Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Безопасность компьютерных систем

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Оценочные материалы
по дисциплине
Дискретная математика-2

Москва
2022

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Евтеев Б.В. Идентификатор: Rbb7ca24a-YevteevBV-e22a6fbb	Б.В. Евтеев
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

ОБЩАЯ ЧАСТЬ

Оценочные материалы по дисциплине предназначены для оценки: достижения обучающимися запланированных результатов обучения по дисциплине, этапа формирования запланированных компетенций и уровня освоения дисциплины.

Оценочные материалы по дисциплине включают оценочные средства для проведения мероприятий текущего контроля успеваемости и промежуточной аттестации.

Формируемые у обучающегося компетенции:

1. ОПК-2 способностью применять соответствующий математический аппарат для решения профессиональных задач

и включает:

для текущего контроля успеваемости:

Форма реализации: Письменная работа

1. Контрольная работа №1 «Булевы функции и их криптографические свойства» (Контрольная работа)
2. Контрольная работа №2 «Комбинаторные методы» (Контрольная работа)
3. Контрольная работа №3 «Графы» ()
4. Контрольная работа №4 «Алгебраические структуры и основы модулярной арифметики» (Контрольная работа)

БРС дисциплины

5 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Булевы функции и их криптографические свойства					
Булевы функции		+			
Криптографические свойства булевых функций		+			
Комбинаторные методы					
Общая комбинаторная схема			+		
Рекуррентные соотношения и производящие функции			+		
Классификация булевых функций			+		
Графы					
Элементы теории графов				+	

Графы преобразований и их свойства			+	
Алгебраические структуры и основы модулярной арифметики				
Алгебраические основы				+
Теоретико-числовые основы				+
Вес КМ:	25	25	25	25

$Общая часть/Для промежуточной аттестации$

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ

I. Оценочные средства для оценки запланированных результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Индекс компетенции	Индикатор	Запланированные результаты обучения по дисциплине	Контрольная точка
ОПК-2	ОПК-2(Компетенция)	Знать: теорию булевых функций и алгебраических структур комбинаторные методы, теорию графов Уметь: анализировать свойства булевых функций и использовать булевы функции с требуемыми свойствами применять методы дискретной математики при решении прикладных задач	Контрольная работа №1 «Булевы функции и их криптографические свойства» (Контрольная работа) Контрольная работа №2 «Комбинаторные методы» (Контрольная работа) Контрольная работа №3 «Графы» Контрольная работа №4 «Алгебраические структуры и основы модулярной арифметики» (Контрольная работа)

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Контрольная работа №1 «Булевы функции и их криптографические свойства»

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Контрольная работа проводиться в письменной форме. В шапке контрольной работы указывается: наименование предмета; номер группы, Ф.И.О. студента. Для выполнения контрольной работы предусматривается несколько вопросов. Время выполнения 2 академических часа. После проверки контрольной работы оглашаются результаты.

Краткое содержание задания:
Ответить на вопросы контрольной работы

Контрольные вопросы/задания:

Уметь: анализировать свойства булевых функций и использовать булевы функции с требуемыми свойствами	1.Быстрым преобразованием Уолша найти нелинейность булевой функции f (x1, x2, x3, x4) = (1,1,0,0,1,1,1,0,1,0,0,0,1,0,1,1) 2.Доказать, что если у функции есть к фиктивных переменных, то её вес делится на 2^к

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-2. Контрольная работа №2 «Комбинаторные методы»

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Контрольная работа проводиться в письменной форме. В шапке контрольной работы указывается: наименование предмета; номер группы, Ф.И.О. студента. Для выполнения контрольной работы предусматривается несколько вопросов. Время выполнения 2 академических часа. После проверки контрольной работы оглашаются результаты.

