МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Механико-математический факультет

УТВЕРЖДАЮ
Декан механико-математического факультета
_____ А.М. Захаров
"11" сентября 20_24__ г.

Рабочая программа дисциплины

Математические основы информационного обслуживания

Направление подготовки магистратуры
02.04.01 Математика и компьютерные науки

Профиль подготовки магистратуры
Математические основы компьютерных наук

Квалификация (степень) выпускника
Магистр

Форма обучения
очная

Саратов,
2024

Статус	ФИО	Подпись	Дата
Преподаватель-разработчик	Новиков В.Е.		11.09.24
Председатель НМК	Тышкевич С.В.		11.09.24
Заведующий кафедрой	Поплавский В.Б.		11.09.24
Специалист Учебного управления			

1. Цели освоения дисциплины

Основными целями освоения дисциплины «Математические основы информационного обслуживания» являются:

- знакомство студентов с основными этапами жизненного цикла информации и математическими инструментами, обслуживающими его функционирование;
- формирование правильного научного подхода к постановке и решению различных задач, связанных с информационным обслуживанием;
- расширение научного кругозора и обучение студентов свободно оперировать современными терминами прикладной математики.

Дисциплина «Математические основы информационного обслуживания» позволяет студентам видеть место различных разделов современной математики в системе информационного обслуживания, овладеть фундаментальными понятиями и методами современной прикладной математики, без знания которых невозможна дальнейшая профессиональная подготовка и профессиональная деятельность в сфере информационных технологий. При освоении данного курса у студентов сформируются навыки грамотной постановки прикладных задач и решения научных задач с применением инструментов современного информационного обслуживания.

2. Место дисциплины в структуре ООП

Дисциплина «Математические основы информационного обслуживания» (Б1.О.05) относится к дисциплинам обязательной части блока 1 «Дисциплины (модули)» учебного плана ООП магистратуры по направлению 02.04.01 Математика и компьютерные науки, профилю «Математические основы компьютерных наук». На ее изучение отводится 108 часов (36 часов аудиторной работы, 36 часов СР, 36 часов контроль). Согласно учебному плану направления и профиля подготовки данный курс в первом семестре заканчивается экзаменом.

Для изучения дисциплины необходимы знания, умения, сформированные у обучающихся в результате освоения курсов «Алгебра», «Дискретная математика», «Теория вероятностей и математическая статистика». Знания, полученные в результате освоения данной дисциплины, позволят использовать соответствующие методы современной математики при изучении различных разделов компьютерных наук. Этот курс является теоретической основой для прикладных задач по информационному обслуживанию современными математическими методами. Его усвоение свидетельствует об уровне квалификации студента в направлении информационных технологий. Компетенции, знания, умения и готовности, сформированные у обучающихся в результате освоения данной дисциплины, могут быть использованы при изучении любого курса, в котором допустимо приложение информационных технологий.

3. Результаты обучения по дисциплине

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
ОПК-2 Способен создавать и исследовать новые математические модели в естественных науках, совершенствовать и разрабатывать концепции, теории и методы	**1.1_М.ОПК-2.** Создает и исследует новые математические модели в естественных науках.	**Знать:** - методы прикладной математики, применяемые в построении математических моделей в естественных науках. **Уметь**: - формулировать математически и проводить анализ задач прикладной математики. **Владеть**: - методами прикладной математики при решении профессиональных задач.
	2.1_М.ОПК-2. Используя методы математического моделирования, находит эффективные решения научных и прикладных задач.	**Знать**: - методы современной математики в системе информационного обслуживания и их применение в решении научных и прикладных задач. **Уметь**: - применять методы современной математики в системе информационного обслуживания в решении научных и прикладных задач. **Владеть**: - навыками применения методов современной математики в системе информационного обслуживания в решении научных и прикладных задач.
	3.1_М.ОПК-2. Совершенствует и разрабатывает методы математического моделирования, оценивает пригодность модели, ее соответствие практике.	**Знать**: - методы математического моделирования в системе информационного обслуживания. **Уметь**: - совершенствовать и разрабатывать методы математического моделирования в системе информационного обслуживания; - оценивать пригодность математической модели, ее соответствие практике. **Владеть**: - навыками разработки модели методами прикладной математики.
ПК-1 Способен демонстрировать фундаментальные	**1.1_М.ПК-1.** Понимает основные концепции, принципы, теории и факты в области математических и (или) естественных наук,	**Знать:** - основные термины и понятия, связанные с жизненным циклом информации; - математический аппарат при

