НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«Київський політехнічний інститут імені Ігоря Сікорського»

Затверджую

Голова Приймальної комісії
Ректор

Михайло
ЗГУРОВСЬКИЙ
підпис
25.04.2024р
дата

ПРОГРАМА
вступного іспиту із спеціальності

для вступу на освітньо-наукову програму підготовки доктора філософії
«Прикладна математика»

за спеціальністю 113 Прикладна математика

Програму ухвалено:
Науково-методичною комісією
за спеціальністю 113 Прикладна математика
Протокол №2 від 19.04.2024 р.
Голова НМК
_____ Михайло САВЧУК

Київ 2024

ЗМІСТ

ІІ. ТЕМИ, ЩО ВИНОСЯТЬСЯ НА ВСТУПНИЙ ІСПИТ

1. Дискретна математика, математична логіка та теорія алгоритмів

1.1. Множини і операції над ними; алгебра множин; потужність множини, кардинальні числа. Відношення на множинах; способи представлення бінарних відношень, операції над відношеннями, властивості бінарних відношень. Відношення еквівалентності, відношення часткового порядку, їх властивості. Функціональні відношення та відображення, їх властивості.

1.2. Основні комбінаторні конфігурації: вибірки, розміщення, перестановки. Потужності комбінаторних конфігурацій. Біноміальні коефіцієнти, їх властивості, біном Ньютона. Конструктивний перелік дискретних об'єктів.

1.3. Булеві функції; представлення булевих функцій таблицею істинності та формулами, елементарні булеві функції; закони булевої алгебри. Досконалі нормальні форми (ДДНФ, ДКНФ, АНФ), поліноми Жегалкіна. Повнота системи булевих функцій, критерій Поста.

1.4. Графи неорієнтовані та орієнтовані; способи представлення графів, матриця суміжності, матриця інцидентності; операції над графами. Зв'язність графів. Способи обходу вершин графів, пошук в ширину, пошук в глибину. Дерева та їх властивості. Ейлерові графи, гамільтонові графи, планарні графи, їх властивості.

1.5. Теорія автоматів: абстрактні автомати та способи їх представлення; розпізнавачі, автомати Мілі та автомати Мура.

1.6. Математична логіка: формально-логічні числення, синтаксис і семантика, теорія доведень, теорія моделей; аксіоматичні теорії, формальна теорія L; формальна арифметика, аксіоматична теорія множин.

1.7. Логіка висловлювань, логіка предикатів 1-го порядку (квантори, інтерпретація, правила виводу, випереджені та скулемівські нормальні форми, метод резолюцій для логіки предикатів).

1.8. Теорія алгоритмів: формалізації понять алгоритму та обчислювальності; машини Тьюрінга; нормальні алгоритми Маркова; рекурсивні функції та рекурсивні множини; проблеми алгоритмічної розв'язності, тезис Черча-Поста; Геделева нумерація та теорема Геделя про повноту; складність алгоритмів, NP-повні проблеми.

2. Чисельні методи

2.1. Чисельні методи лінійної алгебри.

2.2. Чисельне інтегрування, інтерполяція та згладжування.

2.3. Чисельні методи розв'язування диференціальних (звичайних та в частинних похідних) та інтегральних рівнянь.

2.4. Чисельні методи розв'язування операторних рівнянь.

2.5. Оптимізація чисельних методів.

6.5. Методи нормалізації критеріїв. Методи врахування жорсткого пріоритету. Методи врахування гнучкого пріоритету.

6.6. Методи зведення до узагальненого критерію (згортки). Метод головного критерію. Метод послідовних поступок.

6.7. Визначення нечіткої множини. Операції над нечіткими множинами. Відстань між нечіткими підмножинами. Спеціальні операції над нечіткими множинами. Нечіткі відношення, їх властивості та класифікація.

6.8. Функції корисності (ФК) в задачах вибору.

6.9. Відношення еквівалентності, байдужості, переваги, домінування.

6.10. Критерії Вальда, Савіджа, Гурвіца, Ходжеса – Лемана.

7. Математичне моделювання: системний підхід

7.1. Система, складна система, основні властивості і життєвий цикл систем. Основні категорії системного підходу в задачах моделювання складних систем.

7.2. Фізичне та математичне моделювання. Детерміновані, евристичні, імітаційні та ймовірнісні моделі. Внутрішні та зовнішні збурення.

7.3. Математичні моделі динамічних процесів із зосередженими параметрами. Дискретні та неперервні процеси. Адекватність моделей.

7.4. Математичні моделі динамічних процесів з розподіленими параметрами. Коректність моделей.

