2. Комбинаторика.

Комбинаторные конфигурации. Правила суммы и произведения. Сочетания, перестановки, размещения (с повторением и без повторения элементов). Бином Ньютона, треугольник Паскаля. Свойства биномиальных коэффициентов. Полиномиальная теорема. Упорядоченное и неупорядоченное разбиение множеств на непересекающиеся классы элементов.

Рекуррентные соотношения. Линейные рекуррентные уравнения с постоянными коэффициентами. Рекуррентные соотношения в комбинаторике.

ТЕМА 3. Алгебра логики.

Функции алгебры логики (переключательные функции) Способы их задания. Функции алгебры логики (ФАЛ) от n аргументов. СДНФ и СКНФ. Минимизация ФАЛ. Полиномы Жегалкина. Замкнутые классы функций. Теорема о функциональной полноте, примеры функционально-полных базисов. Переключательные схемы.

ТЕМА 4. Теория графов.

Основные понятия теории графов. Виды графов. Способы их задания. Гомоморфизм и изоморфизм графов. Раскраска графов. Планарные графы. Деревья.

Оптимизационные задачи на графах. Алгоритмы поиска кратчайших путей в графах. Анализ графа цепи Маркова. Эйлеровы и гамильтоновы графы. Задача поиска гамильтонова цикла в графе. Задача о коммивояжере.

ТЕМА 5. Теория формальных языков и автоматов.

Понятие конечного автомата. Виды автоматов и их эквивалентность. Преобразование автомата Мили в автомат Мура.

Автоматные языки. Понятие формальной грамматики. Применение грамматик для построения языков высокого уровня.

ТЕМА 6. Арифметические операции в цифровых машинах.

Системы счисления. Позиционные системы с естественными весами разрядов. Инверсные коды: обратный и дополнительный код.

Разрешимые и неразрешимые проблемы. Схемы алгоритмов, схемы потоков данных. Коды с обнаружением и исправлением ошибок

ТЕМА 7. Основы теории управляющих систем.

Схемы из функциональных элементов. Реализация функций алгебры логики схемами. Сумматор. Верхняя оценка сложности сумматора. Вычитатель.

Дешифратор. Асимптотика сложности дешифратора. Верхняя оценка сложности реализации произвольной функции алгебры логики.

Мультиплексор. Верхняя оценка сложности мультиплексора. Метод Шеннона.

Шифратор. Верхняя оценка сложности шифратора.

ТЕМА 8. Теория кодирования.

Алфавитное кодирование. Теорема Маркова о взаимной однозначности алфавитного кодирования. Неравенство Макмиллана. Существование префиксного кода с заданными длинами кодовых слов. Оптимальные коды, их свойства.

Теорема редукции.

Коды с исправлением r ошибок. Оценка функции Mr (n). Коды Хэмминга. Оценка функции Mr (n).

ТЕМА 9. Элементы теории чисел.

Целые числа. Делимость целых чисел. Свойства делимости. Алгоритм Евклида. Свойства наибольшего общего делителя.

Простые числа. Свойства простых чисел. Основная теорема арифметики. Функция Эйлера.

Теория вычетов. Свойства вычетов. Полная и приведенная системы вычетов. Малая теорема Ферма. Теорема Эйлера. Арифметика остатков.

Сравнения первой степени. Решение диафантовых уравнений. Нахождение обратных по модулю значений.

4.3. Практические занятия

Номер раздела	Наименование темы	Наименование тем практических занятий	Норматив времени, час.
		2 семестр	
1	Введение в теорию множеств	Множества. Отношения.	2
2	Комбинаторика	Соединения. Рекуррентные соотношения.	6
	1-ый рубежный контроль	***Тестирование***	***2***
3	Алгебра логики	Переключательные функции (ПФ). Минимизация ПФ.	2
		Переключательные функции (ПФ). Минимизация ПФ.	2
		Функционально полные наборы ПФ.	4
	2-ой рубежный контроль	***Тестирование***	***2***
4	Теория графов	Графы и орграфы.	4
		Оптимизационные задачи на графах.	4
5	Теория формальных языков и автоматов	Конечные автоматы. Автоматные языки.	4
	3-ий рубежный контроль	***Тестирование***	***2***
		Всего за семестр	**34**
		3 семестр	
6	Арифметические операции в цифровых машинах	Арифметические операции в цифровых машинах	2
7	Основы теории управляющих систем	Схемы из функциональных элементов. Реализация функций алгебры логики схемами. Сумматор. Верхняя оценка сложности сумматора. Вычитатель.	2
		Дешифратор. Асимптотика сложности дешифратора. Верхняя оценка сложности реализации произвольной функции алгебры логики.	2
		Мультиплексор. Верхняя оценка сложности мультиплексора. Метод Шеннона.	2
		Шифратор. Верхняя оценка сложности шифратора.	2
	4-ый рубежный контроль	***Тестирование***	***2***
8	Теория кодирования	Алфавитное кодирование. Теорема Маркова о взаимной однозначности алфавитного кодирования.	2
		Неравенство Макмиллана.	2
		Существование префиксного кода с заданными длинами кодовых слов.	2
		Оптимальные коды, их свойства. Теорема редукции.	2
		Коды с исправлением r ошибок. Оценка функции $Mr(n)$.	2
		Коды Хэмминга. Оценка функции $Mr(n)$.	2
	5-ой рубежный контроль	***Тестирование***	***2***
9	Элементы теории чисел	Целые числа. Делимость целых чисел. Свойства делимости. Алгоритм Евклида.	6