знания математических и естественных наук, программирования и информационных технологий.	программирования и информационных технологий.	реализации этапов жизненного цикла информации. **Уметь:** - выбирать необходимые математические инструменты для решения прикладных задач по реализации жизненного цикла информации; **Владеть**: - основными методами сжатия информации; помехоустойчивого кодирования; - методом расширенного алгоритма Евклида для нахождения обратных элементов в мультипликативной группе простого конечного поля; - основными методами шифрования; - основными методами аутентификации.
	2.1_М.ПК-1. Формулирует и решает стандартные задачи в собственной научно- исследовательской деятельности.	**Знать**: - основные задачи теории информационного обслуживания. **Уметь**: - формулировать и решать задачи в собственной научно-исследовательской деятельности, использую теорию информационного обслуживания. **Владеть:** - навыками решения задач и проблем из различных областей математики, которые требуют знаний из прикладной математики.
	3.1_М.ПК-1. Проводит научно-исследовательские работы в области математики и компьютерных наук.	**Знать:** - новые научные результаты в области прикладной математики. **Уметь**: - использовать современный математический аппарат прикладной математики в научно-исследовательской деятельности. **Владеть**: - навыками применения прикладной математики в научно-исследовательской деятельности в области математики и компьютерных наук.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)						Формы текущего контроля успеваемости *(по неделям семестра)* Формы промежуточной аттестации *(по семестрам)*
				лекции	Пр.занятия		КСР	СР	Контроль	
					Общая трудоемкость	Из них - практическая подготовка				
1	Раздел 1. Основные этапы жизненного цикла информации	1	1,3 /2	4	2			10		Форма текущего контроля - опрос, проверка домашнего задания
2	Раздел 2. Обработка и использование информации	1	5,7 ,9, 11/ 4,6 ,8, 10	8	8			14		Опрос, проверка домашнего задания
3	Раздел 3. Передача информации	1	13, 15, 17 /12 ,14 ,16	6	6			12		Опрос, проверка домашнего задания
4	Контрольная работа	1	- /18		2					Контрольная работа
5	**Промежуточная аттестация**	1							36	**Экзамен. Контрольная работа**
	ИТОГО (108ч.)			**18**	**18**	**0**	**0**	**36**	**36**	

СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Раздел 1. Основные этапы жизненного цикла информации.

Тема 1.1. Жизненный цикл информации.

Понятие информации, меры информации. Накопление, хранение, обработка, передача, использование, уничтожение, обновление.

Накопление начальной информации, накопления вторичной информации. Кодирование информации с целью накопления. Кодирование информации с целью хранения.

Тема 1.2. Математика этапов накопления и хранения информации.

Свободная полугруппа, языки. Определение избытка информации в естественных языках. Задача управления избытком информации как одна из главных задач кибернетики. Алгоритмы сжатия информации.

Тема 1.3. Обзор аппаратного и программного обеспечения этапов накопления и хранения информации.

Аппаратное и программное обеспечение накопления начальной информации. Устройства ввода и вывода, периферийные устройства, кодовые таблицы, драйверы, архиваторы.

Раздел 2. **Обработка и использование информации.**

Тема 2.1. Математика этапа обработки информации.

Отношения на множествах. Бинарные отношения, свойства бинарных отношений. Отношение порядка, отношение эквивалентности. Упорядоченные множества, решётки.