Краткое содержание задания:
Ответить на вопросы контрольной работы

Контрольные вопросы/задания:

Уметь: применять методы дискретной математики при решении прикладных задач	1.Найти число целых положительных чисел не превосходящих 1000 и не делящихся ни на одно из чисел 3, 5, 7 2.Найти количество неизоморфных абелевых групп порядка 27648. Описать строение циклической группы этого порядка

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-3. Контрольная работа №3 «Графы»

Формы реализации: Письменная работа
Тип контрольного мероприятия:
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Контрольная работа проводиться в письменной форме. В шапке контрольной работы указывается: наименование предмета; номер группы, Ф.И.О. студента. Для выполнения контрольной работы предусматривается несколько вопросов. Время выполнения 2 академических часа. После проверки контрольной работы оглашаются результаты.

Краткое содержание задания:
Ответить на вопросы контрольной работы

Контрольные вопросы/задания:

Знать: комбинаторные методы, теорию графов	1.Дан граф с пятью вершинами занумерованными числами от 1 до 5 и указанными расстояниями между вершинами: dist(1,2)=2 dist(1,4)=3, dist(2,3)=4, dist(3,4)=6, dist(5,2)=1, dist(3,5)=2 dist(4,5)=3. Найти кратчайшие расстояния между вершинами с помощью алгоритма Флойда- Уоршолла 2.Доказать, что полный граф K_5^5 не является планарным 3.Доказать, что если граф содержит цикл от вершины к ней самой, то он содержит простой цикл от вершины к ней самой

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-4. Контрольная работа №4 «Алгебраические структуры и основы модулярной арифметики»

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Контрольная работа проводится в письменной форме. В шапке контрольной работы указывается: наименование предмета; номер группы, Ф.И.О. студента. Для выполнения контрольной работы предусматривается несколько вопросов. Время выполнения 2 академических часа. После проверки контрольной работы оглашаются результаты.

Краткое содержание задания:
Ответить на вопросы контрольной работы

Контрольные вопросы/задания:

Знать: теорию булевых функций и алгебраических структур	1.Доказать, что все классы вычетов Zn*, элементы которых взаимно просты с n, образуют группу относительно операции умножения. Является ли эта группа циклической при n =11*373? Ответ обосновать. 2.Решить задачу линеаризации наибольшего общего делителя чисел 2428, 788, 120. 3.Решить сравнение 21 X≡ 30 mod (33). В ответе указать классы вычетов по модулю 33.

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3

Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

5 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

<table>
<tr><td>НИУ «МЭИ» ИнЭИ</td><td rowspan="3">ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ

по дисциплине: Дискретная математика-2
направление подготовки: 10.03.01
форма обучения: очная</td><td rowspan="3">Утверждаю:
Зав. кафедрой БИТ

_____
(подпись</td></tr>
<tr><td>Кафедра БИТ</td></tr>
<tr><td></td></tr>
<tr><td colspan="3">1. Нелинейность б.ф. Нахождение нелинейности через спектр Уолша-Адамара, быстрое преобразование Уолша и оценка нелинейности произвольной б.ф.
2. Эйлеровы графы. Сформулировать и доказать эквивалентные определения эйлеровых графов.
3. Найти количество неизоморфных абелевых групп 36-го порядка. Описать строение циклической группы этого же порядка.</td></tr>
</table>

Процедура проведения

Экзамен проводится в письменной форме по билетам согласно программе экзамена

I. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины

1. Компетенция/Индикатор: ОПК-2(Компетенция)

Вопросы, задания

1.Расширенный алгоритм Евклида.
2.Задача линеаризации наибольшего общего делителя n чисел и ее решение.
3.Сравнения и их свойства.
4.Китайская теорема об остатках.
5.Функция Эйлера и её вычисление.
6.Теоремы Эйлера и Ферма (малая).
7.Проблема факторизации целых чисел. Метод выделения множителей Ферма.
8.Проблема дискретного логарифмирования, метод Шэнкса и Полига-Силвера-Хэллмана.
9.Группы и их свойства.
10.Циклические группы, подсчет числа образующих этих групп.
11.Теорема Лагранжа.
12.Теорема Кэли.
13.Теорема о гомоморфизмах групп.
14.Прямая сумма групп (подгрупп).
15.Примарные циклические группы и их свойства.
16.Сформулировать теорему о строении конечных абелевых групп. Найти количество неизоморфных абелевых групп заданного порядка.
17.Алгебраическая нормальная форма б.ф. и быстрое преобразование Мёбиуса для её нахождения.