7.5. Методи ідентифікації параметрів математичних моделей.

8. Математичне моделювання: прикладні аспекти

8.1. Послідовність етапів побудови математичної моделі. Поняття коректності задачі та моделі, фактори, що впливають на вибір методу розв'язання задачі. Перевірка адекватності моделі.

8.2. Проста лінійна регресія. Оцінка точності моделі. Метод найменших квадратів. Багатовимірна лінійна регресія. Побудова прогнозів. Перехресна перевірка. Оцінка взаємозалежності випадкових величин. Рівень значимості лінійного взаємозв'язку.

8.3. Математичні моделі розв'язання задач лінійного програмування. Задачі оптимізації моделей. Методи оптимізації першого порядку (градієнтний метод, метод найшвидшого спуску, метод спряжених градієнтів). Методи оптимізації вищого порядку.

8.4. Генерація випадкових чисел з рівноімовірним розподілом, моделювання випадкових подій і величин. Метод Монте-Карло та його застосування.

8.5. Мережі Петрі, графічне та аналітичне зображення, основні задачі та характеристики.

8.6. Моделі на графах. Пошук мінімального шляху на графі. Пошук в ширину, пошук в глибину. Алгоритм Дейкстри, Алгоритм Флойда. Алгоритми пошуку максимального потоку (Форда й Фалкерсона).

9. Методи та алгоритми криптографії та криптоаналізу

9.1. Основні поняття криптології. Задачі, напрямки та методи захисту інформації. Криптографічний захист інформації, основні терміни та означення. Моделі джерел відкритого тексту, ентропія на символ джерела. Загальна класифікація класичних і сучасних шифрів.

9.2. Симетрична криптографія: класичні схеми шифрування. Визначення шифру підстановки (заміни), моноалфавітні та поліалфавітні підстановки. Визначення шифру перестановки. Класичні шифри: Цезаря, афінної заміни, Хілла, шифр загальної простої підстановки, Віженера, табличні перестановки, грати Кардано та інші. Частотний криптоаналіз шифрів Цезаря, афінної підстановки та Віженера.

9.3. Теорія секретних систем Шеннона. Ієрархія типів атак на криптосистему. Теоретична та практична стійкість. Ентропія. Цілком таємні криптосистеми. Границя Шеннона. Ненадійність ключа та відкритого тексту Відстань однозначності. Принципи Шеннона побудови стійких шифрів.

9.4. Системи блокового та потокового шифрування. Схема Фейстеля. Стандарти блокового шифрування DES, ДСТУ ГОСТ 28147:2009, AES. Регістри зсуву з лінійним зворотним зв'язком. Способи введення нелінійності у схеми потокового шифрування на регістрах зсуву з лінійним зворотним зв'язком.

9.5. Асиметрична криптографія та важкооборотні функції. Проблеми симетричної криптографії 70-х років XX століття. Загальні означення важкооборотної функції, важкооборотної функції зі секретом. Важкооборотні функції Діффі-Хеллмана, RSA, Рабіна. Оцінки складності обчислення та обернення функцій. Схема відкритого розподілу ключів Діффі-Хеллмана.

9.6. Асиметричні системи шифрування. Загальна концепція асиметричних криптосистем шифрування з відкритими ключами. Системи шифрування Мессі-Омури, Ель-Гамаля, RSA, Рабіна. Побудова асиметричних шифросистем, алгоритми зашифрування та розшифрування.

9.7. Геш-функції. Означення та криптографічні властивості геш-функцій. Загальні схеми побудови. Колізії геш-функцій. Оцінки ймовірностей колізій та трудомісткості їх побудови. Застосування геш-функцій.

9.8. Цифровий підпис. Задачі цифрового підпису. Загальна концепція та схема цифрового підпису з геш-функцією в асиметричної криптографії. Цифровий підпис у схемі RSA з використанням геш-функцій, цифрові підписи Ель-Гамаля, Рабіна. Сліпий підпис. Атаки на цифровий підпис.

9.9. Криптографічні протоколи. Протоколи розподілу секретів, доведення без розголошення, схеми пред'явлення випадкових бітів, протоколи електронної готівки. Криптографічні алгоритми автентифікації: парольна

автентифікація, автентифікація з використанням симетричних та асиметричних криптосистем.

9.10. Цілі та підходи у криптоаналізі. Задачі захисту інформації та криптоаналізу. Класифікація атак на криптографічні системи захисту інформації. Підходи до визначення стійкості та до криптоаналізу криптосистем: теоретико-інформаційний, баєсівський, системний, семантичний підхід, доказова стійкість та інші. Загальні методи криптоаналізу симетричних і асиметричних криптосистем.