Элементы теории графов. Задача о кёнигсбергских мостах и задача о коммивояжере. Типы графов. Маршруты и связанность. Степени.

Элементы теории конечных автоматов. Конечный детерминированный автомат. Решётки подавтоматов, конгруэнции автомата. Отношение неразличимости, минимизация конечных автоматов.

Тема 2.2. Обзор программного обеспечения обработки информации.

Инструментальный, системный и прикладной soft. Классификация программного обеспечения по типам обрабатываемой информации и по способу реализации. Основные программные пакеты по обслуживанию математических задач.

Раздел 3. Передача информации

Тема 3.2. Математика этапа передачи информации.

Конечные группы, симметрическая группа, мультипликативная группа классов вычетов взаимно простых с модулем.

Конечные поля. Простые поля положительной характеристики. Многочлены над конечными полями. Расширенный алгоритм Евклида.

Тема 3.1. Кодирование и шифрование.

Общая модель системы связи.

Основная задача помехоустойчивого кодирования. Код с вероятностной оценкой по формуле Бернулли, равновесный код, код проверки на чётность, код Хэмминга длины 7.

Криптографические алгоритмы, примеры симметрических и ассиметрических криптосистем. Криптографические протоколы, протокол Диффи и Хельмана, задача аутентификации и протокол с нулевым разглашением, разделение секрета на основе интерполяционных многочленов Лагранжа.

Тема 3.3. Обзор аппаратного и программного обеспечения этапа передачи информации.

Примеры аппаратной и программной реализации помехоустойчивого кодирования. Основные стандарты шифросистем, их характеристики и приложения.

Темы практических занятий

Практическое занятие 1. Полугруппы и языки.

Практическое занятие 2. Алгоритмы сжатия.

Практическое занятие 3. Отношение эквивалентности и отношение порядка.

Практическое занятие 4. Эйлеровы и Гамильтоновы графы.

Практическое занятие 5. Конечный детерминированный автомат и отношение неразличимости.

Практическое занятие 6. Симметрическая группа.

Практическое занятие 7. Мультипликативная группа классов вычетов взаимно простых с модулем.

Практическое занятие 8. Многочлены над простыми конечными полями.

Практическое занятие 9. Контрольная работа.

5. Образовательные технологии, применяемые при освоении дисциплины

В учебном процессе при реализации компетентностного подхода используются активные и интерактивные формы проведения занятий:

1) при проведении лекционных занятий: информационные лекции, проблемные лекции, лекции беседы, лекции дискуссии, лекции с заранее запланированными ошибками.

Проведение лекционных занятий по дисциплине основывается на активном методе обучения, при котором студенты не пассивные слушатели, а активные участники занятия, отвечающие на вопросы преподавателя. Вопросы преподавателя нацелены на активизацию процессов усвоения материала. Преподаватель заранее намечает список вопросов, стимулирующих ассоциативное мышление и установления связей с ранее освоенным материалом.

2) при проведении практических занятий: традиционные занятия, занятия исследования, проблемные ситуации, ситуации с ошибкой.

Практические занятия проводятся на основе реализации метода обучения действием: определяются проблемные области, формируются группы. При проведении практических занятий ставятся следующие цели: применение знаний отдельных тем и креативных методов для решения проблем; отработка у обучающихся навыков взаимодействия в составе коллектива; закрепление основ теоретических знаний.

Проведение некоторых практических занятий основывается на интерактивном методе обучения, при котором обучающиеся взаимодействуют не только с преподавателем, но и друг с другом. При этом доминирует активность обучающихся в процессе обучения. Место преподавателя в интерактивных занятиях сводится к направлению деятельности обучающихся на достижение целей занятия.

3) при организации самостоятельной работы студентов: поиск и обработка информации, в том числе с использованием информационно-коммуникационных технологий; исследование проблемной ситуации;

постановка и решение задач из предметной области; отработка навыков применения стандартных методов к решению задач предметной области.