18.Полнота системы б.ф. и критерий полноты системы б.ф.
19.Преобразование и обратное преобразование Фурье.
20.Преобразование Уолша-Адамара и обратное преобразование Уолша-Адамара.
21.Связь между коэффициентами Фурье и Уолша-Адамара.
22.Соотношение ортогональности для спектра Уолша-Адамара. Равенство Парсеваля.
23.Нелинейность б.ф. Нахождение нелинейности через спектр Уолша-Адамара, быстрое преобразование Уолша и оценка нелинейности произвольной б.ф.
24.Максимально-нелинейные б.ф.
25.Бент-функции и условия их существования.
26.Лемма Бернсайда.
27.Цикловой индекс группы преобразований и его применение к решению комбинаторных задач, примеры. Терема Пойа. Классификация двоичных функций.
28.Множества и действия над ними. Свойства операций над множествами. Отображения множеств.
29.Формула включений и исключений для подсчета числа элементов в объединении множеств.
30.Комбинаторные объекты и комбинаторные числа. Выборки и их виды. Подсчет количества выборок при заданных условиях.
31.Формула бинома Ньютона, свойства биномиальных коэффициентов. Треугольник Паскаля.
32.Принцип включения и исключения и его применение к решению комбинаторных задач.
33.Установление комбинаторных тождеств, свертка Вандермонда.
34.Инъективные распределения шаров по ящикам.
35.Сюръективные распределения шаров по ящикам. Числа Стирлинга второго рода.
36.Производящие функции, их виды и действия над ними.
37.Применение производящих функций для решения рекуррентных соотношений.
38.Применение производящих функция для подсчета вариантов распределения шаров по ящикам.
39.Рекуррентные соотношения, соответствующие им рекуррентные уравнения и их решение. Понятие характеристического многочлена. Решение линейных рекуррентных соотношений.
40.Нахождение всех решений линейного однородного рекуррентного уравнения второго порядка. Нахождение чисел Фибоначчи.
41.Отношения на множествах. Свойства отношений. Отношение эквивалентности и классы эквивалентности. Фактор-множества по отношению эквивалентности. Разбиения множеств.
42.Отношения порядка. Цепи и антицепи и их свойства. Длина и ширина конечного частично упорядоченного множества. Теорема Дилуорса.
43.Булевы кубы и их характеристики. Расстояние между его элементами и их нумерация. Код Грэя.
44.Сформулировать и доказать теоремы о длине и ширине булева куба.
45.Графы, мультиграфы, псевдографы, ориентированные графы. Подграфы и надграфы. Изоморфизм графов.
46.Матрицы инцидентности и смежности графов (орграфов). Определения связности двух вершин графа и подсчета количества путей из одной вершины в другую заданной длины, соединяющих эти вершины.
47.Матрицы инцидентности и смежности графов (орграфов). Определения связности двух вершин графа и подсчета количества путей из одной вершины в другую заданной длины, соединяющих эти вершины.
48.Компоненты связности графа. Дерево и остовное дерево.

