РЕЦЕНЗІЯ

на дисертаційну роботу **Гуріна Артема Леонідовича** **«Комбінаторні методи розв'язання задач про математичний сейф на графах та матрицях»**, подану на здобуття наукового ступеня доктора філософії **за спеціальністю 113 Прикладна математика**, доктора технічних наук **Гуляницького Леоніда Федоровича**

1. **Актуальність обраної теми дисертації.**

В останні роки стрімко розширюється сфера застосування інформаційних технологій, зростає їх роль у розвитку суспільства. Цим визначається актуальність розробки нових математичних моделей та методів, які можуть бути основою для побудови і функціонування комп'ютерних технологій оптимізації рішень у різних сферах застосувань – цим питанням і присвячено роботу, що розглядається.

Серед прикладних проблем одне з чільних місць займають проблеми вибору оптимальних рішень в дискретних просторах, чим обумовлюються потреби в дослідженні та впровадженні моделей і методів комбінаторної оптимізації.

У дисертаційній роботі досліджуються і розробляються комбінаторні методи оптимізації на прикладі розв'язування комбінаторних задач про математичний сейф, які мають перспективу застосування в теорії кодування, теорії захисту інформації та інших наукових галузях і які можна класифікувати як позиційні ігри на графах та матрицях. Незважаючи на відомі результати в деяких наукових публікаціях, системна побудова методології та обґрунтування методів розв'язання задач про математичний сейф на графах та матрицях є важливим напрямком досліджень сучасної комбінаторної оптимізації, що і робить актуальною тему дисертаційної роботи.

В рамках виконання досліджень за темою розроблено методологію розв'язування задачі про математичний сейф, яка базується на створеному математичному апараті і призначена для застосування в різних сферах використання методів математичного моделювання.

2. **Зв'язок роботи з науковими програмами, планами, темами.**

Основні наукові дослідження за тематикою дисертації проводилися у відділі економічної кібернетики Інституту кібернетики імені В.М. Глушкова НАН України у рамках виконанням науково-дослідних робіт:

ВФ 110.15 «Розробити методи та алгоритми розв'язання оптимізаційних задач на комбінаторних конфігураціях і траєкторіях динамічних систем» (державний реєстраційний номер 0117U000473, протокол приймання та оцінки наукової роботи № 15 від 02.11.2021, термін виконання 01.01.17–31.12.21);

ВФ 110.18 «Побудова гарантованих керувань динаміки систем при різних інформаційних припущеннях» (державний реєстраційний номер 012U000663, протокол затвердження №1 від 08.07.2021, термін виконання 01.01.22–31.12.26);

3. Наукова новизна одержаних результатів.

У дисертаційній роботі проведено актуальні дослідження та прикладний аналіз комбінаторних методів розв'язування специфічного класу задач позиційних ігор на графах та матрицях – задачі про математичний сейф. Системність та глибина проведених досліджень, одночасно з розробкою та обґрунтуванням нових універсальних методів та алгоритмів пошуку розв'язку таких задач дозволило досягти мети дисертаційної роботи – побудови цілісної методології розв'язування досліджуваної задачі про математичний сейф. Наукову новизну в цій роботі мають такі теоретичні та практичні результати:

– вперше доведено необхідні та достатні умови, за яких початкові стани замків сейфа гарантують існування розв'язку задачі про математичний сейф на графах;

– вперше подано та обґрунтовано метод сумарних представлень розв'язків задачі про математичний сейф на графах та параметричний метод, які застосовуються для графів у полі лишків за модулем простого числа;

– вперше розроблено та застосовано метод формування підсистем розв'язування задачі про математичний сейф на матрицях, який дозволяє за скінчену кількість кроків отримати розв'язок задачі з одним та двома типами замків у полях лишків за модулем простого числа;

– вперше запропоновано метод сумарних представлень для розв'язання задачі про математичний сейф на матрицях, який зводиться до розв'язання системи лінійних порівнянь у полі лишків за модулем простого числа;

– вперше комплексно проаналізовано арифметичну складність алгоритмів існуючих методів розв'язання задачі про математичний сейф на матрицях у полі лишків за модулем простого числа.

4. Практичне значення отриманих результатів.