Успешное освоение материала курса предполагает большую самостоятельную работу студентов и руководство этой работой со стороны преподавателей. Применяются следующие формы контроля: устный опрос, проверка решения практических задач, контрольная работа.

При проведении лекционных и практических занятий предусматривается использование информационных технологий: пакеты офисных программ (LibreOffice и др.) для создания презентаций, которые могут быть использованы при введении нового материала, а также для быстрого обзора предыдущего теоретического материала к текущему занятию; стандартные пакеты программ для визуализации и решения задач; языки программирования для решения практических заданий.

Удельный вес занятий, проводимых в интерактивных формах, определяется главной целью (миссией) программы, особенностью контингента обучающихся и содержанием конкретных дисциплин, и в целом в учебном процессе они должны составлять не менее 30% аудиторных занятий. Занятия лекционного типа для соответствующих групп студентов не могут составлять более 50% аудиторных занятий.

Особенности проведения занятий для граждан с ОВЗ и инвалидностью

При обучении лиц с ограниченными возможностями здоровья и инвалидностью используются подходы, способствующие созданию безбарьерной образовательной среды: технологии дифференциации и индивидуализации обучения, применение соответствующих методик по работе с инвалидами, использование средств дистанционного общения.

Для студентов с ограниченными возможностями здоровья и инвалидов предусмотрены следующие формы организации учебного процесса и контроля знаний:

-*для слабовидящих:*

обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

для выполнения контрольных заданий при необходимости предоставляется увеличивающее устройство;

задания для выполнения, а также инструкция о порядке выполнения контрольных заданий оформляются увеличенным шрифтом (размер 16-20);

- *для глухих и слабослышащих:*

обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости студентам предоставляется звукоусиливающая аппаратура индивидуального пользования;

- *для лиц с тяжелыми нарушениями речи, глухих, слабослышащих* все контрольные задания по желанию студентов могут проводиться в письменной форме.

Основной формой организации учебного процесса является интегрированное обучение инвалидов, т.е. все студенты обучаются в

смешанных группах, имеют возможность постоянно общаться со сверстниками, легче адаптируются в социуме.

6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

На данный курс отводится много часов для самостоятельной работы, поэтому существенные вопросы этого курса предполагается усвоить в процессе самостоятельной работы. В качестве рекомендуемой литературы предлагается использовать книги: (а) [1], (б) [1], (б) [7], (б) [8], которые содержат большое число упражнений, представляющих собой теоретические задачи по данному курсу. Предполагается написание рефератов по ряду вопросов курса, отведенным для самостоятельной работы, с последующим их обсуждением на практических занятиях для текущего контроля успеваемости и промежуточной аттестации.

Темы самостоятельных работ

1. Энтропия. (а) [1] стр. 18
2. Энтропия на сообщение дискретного стационарного источника. (а) [1] стр. 34
3. Прямая и обратная теоремы кодирования для дискретного постоянного источника. (а) [1] стр. 43
4. Монотонные коды. (а) [1] стр. 129
5. Интервальное кодирование и метод «стопка книг». (а) [1] стр. 133
6. Метод скользящего словаря (LZ-77). (а) [1] стр. 138
7. Алгоритм LZW (LZ-78). (а) [1] стр. 145
8. Сравнения способов кодирования, характеристики архиваторов. (а) [1] стр. 164
9. Бинарные отношения между множествами. (б) [1] стр. 30
10. Отношения эквивалентности. (б) [1] стр. 50
11. Упорядоченные множества. (б) [1] стр. 68-79
12. Решетки как упорядоченные множества и как алгебры. (б) [1] стр. 157
13. Графы, теорема о деревьях. (б) [1] стр. 7-8, 249
14. Формула Эйлера для планарных графов. (б) [1] стр. 7-8, 252
15. Теорема Понтрягина-Куратовского. (б) [1] стр. 7-8, 254
16. Критерий эйлерова графа. (б) [1] стр. 7-8, 258
17. Достаточное условие гамильтонова графа. (б) [1] стр. 7-8, 260
18. Автоматы, минимизация по отношению неразличимости. (б) [1] стр. 8-12, 329-333
19. Порождающие множества. (б) [7] стр. 24
20. Циклические группы и их структура. (б) [7] стр. 28, (б) [8] стр. 206.
21. Теорема Лагранжа. (б) [7] стр. 31, (б) [8] стр. 229.
22. Идеалы кольца, делители нуля, область целостности. (б) [8] стр. 283, 296.