ІІІ. НАВЧАЛЬНО-МЕТОДИЧНІ МАТЕРІАЛИ

Література до розділу 1

1. Темнікова О.Л. Дискретна математика: Конспект лекцій (Частина 1) [Електронний ресурс]: навч. посіб. для студ. спеціальності 113 «Прикладна математика», освітньої програми «Наука про дані та математичне моделювання» / О.Л. Темнікова ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,97 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 154 с.

2. Темнікова О.Л. Дискретна математика: Конспект лекцій (Частина 2) [Електронний ресурс]: навч. посіб. для студ. спеціальності 113 «Прикладна математика», освітньої програми «Наука про дані та математичне моделювання» КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 1,84 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2019. – 128 с.

3. Бардачов Ю.М., Соколова Н.А., Ходаков В.Є. Дискретна математика. – К.: Вища школа. 2002. – 287 с.

4. Нікольський Ю.В., Пасічник В.В., Щербина Ю.М. Дискретна математика. – К.: Видавнича група BHV. 2007. – 368 с.

5. Темнікова О.Л. Дискретна математика: практикум з дисципліни «Дискретна математика» для студентів спеціальності 113 «Прикладна математика» [Електронне видання] – К. : КПІ ім. Ігоря Сікорського, 2018. – 88 с.

6. Темнікова О.Л. Математична логіка. Практикум [Електронний ресурс]: навч. посіб. для студ. спеціальності 113 «Прикладна математика», освітньої програми «Наука про дані та математичне моделювання»; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 1,37 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2020. – 76 с.

7. Темнікова О.Л. Математична логіка та теорія алгоритмів: Конспект лекцій [Електронний ресурс]: навч. посіб. для студ. спеціальності 113 «Прикладна математика», освітньої програми «Наука про дані та математичне моделювання» / О.Л.Темнікова ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 3,60 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 177 с.

8. Темнікова О.Л. Теорія алгоритмів. Алгоритмічні схеми. Практикум [Електронний ресурс]: навч. посіб. для студ. спеціальності 113 «Прикладна математика», освітньої програми «Наука про дані та математичне моделювання» / О.Л.Темнікова ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 1,54 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2022. – 43 с.

9. Нікольський Ю.В., Пасічник В.В., Щербина Ю.М. Системи штучного інтелекту : Навчальний посібник. За ред. В.В.Пасічника. – 2-ге вид., випр. та доп. - Львів : Магнолія -2006, 2013.

Література до розділу 2

1. В.В. Третинник, Н.Д. Любашенко. Методи обчислень, частина 1. Чисельні методи алгебри : навчальний посібник – Київ, КПІ ім. Ігоря Сікорського, 2019.

2. М.А. Новотарський. Алгоритми та методи обчислень [Електронний ресурс]. – КПІ ім. Ігоря Сікорського, 2019. – Режим доступу: https://ela.kpi.ua/bitstream/123456789/27864/1/Alhorytmy_ta_metody_obchislenn.pdf

3. Комп'ютерне моделювання систем та процесів. Методи обчислень. Гл.5, Методи розв'язання диференціальних рівнянь в частинних похідних./Квєтний Р.Н. та ін. Електронний ресурс. - Режим доступу: https://web.posibnyky.vntu.edu.ua/fksa/2kvetnyj_komp%27yuterne_modelyuvannya_system_procesiv/t1/5.htm

4. Б.М. Ляшенко, О.М. Кривонос, Т.А. Вакалюк. Методи обчислень : навчально-методичний посібник для студентів фізико-математичного факультету [Електронний ресурс]. – Житомир, вид-во ЖДУ ім. І. Франка, 2014. – Режим доступу: http://eprints.zu.edu.ua/18543/1/metody_obchyslen.pdf

5. James F. Epperson. An introduction to numerical methods and analysis / Mathematical Reviews. — Second edition, 2013.

Література до розділу 3

10. Гнєденко Б.В. Курс теорії ймовірностей. – К.: ВПЦ Київський університет, 2010. – 464 с.

11. Турчин В.Н. Теорія ймовірностей і математична статистика. Основні поняття, приклади, задачі: Підручник для студентів вищих навчальних закладів. – Дніпропетровськ: ІМА-прес, 2014. - 556 с.

12. Огірко О. І., Галайко Н. В. Теорія ймовірностей та математична статистика: навчальний посібник. –Львів: ЛьвДУВС, 2017. – 292 с.

13. Турчин В.Н. Теорія ймовірностей: Основні поняття, приклади, задачі: Навч. посіб. – К.: Видавництво А.С.К., 2004. – 208 с.