Запропоновані в дисертації комбінаторні методи розв'язування задач про математичний сейф на графах та матрицях мають практичне значення, що дозволить їх застосовувати для побудови моделей та знаходження розв'язків багатьох практичних задач, які зводяться до позиційних ігор подібного класу і можуть бути використані для розв'язування задач теорії прийняття рішень, теорії кодування та захисту інформації. В дисертації розглянуто приклади застосування алгоритмів розв'язування задачі про математичний сейф на графах у теорії кодування та захисту інформації. Також наведені приклади кодування повідомлень у месенджерах та захисту ліцензійного програмного забезпечення на базі системи шифрування Віжінера.

5. Ступінь обґрунтованості основних положень та висновків дисертації.

Основні наукові положення, висновки, рекомендації дисертаційної роботи мають належне теоретичне, методологічне та практичне обґрунтування. Обґрунтованість положень дисертації базується на системному дослідженні здобувачем багатьох відомих вітчизняних та зарубіжних джерел, які відповідають темі дисертації.

Дисертаційна робота Гуріна А.Л. має чітку концептуальну мету, яка включає комплексне дослідження та розробку методів розв'язування задачі про математичний сейф, що дозволяє створити цілісну методологію розв'язання зазначеного типу задач. Основні наукові положення та висновки дисертації базуються на власних твердженнях та розрахунках автора, логічно витікають із матеріалів дисертації та утворюють завершене дослідження. Структура дисертаційного дослідження логічна, послідовна і у повному обсязі розкриває задекларовану тему.

6. Повнота викладення наукових положень та висновків в опублікованих працях.

Основні положення та результати дисертаційної роботи опубліковано у 7 наукових працях у виданнях, що входять до міжнародних наукометричних баз даних (5 з них – у СКОПУСі) і фахових наукових виданнях, а також у матеріалах 3 міжнародних та національних конференцій. Дві наукові публікації здобувач написав особисто, а в 5 опублікованих у співавторстві внесок автора по питанням, висвітленим в дисертації, є або вагомим, або переважаючим.

Основні наукові положення та висновки сформульовані відповідно до поставлених завдань дисертаційної роботи.

7. Недоліки дисертації щодо її змісту і оформлення.

Автору не вдалося уникнути певних недоліків у роботі, серед яких відмітимо такі:

1. Спостерігається нечітке чи неточне вживання математичних термінів і понять, перш за все, задач комбінаторної чи дискретної оптимізації та їх змішування із задачами комбінаторики. Не завжди правильно вживаються поняття "розв'язок", "розв'язування" та "рішення" (solution-solving-decision making). До прикладу, задачі розв'язуються, а проблеми вирішуються.

2. Є неув'язка із викладом історії досліджень задачі про сейф: на с.23 та 33 їх початок віднесено до XX століття, починаючи з роботи (Пшеничный 1980), а на с.16 читаємо, що постановка задачі вперше представлена у (Донец 2002a).

3. Параметричний метод розв'язування у розд.3 подається на прикладах, а його більш формалізований виклад наведено тільки у висновках ло розділу.

4. Занадто велика роль відведена детальним описам прикладів, а важливі результати (напр., про обчислювальну складність алгоритмів) часто подаються ледь не як зауваження, що ускладнює розуміння суті власних результатів автора.

5. Некоректними є висловлювання на кшталт, що якийсь висновок доводиться наведенням прикладів (с. 73, 91, 92, 127, 134, 136). Навряд чи подібне дозволяє стверджувати, наприклад, таке: "Результати розв'язку усіх 3 прикладів довели ефективність і універсальність запропонованих методів розв'язання задач про математичних сейф на графах..." (с.92).

6. Помилковими чи тавтологічними є ряд висловлювань, наприклад: "... можливість представлення множини позицій у вигляді деревоподібної *впорядкованої множини*" – і тут же "Дерево гри – *це граф*" (до того ж, тут мова йде про орграф, тому маємо не ребра, а дуги, с.24); "задача на перестановках *об'єктів* (???) у структурі графу" (с.26); "...питання комбінаторних методів *розв'язання* позиційних *ігор*" (с.29); "методи логіки та мінімізації, що можуть застосовувати методи логіки та мінімізації" (с.29); "безліч рішень" (це множина розв'язків) (с.70).