23. Неприводимые многочлены. (б) [8] стр. 322
24. Поле вычетов по неприводимому многочлену. (б) [8] стр. 329
25. Помехоустойчивой код Хэмминга (линейный код). (а) [2] стр. 12-14,

Примерный вариант контрольной работы

Вариант 1

1. Для дискретного постоянного источника $X = \{a, b, c\}$ при распределении вероятностей $p(a) = p(b) = p(c) = 1/3$ определить собственную информацию каждой из букв, энтропию. Сколько информации содержится в последовательности *abaac*?
2. Задано число $m = 11$ и слова p: $x_0\,x_1$, $x_1\,x_1$, $x_2\,x_2\,x_2$, $x_1\,x_0\,x_2$, $x_0\,x_0\,x_1\,x_2\,x_2$.
   Запись $a \equiv b (\mathrm{mod}\ m)$ означает, что нужно положить число a равным остатку от деления числа b на число m. Через $[a]$ обозначается *целая часть* числа a, т.е. наибольшее целое число, не превосходящее a.

   Рассмотрим автомат $A=(S,X,Y,\delta,\lambda)$, где $S=\{s_0, s_1,\ldots, s_{m-1}\}$, $X=\{x_0, x_1, x_2\}$, $Y=\{y_0, y_1\}$, а функции δ: $S\times X\to S$ и λ: $S\times X\to Y$ определяются так:

   Для всех $s_i \in S$ и $x_j \in X$

   $\delta(s_i, x_j) = s_l$, где l: $\equiv i^2+j+N (\mathrm{mod}\ m)$ (N – номер варианта)

   $\lambda(s_i, x_j) = y_q$, где q: $\equiv \left[\frac{i+j+N}{2}\right] (\mathrm{mod}\ 2)$.

   Задание:

a) Выписать множество S;
b) Выписать таблицы для функций δ и λ;
c) Изобразить диаграмму автомата A;
d) Вычислить $\delta(s_0, p)$ и $\lambda(s_0, p)$ для всех заданных слов p;
e) Минимизировать автомат A. Для полученного минимального автомата B:
   – выписать множества состояний, входных и выходных сигналов;
   – выписать таблицы, задающие функции переходов и выходов автомата B;
   – изобразить диаграмму автомата B.

3. Для группы S_2 выписать все элементы и определить их порядки. Доказать, что группы первого, второго и третьего порядка являются циклическими.
4. Применяя расширенный алгоритм Евклида, найти a^{-1} в мультипликативной группе $FG(p)$, если $a = 126$, $p = 1789$.
5. Построить таблицы сложения и умножения для факторкольца $F_2[x]/(x^3 + x^2 + x)$. Определить, будет ли это кольцо полем.

Вариант 2

1. Для дискретного постоянного источника $X = \{a, b, c\}$ при распределении вероятностей $p(a) = p(b) = 1/4$, $p(c) = 1/2$ определить собственную информацию каждой из букв, энтропию. Сколько информации содержится в последовательности *abaac*?

2. Задано число $m = 12$ и слова p: $x_1 x_0$, $x_0 x_1$, $x_1 x_2 x_0$, $x_2 x_1 x_1$, $x_0 x_2 x_1 x_0 x_2$.
   Запись $a{:}\equiv b(\mathrm{mod}\ m)$ означает, что нужно положить число a равным остатку от деления числа b на число m. Через $[a]$ обозначается *целая часть* числа a, т.е. наибольшее целое число, не превосходящее a.

