

**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 (продвинутый уровень)

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

**Оценочные материалы
по дисциплине
Дискретная математика**

**Москва
2022**

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель

(должность)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Евтеев Б.В.
	Идентификатор	Rbb7ca24a-YevteevBV-e22a6fbb

(подпись)

Б.В. Евтеев

(расшифровка
подписи)

СОГЛАСОВАНО:

Руководитель
образовательной
программы

(должность, ученая степень, ученое
звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Баронов О.Р.
	Идентификатор	R90d76356-BaronovOR-7bf8fd7e

(подпись)

О.Р. Баронов

(расшифровка
подписи)

Заведующий
выпускающей кафедры

(должность, ученая степень, ученое
звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Невский А.Ю.
	Идентификатор	R4bc65573-NevskyAY-0b6e493d

(подпись)

А.Ю.

Невский

(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-3 способен использовать необходимые математические методы для решения задач профессиональной деятельности

ИД-2 Применяет соответствующий математический аппарат для решения профессиональных задач

и включает:

для текущего контроля успеваемости:

Форма реализации: Письменная работа

1. Контрольная работа №1 «Алгебраические структуры и основы модулярной арифметики» (Контрольная работа)

2. Контрольная работа №2 «Булевы функции и их криптографические свойства» (Контрольная работа)

3. Контрольная работа №3 «Комбинаторные методы» (Контрольная работа)

4. Контрольная работа №4 «Графы» (Контрольная работа)

БРС дисциплины

2 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Алгебраические структуры и основы модулярной арифметики					
Бинарные операции на множестве		+	+	+	+
Булевы функции и их криптографические свойства					
Представления булевых функций, полиномы Жегалкина, быстрое преобразование Мёбиуса		+	+	+	+
Комбинаторные методы					
Элементы комбинаторики, комбинаторные числа, формула включений и исключений		+	+	+	+
Графы					
Способы задания графов и свойства графов		+	+	+	+
	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-3	ИД-2опк-3 Применяет соответствующий математический аппарат для решения профессиональных задач	Знать: способы задания, свойства множеств, отношений, функций и отображений основные положения алгебраических структур и комбинаторики методы осуществления операций над графами и выполнения количественных оценок их характеристик Уметь: использовать методы дискретной математики при решении задач защиты информации и разработке соответствующего программного обеспечения применять символику дискретной математики для выражения количественных и качественных отношений объектов	Контрольная работа №1 «Алгебраические структуры и основы модулярной арифметики» (Контрольная работа) Контрольная работа №2 «Булевы функции и их криптографические свойства» (Контрольная работа) Контрольная работа №3 «Комбинаторные методы» (Контрольная работа) Контрольная работа №4 «Графы» (Контрольная работа)

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Контрольная работа №1 «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: методы осуществления операций над графами и выполнения количественных оценок их характеристик	1. Доказать, что все классы вычетов \mathbb{Z}_n^* , элементы которых взаимно просты с n , образуют группу относительно операции умножения. Является ли эта группа циклической при $n = 11 \cdot 373$? Ответ обосновать.
Знать: основные положения алгебраических структур и комбинаторики	1. Решить задачу линейаризации наибольшего общего делителя чисел 2428, 788, 120.
Знать: способы задания, свойства множеств, отношений, функций и отображений	1. Решить сравнение $21x \equiv 30 \pmod{33}$. В ответе указать классы вычетов по модулю 33.
Уметь: использовать методы дискретной математики при решении задач защиты информации и разработке соответствующего программного обеспечения	Найти LOG_{712} в кольце классов вычетов по модулю 61 методом Полига-Силвера-Хеллмана. 1.
Уметь: применять символику дискретной математики для выражения количественных и качественных отношений объектов	1. Выяснить методом выделения множителей Ферма является ли число 116939 простым или составным?