14. Скороход А.В. Лекції з теорії випадкових процесів: Навч. Посібник. – К.: Либідь, 1990. - 168 с.

15. Новицький І.В. Випадкові процеси. Навчальний посібник / І.В. Новицький, С.А. Ус. – Д.: Національний гірничий університет, 2011. – 125 с.

16. Дороговцев А.Я., Сільвестров Д.С., Скороход А.В., Ядренко М.Й. Теорія ймовірностей. Збірник задач. – К.: Вища школа, 1976. – 384 с.

Література до розділу 4

1. Капітонова Ю.В., Кривий С.Л., Летичевський О.А. і ін. Основи дискретної математики. - Київ: Наукова думка, 2002.-580с.

2. Базилевич Л.Є. Дискретна математика у прикладах і задачах: підручник. – Львів: Видавець І.Е. Чижиков, 2013 – 488 с.

3. Riordan J. An Introduction to Combinatorial Analysis. – New York: John Wiley & Sons, Ins. London.Chapman & Hall, Limited, 1958.

4. Reincold E., Nievergelt J., Deo N. Combinatorial Algorithms. Theory and Practice. – New Jersey: Prentice-Hall, Inc., Englewood Cliffs, 1977.

5. Дискретний аналіз. Курс лекцій для студентів спеціальностей, пов'язаних з інформаційними технологіями та захистом інформації. Частина 1. Множини та відношення. Укладач Мороховець М.К. – К.: НТУУ «КПІ», 2006. – 68 с.

6. Дискретний аналіз. Курс лекцій для студентів спеціальностей, пов'язаних з інформаційними технологіями та захистом інформації. Частина 4. Елементи загальної алгебри. Укладач Мороховець М.К. – К.: НТУУ «КПІ», 2015. – 81с.

7. Бородін О.І. Теорія чисел. - К.: Видавництво «Радянська школа», 1960. – 244 с.

8. Завадська Л.О. Спеціальні розділи математики. Елементи теорії скінченних полів. – К.: Політехніка, 2006. – 54с.

9. Ковальчук Л. В., Яремчук Ю. Є. Прикладна алгебра. Частина 1. Основи абстрактної алгебри. – Вінниця: ВНТУ, 2015. – 98 с.

10. Ковальчук Л. В., Яремчук Ю. Є. Прикладна алгебра. Частина 2. Теорія чисел. – Вінниця: ВНТУ, 2017. – 129 с.

Література до розділу 5

1. Burkov, A. (2019) The Hundred-Page Machine Learning Book (https://themlbook.com/).

2. James, G.M., Witten, D.M., Hastie, T.J., & Tibshirani, R. (2021). An Introduction to Statistical Learning. Springer Texts in Statistics (https://hastie.su.domains/ISLR2/ISLRv2_website.pdf).

3. Кононова К. Ю. Машинне навчання: методи та моделі. – Харків: ХНУ імені В. Н. Каразіна, 2020. – 301 с. (https://github.com/katerynakononova/ML/blob/master/ML.pdf)

4. Інтелектуальний аналіз даних та машинне навчання. Ч. 1 : Базові методи та засоби аналізу даних / Я. В. Іванчук та ін. / Вінниц. нац. техн. ун-т. - Вінниця : ВНТУ, 2021. - 68 с. (http://pdf.lib.vntu.edu.ua/books/2022/Ivanchuk_P1_2021_69.pdf).

Література до розділу 6

1. Томашевський В.М. Моделювання систем. – К.: Видавнича група BHV, 2005. – 352 с.

2. Зайченко Ю.П. Теорія прийняття рішень: підручник. – НТУУ «КПІ», 2014. – 412 с.

3. О. Ф. Волошин Моделі та методи прийняття рішень [Електронний ресурс]: навч. посіб. для студ. вищ. навч. закл. / О. Ф. Волошин, С. О. Мащенко. – 3-є вид., перероб. – К.: «Видавництво Людмила», 2018. – 292 с.

4. Верес О. М. Технології підтримки процесів прийняття рішень : підручник / О.М. Верес, А.В. Катренко, В.В. Пасічник; Міністерство освіти і науки України. – Львів :"Новий Світ-2000",2021. – 567 сторінок.

5. Висоцька В. А. Методи та засоби функціонування систем підтримки прийняття рішень на основі онтологій :монографія / В.А. Висоцька, Д.Г. Досин, Х.І. Микіч, І.І. Завущак, З.Л. Рибчак; Міністерство освіти і науки України, Національний університет "Львівська політехніка". – Львів :Видавництво "Новий Світ-2000", 2021. – 334 сторінки.