Рассмотрим автомат $A=(S,X,Y,\delta,\lambda)$, где $S=\{s_0, s_1,\ldots, s_{m-1}\}$, $X=\{x_0, x_1, x_2\}$, $Y=\{y_0, y_1\}$, а функции δ: $S\times X\to S$ и λ: $S\times X\to Y$ определяются так:

Для всех $s_i\in S$ и $x_j \in X$

$\delta(s_i, x_j)= s_l$, где l: $\equiv i^2+j+N(\mathrm{mod}\ m)$ (N – номер варианта)

$\lambda(s_i, x_j)=y_q$, где q: $\equiv\left[\frac{i+j+N}{2}\right](\mathrm{mod}\ 2)$.

Задание:

f) Выписать множество S;
g) Выписать таблицы для функций δ и λ;
h) Изобразить диаграмму автомата A;
i) Вычислить $\delta(s_0, p)$ и $\lambda(s_0, p)$ для всех заданных слов p;
j) Минимизировать автомат A. Для полученного минимального автомата B:
   – выписать множества состояний, входных и выходных сигналов;
   – выписать таблицы, задающие функции переходов и выходов автомата B;
   – изобразить диаграмму автомата B.

3. Для группы S_3 выписать все элементы и определить их порядки. Доказать, что группа простого порядка является циклической.
4. Применяя расширенный алгоритм Евклида, найти a^{-1} в мультипликативной группе $FG(p)$, если $a = 1541$, $p = 1823$.
5. Построить таблицы сложения и умножения для факторкольца $F_2[x]/(x^3 + x)$. Определить, будет ли это кольцо полем.

Вопросы для текущего контроля успеваемости

1. Понятие информации, различие между данными и информацией.
2. Энтропия на сообщение дискретного стационарного источника
3. Синтаксическая мера информации.
4. Семантическая мера информации и понятие тезауруса.
5. Прагматическая мера информации.
6. Модель системы связи.
7. В каких случаях применяется помехоустойчивое кодирование.
8. Системы добычи данных (получение и накопление первичной информации).
9. Классификация систем добычи знаний (получения вторичной информации).
10. Основные этапы жизненного цикла информации.
11. Отношения на множестве, свойства бинарных отношений.
12. Произведение бинарных отношений.
13. Полугруппа, теорема о представлении всякой полугруппы полугруппой преобразований.
14. Свободная полугруппа, теорема о представлении произвольной полугруппы гомоморфным образом свободной полугруппы.
15. Отношение эквивалентности, фактор-множество, трансверсаль.
16. Свободный моноид, язык, код.
17. Избыток информации в естественных языках.

18. Методы сжатия без потерь.
19. Метод скользящего словаря (LZ-77).
20. Алгоритм LZW (LZ-78).
21. Методы сжатия изображений.
22. Методы сжатия видеоданных.
23. Отношение порядка, упорядоченные множества, решётки.
24. Графы, теорема о деревьях.
25. Критерий эйлерова графа.
26. Достаточное условие гамильтонова графа.
27. Конечный детерминированный автомат, способы задания.
28. Гомоморфизм и изоморфизм автоматов, сравнимые автоматы.
29. Подавтоматы, решётка подавтоматов, отношение достижимости.
30. Конгруэнции, фактор-автомат.
31. Отношение неразличимости, минимизация автомата.
32. Группа, симметрическая группа.
33. Группа классов вычетов взаимно простых с модулем.
34. Кольца и поля, простые конечные поля и их конечные расширения.
35. Код с вероятностной оценкой по формуле Бернулли.
36. Код Хэмминга длины 7.
37. Шифры перестановок и шифры замены.
38. Шифрование с открытым ключом.
39. Основные современные стандарты шифрования.
40. Протокол Диффи и Хельмана.
41. Доказательство с нулевым разглашением на основе гамильтоновых графов.
42. Аутентификация на основе протокола с нулевым разглашением.
43. Разделение секрета на основе интерполяционных многочленов Лагранжа.