		Свойства наибольшего общего делителя.	
	6-ий рубежныйконтроль	***Тестирование***	***2***
		Всего за семестр	***34***
		ИТОГО	***68***

4.4. Лабораторные работы

Номер темы	Наименование темы	Наименование тем лабораторных работ	Норматив времени, час.
		2 семестр	
1	Введение в теорию множеств	*Лабораторная работа №1.* Введение в теорию множеств.	2
		Лабораторная работа №2. Отношения. Соответствия. Функции. Преобразования.	2
2	Комбинаторика	*Лабораторная работа №3.* Классическая комбинаторика. Основные соединения. Соединения с повторениями.	2
		Лабораторная работа №4. Комбинаторные задачи с ограничениями. Линейные рекуррентные уравнения.	2
3	Алгебра логики	*Лабораторная работа №5.* Минимизация булевых функций. Таблицы истинности. Элементарные преобразования. Диаграммы Вейча.	2
		Лабораторная работа №6. Минимизация частично определенных функций. Функционально полные наборы и базисные наборы. Полиномы Жегалкина. Переключательные схемы.	2
4	Теория графов	*Лабораторная работа №7.* Теория графов.	2
5	Теория формальных языков и автоматов	*Лабораторная работа №8.* Теория формальных языков и автоматов	2
		Всего за семестр	***16***
		3 семестр	
6	Арифметические операции в цифровых машинах	*Лабораторная работа №9.* Арифметические операции в цифровых машинах	2
7.	Основы теории управляющих систем	*Лабораторная работа №10.* Дешифратор. Асимптотика сложности дешифратора. Верхняя оценка сложности реализации произвольной функции алгебры логики.	2
		Лабораторная работа №11. Мультиплексор. Верхняя оценка сложности мультиплексора. Метод Шеннона.	2
8.	Теория кодирования	*Лабораторная работа №12.* Алфавитное кодирование. Теорема Маркова о взаимной однозначности алфавитного кодирования.	2
		Лабораторная работа №13. Коды с исправлением r ошибок. Оценка функции $Mr(n)$.	2

		Лабораторная работа №14. Моделирование автоматной функции схемой из функциональных элементов и элементов задержки.	2
9.	Элементы теории чисел	*Лабораторная работа №15.* Целые числа. Делимость целых чисел. Свойства делимости.	2
		Лабораторная работа №16. Теория вычетов. Свойства вычетов.	2
		Всего за семестр	***16***
		Итого	**32**

4.5. Контрольная работа

Дисциплина «Дискретная математика» является составной частью фундаментальной инженерной и специальной математической подготовки. Изучение дисциплины способствует овладению математическими основами профилирующих дисциплин и методами построения и реализации эффективных алгоритмов.

Самостоятельное решение контрольных заданий способствует более углубленному изучению математических основ дисциплины. Обучающийся должен выполнить контрольную работу по варианту, совпадающему с последней цифрой номера его зачётной книжки. Варианты заданий разработаны в соответствии с федеральным государственным образовательным стандартом высшего образования по специальности 10.05.03 «Информационная безопасность автоматизированных систем» и размещены в методическом пособии «Дискретная математика. Задания к выполнению контрольной работы». Контрольные задания содержат четыре основные темы: «Теория множеств», «Комбинаторика», «Элементы теории графов», «Булева алгебра».

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

При прослушивании лекций рекомендуется в конспекте отмечать все важные моменты, на которых заостряет внимание преподаватель, в частности те, которые направлены на качественное выполнение соответствующей лабораторной или практической работе.

Преподавателем запланировано использование при чтении лекций технологии учебной дискуссии. Поэтому рекомендуется фиксировать для себя интересные моменты с целью их активного обсуждения на дискуссии в конце лекции.

Залогом качественного выполнения практических работ и лабораторных работ является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Рекомендуется подготовить вопросы по неясным моментам и обсудить их с преподавателем перед началом работы.

Преподавателем запланировано применение на практических занятиях и лабораторных работах технологий развивающейся кооперации, коллективного взаимодействия, разбора конкретных ситуаций.