6. Григорків В. С. Моделі прийняття рішень в економіці :навчальний посібник / В.С. Григорків, М.В. Григорків; Міністерство освіти і науки України, Чернівецький національний університет імені Юрія Федьковича. – Чернівці :Чернівецький національний університет імені Юрія Федьковича,2021. – 255 сторінок.

7. Катренко А. В. Прийняття рішень: теорія та практика : підручник / А.В. Катренко, В.В. Пасічник; за науковою редакцією В.В. Пасічника; Міністерство освіти і науки. – Львів : "Новий Світ-2000",2021. – 446 сторінок.

8. Кузьмін О. Є. Системний аналіз і прийняття інноваційних рішень :навчальний посібник / О.Є. Кузьмін, О.О. Жовтанецька, Н.О. Заяць ; Міністерство освіти і науки України. – Львів :Видавництво "Новий Світ-2000", 2021. – 226 сторінок.

9. Згуровський, М. З. Combinatorial Optimization Problems in Planning and Decision Making :Theory and Applications / Mikhail Z. Zgurovsky, Alexander A. Pavlov. – Cham, Switzerland :Springer,2019. – 471 сторінка.

10. В.Є. Стрілець Методи машинного навчання у задачах системного аналізу і прийняття рішень: монографія/ В.Є. Стрілець, С.І. Шматов, М.Л. Угрюмов, Є.С. Мєняйлов [та 2 інших]; Міністерство освіти і науки України, Харківський національний університет імені В.Н. Каразіна. – Харків: ХНУ імені В.Н. Каразіна, 2020. – 159 сторінок.

11. М.П. Бутко Теорія прийняття рішень: підручник для студентів вищих навчальних закладів / М.П. Бутко [та ін.]; за загальною редакцією М.П. Бутка; Міністерство освіти і науки України; Чернігівський національний технологічний університет. – Київ: Центр учбової літератури, 2018. – 356 с.

12. Нестеренко О.В. Інтелектуальні системи підтримки прийняття рішень: навчальний посібник / Нестеренко О.В., Савенков О.І., Фаловський О.О.; Київ, Національна академія управління, 2016, - 188 сторінки.

13. Marchau, V. A., Walker, W. E., Bloemen, P. J., & Popper, S. W. (2019). Decision making under deep uncertainty: from theory to practice (405 p.). Springer Nature.

Література до розділів 7 та 8

14. Математичне моделювання систем і процесів [Електронний ресурс] : конспект лекцій для студентів спеціальності 153 «Мікро- та наносистемна техніка» спеціалізації «Електронні біомедичні системи і технології» «Інформаційні технології проектування в електроніці та наносистемах» / КПІ ім. Ігоря Сікорського ; уклад.: П. П. Лошицький. – Електронні текстові дані (1 файл: 5,48 Мбайт). – Київ, 2018. Київ, 2018. https://ela.kpi.ua/handle/123456789/41228

15. Мельник, В. П. Моделювання складних систем і процесів :навчальний посібник для студентів старших курсів і аспірантів університетів /В.П. Мельник. – Івано-Франківськ :НАІР,2018. – 258 с. Івано-Франківськ : НАІР, 2018.

16. Виклюк, Я. І. Моделювання складних систем :посібник /Я.І. Виклюк, Р.М. Камінський, В.В. Пасічник ; за загальною редакцією В.В. Пасічника ; Міністерство освіти і науки України, Національний університет "Львівська політехніка". – Львів :Новий Світ-2000,2017 .– 403 с. Львів :Новий Світ-2000, 2017.

17. Eck, Christof. Mathematical Modeling[electronic resource] /by Christof Eck, Harald Garcke, Peter Knabner.1st ed. 2017.Cham :Springer International Publishing :Imprint: – Springer,2017.XV, –509 p. Cham :Springer International Publishing :Imprint: Springer,2017. https://doi.org/10.1007/978-3-319-55161-6 Доступно через SpringerLink лише в локальній мережі НТБ КПІ ім. Ігоря Сікорського.

18. Бахрушин В.Є. Математичне моделювання. – Запоріжжя: ГУ «ЗІДМУ», 2004. – 140 с.

19. Математичне моделювання: комп'ютерний практикум з дисципліни «Математичне моделювання. Т. С. Ладогубець, О. Д. Фіногенов – Київ: КПІ ім. Ігоря Сікорського, 2018. – 58 с.

20. Махней О. В., Супрун В.П. Математичне моделювання. — Івано-Франківськ, 2015. – 372 с.