Вопросы для промежуточной аттестации по итогам освоения дисциплины

1. Понятие информации, различие между данными и информацией.
2. Энтропия на сообщение дискретного стационарного источника
3. Синтаксическая мера информации.
4. Модель системы связи.
5. Основные этапы жизненного цикла информации.
6. Отношения на множестве, свойства бинарных отношений.
7. Произведение бинарных отношений.
8. Теорема о представлении всякой полугруппы полугруппой преобразований.
9. Теорема о представлении полугруппы гомоморфным образом свободной полугруппы.
10. Отношение эквивалентности, фактор-множество, трансверсаль.
11. Свободный моноид, язык, код.
12. Избыток информации в естественных языках.
13. Метод скользящего словаря (LZ-77).
14. Алгоритм LZW (LZ-78).
15. Отношение порядка, упорядоченные множества, решётки.
16. Графы, теорема о деревьях.
17. Критерий эйлерова графа.
18. Конечный детерминированный автомат, способы задания.
19. Конгруэнции, фактор-автомат.
20. Отношение неразличимости, минимизация автомата.
21. Симметрическая группа, порождающее множество.
22. Группа классов вычетов взаимно простых с модулем.

23. Кольца и поля, простые конечные поля.
24. Код с вероятностной оценкой по формуле Бернулли.
25. Код Хэмминга длины 7.
26. Шифры перестановок и шифры замены.
27. Шифрование с открытым ключом.
28. Основные современные стандарты шифрования.
29. Протокол Диффи и Хельмана.
30. Доказательство с нулевым разглашением на основе гамильтоновых графов.
31. Аутентификация на основе протокола с нулевым разглашением.
32. Разделение секрета на основе интерполяционных многочленов Лагранжа.

7. Данные для учета успеваемости студентов в БАРС

Таблица 1.1 Таблица максимальных баллов по видам учебной деятельности.

1	2	3	4	5	6	7	8	9
Семестр	Лекции	Лабораторные занятия	Практические занятия	Самостоятельная работа	Автоматизированное тестирование	Другие виды учебной деятельности	Промежуточная аттестация	Итого
1	10	0	15	15	0	20	40	**100**

Программа оценивания учебной деятельности студента
1 семестр

Лекции
Посещаемость, активность, умение выделить главную мысль и др. (от 0 до 10 баллов)
Критерии оценки:
- менее 25% – 0 баллов;
- от 25% до 50% – 4 баллов;
- от 51% до 75% – 7 баллов;
- от 76% до 100% – 10 баллов.

Лабораторные занятия
Не предусмотрены
Практические занятия
Самостоятельность при выполнении работы, активность работы в аудитории, правильность выполнения заданий, уровень подготовки к занятиям и т.д. (от 0 до 15 баллов)
Критерии оценки:
- менее 25% – 0 баллов;
- от 25% до 50% – 5 баллов;
- от 51% до 75% – 10 баллов;
- от 76% до 100% – 15 баллов.

Самостоятельная работа

Качество и количество выполненных домашних работ, правильность выполнения и т.д. (от 0 до 15 баллов)

Критерии оценки:

- менее 25% – 0 баллов;
- от 25% до 50% – 5 баллов;
- от 51% до 75% – 10 баллов;
- от 76% до 100% – 15 баллов.

Автоматизированное тестирование

Не предусмотрено.

Другие виды учебной деятельности

Контрольная работа (от 0 *до* 20 *баллов)*

Промежуточная аттестация – *от 0 до 40 баллов*

Формой промежуточной аттестации по итогам освоения дисциплины в 1 семестре является *экзамен*, который проводится в виде ответа на экзаменационный билет, состоящий из двух вопросов. Задаются еще два – три дополнительных вопроса из перечня вопросов к промежуточной аттестации. На прохождение аттестации студенту отводится 30 минут.