7. Висновки часто подаються як перелік зробленого, а не як власне висновки: що ж це дає. Часто також в них зустрічаються "розглянуто" чи "розроблено та *представлено*".

8. В анотації вказано, що видатні науковці вже розглянули всі аспекти класифікації та методології розв'язування задачі про математичний сейф, що викликає певні запитання щодо новизни огляду робіт у дисертації. До того ж, у списку літератури слабко представлено зарубіжні роботи останнього десятиліття, їх всього 2.

9. На с.30 у перелік конкретних методів комбінаторної оптимізації включено і "евристика та метаевристика", хоча це не окремі алгоритми, а їх класи. Далі робиться не зрозуміла диференціація між метаевристиками та метаевристичними методами – це є синоніми. Більше того, неправильним є твердження, що "метаевристики ґрунтуються на інтуїції та досвіді" (як сказано тут же), вони утворюють великий і перспективний клас алгоритмів комбінаторної оптимізації з ієрархічною структурою (Сергиенко, Гуляницкий, и Сиренко 2009). Алгоритм Particle Swarm Optimization (PSO) перекладається як оптимізація *роєм* частинок (ОРЧ).

10. На с. 130 пропущені умови у першому рядку, змінна G є зайвою, а змінні y_i не описані.

11. Потребують більш наближеного до математики формулювання вирази: *запишемо* у множину, *складемо* множину (с.67); *сутність* методу полягає у *позначенні змінних*, що відповідають деяким вершинам графу *певними параметрами* (с.83); останні k вершин *об'єднуємо* в систему рівнянь, підставляючи ці значення в *значення* кожної *вершини* (с.91); дається *довершене теоретичне* обґрунтування цього методу (с.93); розв'язок *правильний* (с.102); у загальному випадку, k-е асоціативне комутативне кільце k-го порядку *будується в один рядок* (с.130).

12. На жаль, у роботі наявні синтаксичні та орфографічні помилки, хоча вони не заважають уяснювати сутність викладеного у дисертації.

8. Рекомендації щодо впровадження результатів дисертаційного дослідження в практику.

Результати дослідження можна рекомендувати для розробки, вдосконалення та перевірки спеціалізованих програмних систем кіберзахисту як у приватних компаніях, так і у державних установах.

Значна частина результатів дисертації може бути використана у навчальному процесі вищих навчальних закладів України для студентів ІТ-спеціальностей, де викладаються такі дисципліни як «Проектування та аналіз алгоритмів», «Дискретна математика» та «Прикладна математика».

9. Висновок на відповідність дисертації встановленим вимогам.

Дисертаційна робота Гуріна А.Л. на тему: «Комбінаторні методи розв'язання задач про математичний сейф на графах та матрицях» на здобуття наукового ступеня доктора філософії заспеціальністю 113 «Прикладна математика», є теоретичним узагальненням і завершеним вирішенням наукової проблеми – побудови цілісної методології розв'язання задачі про математичний сейф на графах та матрицях, яка супроводжувалась як комплексним аналізом існуючих методів, так і створенням нових. Ефективність запропонованих методів та алгоритмів перевірялась як аналітичним розрахунками, так і на характеристичних прикладах. Отримані наукові результати в розвитку методології розв'язання комбінаторних задач про математичний сейф сприятимуть все більш широкому їх застосуванню при моделюванні та розв'язуванні прикладних задач.

Зважаючи на вищесказане, дисертація Гуріна А.Л. за актуальністю, обсягом і рівнем проведених досліджень, науковою новизною і практичною значимістю відповідає вимогам «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого постановою Кабінету Міністрів України №44 від 12 січня 2022 року, а її автор заслуговує присудження ступеня доктора філософії за спеціальністю 113 «Прикладна математика».

Завідувач відділу методів комбінаторної оптимізації та інтелектуальних інформаційних технологій Інституту кібернетики ім.В.М.Глушкова НАН України, член-кореспондент НАН України, доктор технічних наук, старший науковий співробітник _____ Леонід ГУЛЯНИЦЬКИЙ

(підпис)

Інститут кібернетики імені В.М.Глушкова Національної Академії наук України * Ідентифікаційний код 05417178 * м.Київ *
ДЛЯ ДОВІДОК

Підпис Л. Гуляницького
ЗАСВІДЧУЮ
Зав. канц. _____
ІК НАН України 25.10.2023