21. Маценко В.Г. Математичне моделювання. – Чернівці: Чернівецький національний університет, 2014. – 519 с.

22. Стеценко І.В. Моделювання систем. – Черкаси : ЧДТУ, 2010. – 399 с.

23. Трусов П.В. Введение в математическое моделирование. Учебное пособие. – М.: Логос, 2016. – 440 с.

24. Томашевський В.М. Моделювання систем. – К.: Видавнича група BHV, 2005. – 352 с.

25. Математичні моделі в менеджменті та маркетингу: навчальний посібник / за заг. ред. О. В. Кузьменко/. – Суми: видавництво "Ярославна», 2020, – 214 с.

26. Математичне моделювання систем і процесів: комп'ютерний практикум [Електронний ресурс]: навчальний посібник для студентів спеціальності 121 «Інженерія програмного забезпечення», спеціалізації «Програмне забезпечення комп'ютерних та інформаційно-пошукових систем» / І. А. Дичка, М. В. Онай, Р. А. Гадиняк ; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,95 Мбайт). – Київ: КПІ ім. Ігоря Сікорського, 2018. – 130 с. https://ela.kpi.ua/handle/123456789/23550

27. Математичне моделювання нерівноважних процесів у складних системах: монографія /Білущак Ю., Гайвась Б., Гера Б., Грицина О. [та 10 інших]; під загальною редакцією Євгена Чаплі; Національна академія наук України, Центр математичного моделювання Інституту прикладних проблем механіки і математики ім. Я.С. Підстригача. – Львів: Растр-7,2019. – 253 сторінки.

Література до розділу 9

28. Koblitz N. A course in number theory and cryptography. – N.Y.: Springer-Verlag, 1987. – P. 312.

29. Математичні методи захисту інформації. Курс лекцій. Ч І. / Укладачі Завадська Л.О., Савчук М.М. – К.: НТУУ «КПІ», 2008. – 128 с.

30. Кузнецов Г.В., Фомичев В.В., Сушко С.О. Фомичова Л.Я. Математичні основи криптографії. – Дніпропетровськ: Національний гірничій університет, 2004. – Ч.1. – 391 с.

31. Вербіцький О.В. Вступ до криптології. – Львів: Науково-технічна література, 1998. – 248с.

32. Сушко С.О., Кузнецов В.Г., Фомичева Л.Я., Корабльов А.В. Математичні основи криптоаналізу. – Д.: Національний гірничий університет, 2010. – 466 с.

33. Задірака В.К., Олексюк О.С. Комп'ютерна криптологія. – К.: 2002. – 504 с.

34. Katz Jonathan, Lindell Yehuda. Introduction to Modern Cryptography. – Boca Raton London New York: Chapman & Hall /CRC Taylor & Francis Group, 2008. – 534 p.

35. Henk C.A. van Tilborg. Fundamentals of Cryptology. – A Professional Reference and Interactive Tutorial. – Kluwer Academic Publishers, 1999, 2000. Second Printing 2001.

36. Mao Wenbo. Modern Cryptography. Theory and Practice. - Prentice Hall PTR, Upper Saddle River, New Jersey, 2004.

37. Schneier B. Applied Cryptography: protocols, algorithms and source code in C. John Wiley & Sons, New York, 1996.

IV. РЕЙТИНГОВА СИСТЕМА ОЦІНЮВАННЯ ВСТУПНОГО ІСПИТУ

1. Початковий рейтинг вступника за екзамен розраховується за 100-бальною шкалою. При визначенні загального рейтингу вступника початковий рейтинг за екзамен перераховується у оцінку за 200-бальною шкалою за відповідною таблицею перерахунку (п. 4 цього розділу).

2. Екзаменаційний білет вступного екзамену складається з 2 частин – тестової частини та усної відповіді на відкрите завдання. У випадку дистанційної форми проведення вступне випробування проводиться на платформі дистанційного навчання «Сікорський».

Екзаменаційний білет складається з таких розділів:

а) шість питань з тем 1, 2 та 3;

б) варіативний блок: по чотири питання з тем 4, 5 та 6; вступнику необхідно відповісти на питання лише одного блоку на свій вибір;

в) відкрите завдання: вступнику надається на вибір по одному теоретичному питанню з тем 7, 8 та 9; вступнику необхідно відповісти на одне питання на свій вибір.

Кожне тестове питання оцінюється в 4 бали. Тестові питання можуть бути як з варіантами відповіді, так і з відкритими відповідями.