При проведении промежуточной аттестации
ответ на «отлично» оценивается от 31 до 40 *баллов;*
ответ на «хорошо» оценивается от 21 до 30 *баллов;*
ответ на «удовлетворительно» оценивается от 11 до 20 *баллов;*
ответ на «неудовлетворительно» оценивается от 0 до 10 *баллов.*

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за 1 семестр по дисциплине «Математические основы информационного обслуживания» составляет **100** баллов.

Таблица 2.2 Таблица пересчета полученной студентом суммы баллов по дисциплине «Математические основы информационного обслуживания» в оценку (экзамен):

85 – 100 баллов	«отлично»
71 – 84 баллов	«хорошо»
56 – 70 баллов	«удовлетворительно»
менее 55 баллов	«неудовлетворительно»

9. Материально-техническое обеспечение дисциплины

Лекционные и практические занятия проводятся в аудиториях на 15-20 посадочных мест. В отведенных для занятий аудиториях имеются учебные доски для требуемых визуализаций излагаемой информации.

В ходе лекционных и практических занятий могут использоваться учебно-демонстрационные мультимедийные презентации, которые обеспечиваются следующим техническим оснащением:

1. Компьютеры (в комплекте с колонками).
2. Мультимедийный проектор
3. Экран.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 02.04.01 Математика и компьютерные науки и профилю подготовки «Математические основы компьютерных наук».

Автор
доцент кафедры геометрии Новиков В.Е.

Программа актуализирована и утверждена на заседании кафедры геометрии от 11 сентября 2024 года, протокол № 3.

Приложение

Учебно-методическое и информационное обеспечение дисциплины

Рекомендуемая литература:

1. Богомолов А. М., Салий В. Н. Алгебраические основы теории дискретных систем – М.: Наука, Физматлит, 1997. - 367 с.
2. Панин В.В. Основы теории информации [Текст] : учеб. пособие для вузов / В.В. Панин. - 3-е изд., испр. и доп. - Москва : БИНОМ. Лаб. знаний, 2011. - 438 с.
3. Салий В.Н. Универсальная алгебра и автоматы [Текст] : учеб. пособ. для студентов мех.-мат. фак. / В.Н. Салий. - Саратов : Изд-во Сарат. ун-та, 1988. - 71 с.
4. Верников Б.М. Элементы теории графов [Текст] : учеб. пособие / Б. М. Верников ; Федер. агентство по образованию, Урал. гос. ун-т им. А.М. Горького. - Екатеринбург : Изд-во Урал. ун-та, 2005. - 191 с.
5. Биркгоф Г. Современная прикладная алгебра [Текст] : [учеб. пособие] / Г. Биркгоф, Т. К. Барти ; пер. с англ. Ю. И. Манина. - 2-е изд., стер. - Санкт-Петербург ; Москва ; Краснодар : Лань, 2005.
6. Логачёв, О.А. Булевы функции в теории кодирования и криптологии [Текст] / О.А. Логачёв, А.А. Сальников, В.В. Ященко. - Москва : Изд-во МЦНМО, 2024. - 288 с.
7. Математические и компьютерные основы криптологии [Текст] : учеб. пособие / Ю. С. Харин, В. И. Берник, Г. В. Матвеев, С. В. Агиевич. - Минск : Новое знание, 2003. - 381 с.
8. Сидельников В.М. Теория кодирования. — М.: ФИЗМАТЛИТ, 2008, 324 с.
9. Балюкевич, Э. Л. Теория информации и кодирования [Электронный ресурс] : учебное пособие / Балюкевич Э. Л. - Москва : Евразийский открытый институт, Московский государственный университет экономики, статистики и информатики, 2004. - 113 с. (ЭБС IPRbooks).
10. Гаврилов Г.П. Задачи и упражнения по дискретной математике [Текст] : учеб. пособие / Г. П. Гаврилов, А. А. Сапоженко. - 3-е изд., перераб. - Москва : ФИЗМАТЛИТ, 2005. - 416 с.