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 «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 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: методы осуществления операций над графами и выполнения количественных оценок их характеристик	1. Для булевой функции $f(x_1, x_2, x_3) = (1, 1, 1, 0, 0, 0, 1, 1)$ методом Блейка найти сокращенную ДНФ, после чего найти все тупиковые и минимальные ДНФ
Знать: основные положения алгебраических структур и комбинаторики	1. Для булевой функции $f(x_1, x_2, x_3, x_4) = (1, 0, 1, 1, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1)$ графическим методом (карта Карно) найти сложность сокращенной ДНФ
Знать: способы задания, свойства множеств, отношений, функций и отображений	1. Для булевой функции $f(x_1, x_2, x_3, x_4) = (0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1)$ быстрым преобразованием Мёбиуса найти полином Жегалкина
Уметь: использовать методы дискретной математики при решении задач защиты информации и разработке соответствующего программного обеспечения	1. Быстрым преобразованием Уолша найти нелинейность булевой функции $f(x_1, x_2, x_3, x_4) = (1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1)$
Уметь: применять символику дискретной математики для выражения количественных и качественных отношений объектов	1. Доказать, что если у функции есть k фиктивных переменных, то её вес делится на 2^k

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 «Комбинаторные методы»

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: методы осуществления операций над графами и выполнения количественных оценок их характеристик	1.Методом производящих функций решить однородное рекуррентное соотношение: $a_{n+2} - 5a_{n+1} + 4a_n = 0$
Знать: основные положения алгебраических структур и комбинаторики	1.Найти количество классов эквивалентных булевых функций от 3 переменных относительно симметрической группы S_3^3
Знать: способы задания, свойства множеств, отношений, функций и отображений	1.Сколькими способами можно разместить семь различных шаров по четырем неразличимым ящикам
Уметь: использовать методы дискретной математики при решении задач защиты информации и разработке соответствующего программного обеспечения	1.Найти число целых положительных чисел не превосходящих 1000 и не делящихся ни на одно из чисел 3, 5, 7
Уметь: применять символику дискретной математики для выражения количественных и качественных отношений объектов	1.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-4. Контрольная работа №4 «Графы»

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: методы осуществления операций над графами и выполнения количественных оценок их характеристик	1. Дан граф с пятью вершинами занумерованными числами от 1 до 5 и указанными расстояниями между вершинами: $\text{dist}(1,2)=2$, $\text{dist}(1,4)=3$, $\text{dist}(2,3)=4$, $\text{dist}(3,4)=6$, $\text{dist}(5,2)=1$, $\text{dist}(3,5)=2$, $\text{dist}(4,5)=3$. Найти кратчайшие расстояния между вершинами с помощью алгоритма Флойда- Уоршола
Знать: основные положения алгебраических структур и комбинаторики	1. Доказать, что полный граф K_5^5 не является планарным
Знать: способы задания, свойства множеств, отношений, функций и отображений	1. Доказать, что если граф содержит цикл от вершины к ней самой, то он содержит простой цикл от вершины к ней самой
Уметь: использовать методы дискретной математики при решении задач защиты информации и разработке соответствующего программного обеспечения	1. Построить код Грея для $n=6$
Уметь: применять символику дискретной математики для выражения количественных и качественных отношений объектов	1. Найти количество подстановок степени 6, в записи которых не менее двух и не более четырех независимых циклов

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

2 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

НИУ «МЭИ» ИнЭИ	ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1 по дисциплине: <i>Дискретная математика</i> направление подготовки: <i>10.03.01</i> форма обучения: <i>очная</i>	Утверждаю: Зав. кафедрой БИТ
Кафедра <i>БИТ</i>		_____
2021 год		(подпись)
1. Алгебраическая нормальная форма б.ф. и быстрое преобразование Мёбиуса для её нахождения 2. Полные, двудольные и полные двудольные графы. Сформулировать и доказать необходимое и достаточное условие двудольности графа. 3. Методом производящих функций решить рекуррентное соотношение: $a_{n+1}^{n+1} - 5a_n^n + 36n = 0$		

Процедура проведения

Экзамен проводится в письменной форме по билетам согласно программе экзамена

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

1. Компетенция/Индикатор: ИД-2_{ОПК-3} Применяет соответствующий математический аппарат для решения профессиональных задач

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 Парсевала.
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 функций 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. Степени вершины. Связь между суммарной степенью вершин и количеством ребер графа. Маршруты (пути), цепи и простые цепи. Выделение в маршруте простой цепи. Циклы и простые циклы.

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-Уоршола 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 A . 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).

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.