Відкрите завдання оцінюється у 60 балів за такими критеріями:

– «відмінно», повна відповідь, не менше 90% потрібної інформації – 55-60 балів;

– «добре», достатньо повна відповідь, не менше 75% потрібної інформації (допустимі окремі неточності) – 45-54 балів;

– «задовільно», неповна відповідь, не менше 60% потрібної інформації (відповідь містить певні недоліки) – 36-44 бали;

– «незадовільно», відповідь не відповідає умовам до «задовільно» – 0 балів.

3. Сума балів за відповіді на екзамені переводиться до екзаменаційної оцінки згідно з таблицею:

Бали	**Оцінка**
95…100	Відмінно
85…94	Дуже добре
75…84	Добре
65…74	Задовільно
60…64	Достатньо
Менше 60	Незадовільно

4. Сума балів за відповіді на екзамені переводиться до 200-бальної шкали згідно з таблицею:

Таблиця відповідності оцінок РСО (60…100 балів)
оцінкам 200-бальної шкали (100…200 балів)

шкала РСО	шкала 100…200	шкала РСО	шкала 100…200	шкала РСО	шкала 100…200	шкала РСО	шкала 100…200
60	100	70	140	80	160	90	180
61	105	71	142	81	162	91	182
62	110	72	144	82	164	92	184
63	115	73	146	83	166	93	186
64	120	74	148	84	168	94	188
65	125	75	150	85	170	95	190
66	128	76	152	86	172	96	192
67	131	77	154	87	174	97	194
68	134	78	156	88	176	98	196
69	137	79	158	89	178	99	198
						100	200

V. ПРИКЛАД ЕКЗАМЕНАЦІЙНОГО ЗАВДАННЯ

Форма № Н-5.05

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

(повне найменування вищого навчального закладу)

Освітній ступінь *доктор філософії*

Спеціальність 113 «Прикладна математика»
(назва)

Навчальна дисципліна *Вступний іспит*

ЕКЗАМЕНАЦІЙНИЙ БІЛЕТ № __1__

І. Тестова частина (обов'язкова)

Питання 1. Які властивості має бінарне відношення $x\rho y \Leftrightarrow y = |x|$, що визначено на множині дійсних чисел?

Варіанти відповіді:

А. Антисиметричне, транзитивне.
Б. Симетричне, транзитивне.
В. Рефлексивне, транзитивне.
Г. Рефлексивне.
Д. Еквівалентне.

Питання 2. Побудувати таблицю істинності для виразу $\forall y(P(y) \rightarrow \exists x Q(x))$ на області інтерпретації з двох елементів $\{a, b\}$.

Питання 3. Розглянемо матричну геометричну прогресію

$$E + A + A^2 + A^3 + \cdots + A^m + \cdots$$

Яке з трьох наведених тверджень є вірним?

Варіанти відповіді:

А. Для збіжності цього матричного ряду необхідно і достатньо, щоб усі елементи квадратної матриці A за модулем були менші одиниці;
Б. Для збіжності цього матричного ряду необхідно і достатньо, щоб усі власні значення матриці A за модулем були менші одиниці;
В. Для збіжності цього матричного ряду необхідно і достатньо, щоб усі елементи матриці A і всі власні значення були за модулем менші одиниці?

Питання 4. Яка із формул чисельного інтегрування серед перелічених забезпечує найбільш точний результат?

Варіанти відповіді:

А. Формула прямокутників
Б. Формула трапецій
В. Формула Сімпсона

Питання 5. Яке з трьох наведених тверджень є вірним?

Варіанти відповіді:

А. Зі збіжності послідовності випадкових величин з ймовірністю 1 випливає збіжність у середньому квадратичному;
Б. Зі збіжності послідовності випадкових величин з ймовірністю 1 випливає збіжність за ймовірністю;
В. Зі збіжності послідовності випадкових величин за ймовірністю випливає збіжність у середньому квадратичному ?

Питання 6. Знайдіть ймовірність появи принаймні двох шестірок при підкиданні 12 гральних кубиків.

II. Тестова частина (варіативна)
Вам необхідно відповісти на питання лише одного з блоків А, Б або В на ваш вибір. Відповіді на інші блоки не будуть враховані.

Обраний блок відповідей: ____ *(вписати літеру А, Б або В)*

Блок А.

Питання 7. Знайти AUC ROC, якщо відповідні результати класифікації представлені такою таблицею:

id	оцінка	клас
1	0.2	1
2	0.4	0
3	0.7	1
4	0.4	1
5	0.1	0
6	0.5	1
7	0.4	0

Питання 8. Якщо у Вас набір даних зашумлений, то який варіант необхідно обрати в методі KNN (*k*-найближчих сусідів)?