49.Оценка числа компонент в графе с использованием количества вершин и ребер графа и точный их подсчет в графах без циклов.
50.Раскраска графов, эвристические и оптимальные алгоритмы.
51.Сформулировать и доказать эквивалентные определения дерева.
52.Эйлеровы графы. Сформулировать и доказать эквивалентные определения эйлеровых графов.
53.Эйлеровы пути и собственные эйлеровы пути. Необходимое и достаточное условие существования в графе собственного эйлерова пути.
54.Подразделение графа. Гомеоморфизм графов. Сформулировать и решить задачу о кенигсбергских мостах.
55.Геометрическая реализация графов в трехмерном пространстве и на плоскости. Сформулировать и доказать теорему о геометрической реализации графа в трехмерном пространстве.
56.Полные, двудольные и полные двудольные графы. Сформулировать и доказать необходимое и достаточное условие двудольности графа.
57.Планарные графы. Доказать формулу Эйлера, связывающую число вершин, ребер и граней планарного графа.
58.Сформулировать теорему Понтрягина-Куратовского и доказать условие необходимости этой теоремы.
59.Оптимизация на графах. Алгоритмы Дейкстры и Флойда-Уоршолла поиска кратчайшего пути в графе.
60.Графы преобразований и их свойства. Числа Стирлинга первого рода.

Материалы для проверки остаточных знаний

1.Комбинаторные объекты и комбинаторные числа

Ответы:

-

Верный ответ: Комбинаторный объект – это подмножество с определенными свойствами из элементов множества А. Комбинаторное число (связанное с комбинаторным объектом) – это количество комбинаторных объектов этого вида.

2.Найти количество неизоморфных графов с четырьмя вершинами

Ответы:

-

Верный ответ: 11

3.Матрица инцидентности графов

Ответы:

-

Верный ответ: Матрица инцидентности — одна из форм представления графа, в которой указываются связи между инцидентными элементами графа (ребро(дуга) и вершина).

4.Предприятие может предоставить работу по одной специальности 4 женщинами, по другой - 6 мужчинам, по третьей - 3 работникам независимо от пола. Сколькими способами можно заполнить вакантные места, если имеются 14 претендентов: 6 женщин и 8 мужчин?

Ответы:

-

Верный ответ: 1680 способов

5.На одной из кафедр университета работают 13 человек, причем каждый из них знает хотя бы один иностранный язык. Десять человек знают английский, семеро - немецкий, шестеро - французский, пятеро знают английский и немецкий, четверо - английский и французский, трое - немецкий и французский. Выяснить: 1) сколько человек знают все

три языка; 2) сколько человек знают ровно два языка; 3) сколько человек знают только английский язык.

Ответы:

-

Верный ответ: 1) 2 человека 2) 6 человек 3) 3 человека

6.Найти полином Жегалкина для F = (1,0,0,1,1,0,1,1)

Ответы:

-

Верный ответ: Вектор коэффициентов g = (1,1,1,0,0,0,1,1,)

7.Найти нелинейность булевой функции F= (0,1,0,1,0,0,1,1,)

Ответы:

-

Верный ответ: 2

8.Сколькими способами можно раскрасить грани правильного тетраэдра в три разных цвета

Ответы:

-

Верный ответ: 15

9.С помощью расширенного алгоритма Евклида решить задачу линеаризации для чисел 72 и 100

Ответы:

-

Верный ответ: Коэффициенты равны 7 и -5 соответственно.

10. Найти LOG527 в кольце классов вычетов по модулю 43 методом Шэнкса .

Ответы:

-

Верный ответ: 27

II. Описание шкалы оценивания

Оценка: 5

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Работа выполнена в рамках "продвинутого" уровня. Ответы даны верно, четко сформулированные особенности практических решений

Оценка: 4

Нижний порог выполнения задания в процентах: 60

Описание характеристики выполнения знания: Работа выполнена в рамках "базового" уровня. Большинство ответов даны верно. В части материала есть незначительные недостатки

Оценка: 3

Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Работа выполнена в рамках "порогового" уровня. Основная часть задания выполнена верно. на вопросы углубленного уровня

III. Правила выставления итоговой оценки по курсу

Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и экзаменационной составляющих.