Варіанти відповіді:

А. Збільшити значення k;
Б. Зменшити значення k;
В. Не змінювати параметр k, бо така зміна ніяк не вплине на обробку шуму в даних.

Питання 9. Які значення може приймати ентропія Шеннона для ансамблю з n елементів?

Варіанти відповіді:

А. Від 0 до 1.
Б. Від 0 до $\log_2(n)$
В. Від 0 до n.
Г. Від 0 до 2^n.

Питання 10. Нехай дано такий набір даних:

x_1	x_2	x_3	y
1	1	1	+1
0	1	0	-1
1	0	1	-1
0	0	1	+1

Якщо по цьому набору даних будується дерево прийняття рішень, то який з вхідних атрибутів x_1, x_2 чи x_3 потрібно взяти для розщеплення в корені дерева?

Блок Б.

Питання 7. Для даного профілю переваг вибрати переможця за більшістю:

35	A→B→C
23	C→B→A
17	B→C→A
10	A→C→B
8	C→A→B
2	B→A→C

Варіанти відповіді:

А. A Б. B В. C Г. A, C Д. B, C

Питання 8. На множині альтернатив X задані два критерії: $f_1(x) = -247 - 545(x + 515)^2$ і $f_2(x) = -514 - 254(x + 191)^2$. Визначити множину Парето. У відповіді вказати відрізок на x, що є множиною Парето.

Варіанти відповіді:

А. Відрізок [-515, -191]. Б. Відрізок [-254, -545].
В. Відрізок [-514, -247]. Г. Відрізок [-51, -27].
Д. Відрізок [-515, -247].

Питання 9. Які з даних двійкових векторів домінуються вектором 0111?

Варіанти відповіді:

А. 1110 Б. 0110 В. 1010 Г. 1111

Питання 10. На множині A = {1, 2, 3, 4} задано відношення R = {(2, 2) , (2, 3) , (2, 4) , (3, 2) , (3, 3) , (3, 4)}. Побудувати відношення $R^2 \cap R^{-1}$

А. {(1, 2), (3, 2), (2, 3), (4, 3)}
Б. {(2, 2), (3, 2), (2, 3), (3, 3)}
В. {(4, 2), (3, 2), (4, 3), (3, 3)}
Г. {(3, 2), (2, 2), (3, 3), (4, 3)}

Блок В.

Питання 7. Які з наведених лишків є оборотними за модулем 36?

А. 3 Б. 4 В. 5 Г. 6

Питання 8. Задача факторизації натурального числа відноситься до класу

А. Поліноміальних задач (P)
Б. NP-проміжних задач (NP-intermediate, NPI)
В. NP-повних задач (NP-complete, NPC)
Г. Експоненційних задач (EXP).

Питання 9. Знайдіть усі генератори скінченного поля $GF(17)$.

Питання 10. Які з наведених булевих функцій є афінними?

А. $f(x, y) = x \,\&\, y$
Б. $f(x, y) = x \vee y$
В. $f(x, y) = x \oplus y$
Г. $f(x, y) = x \rightarrow y$

III. Відкрите завдання

Оберіть для відповіді одне з питань а), б) або в).
Обране вами питання повинно бути максимально повно розкрите.

а) Математичні моделі динамічних процесів із зосередженими параметрами. Дискретні та неперервні процеси. Адекватність моделей.

б) Мережі Петрі, графічне та аналітичне зображення, основні задачі та характеристики.

в) Асиметричні системи шифрування. Загальна концепція асиметричних криптосистем шифрування з відкритими ключами. Системи шифрування Мессі-Омури, Ель-Гамаля, RSA, Рабіна. Побудова асиметричних шифросистем, алгоритми зашифрування та розшифрування.

Затверджено:
Гарант освітньої програми _____ Наталія КУССУЛЬ

Київ 2024

РОЗРОБНИКИ ПРОГРАМИ:

Куссуль Наталія Миколаївна,
доктор техн. наук, проф.,
завідувач кафедрою математичного моделювання
та аналізу даних НН ФТІ

Чертов Олег Романович,
доктор техн. наук, проф.,
завідувач кафедрою прикладної математики ФПМ

Маслянко Павло Павлович,
кандидат техн. наук, с.н.с.,
доцент кафедри прикладної математики ФПМ

Савчук Михайло Миколайович,
член-кор. НАН України, доктор фіз.-мат. наук,
професор кафедри математичних методів
захисту інформації НН ФТІ

Яковлєв Сергій Володимирович,
кандидат техн. наук,
в.о. завідувача кафедрою математичних методів
захисту інформації НН ФТІ