ВИСНОВОК
про наукову новизну, теоретичне та практичне значення результатів дисертації Цирканюк Діани Андріївни
на тему «Методи та моделі оптимізації розподілу обчислювальних ресурсів хмарних систем для підвищення безпеки»,
поданої на здобуття ступеня доктора філософії
з галузі знань 12 Інформаційні технології
за спеціальністю 125 Кібербезпека

Актуальність теми дослідження.

Протягом останніх десятиліть відбулися значні зміни обчислювальних парадигм. Хмарні обчислення (ХО) віддзеркалили найбільш помітні з цих змін. Завдяки розгортанню хмарних технологій, хмарні центри обробки даних сьогодні керують аналізом, зберіганням даних та прийняттям рішень в більшості бізнес-процесів. ХО, які надали користувачам масштабовані ресурси за моделями IaaS, PaaS та SaaS, заклали фундамент розгортання важливих для бізнесу хмарних сервісів, проте їхня багатокористувацька природа та розподілена архітектура створили нові вектори кіберзагроз. В умовах зростання інтенсивності атак, зокрема розподілена відмова в обслуговуванні 'Distributed Denial of Service' (DDoS), економічне заперечення сталого розвитку 'Economic Denial of Sustainability' (EDoS) та цілеспрямованих вторгнень (APT), наявні методи, моделі та інформаційні технології (ІТ) в завданнях управління ресурсами хмарних систем (ХМС), виявилися недостатньо ефективними. Що більше, світова статистика інцидентів засвідчила, що фінансові та репутаційні втрати від простою ХМС зросли експоненційно, перетворив завдання управління ресурсами з суто технічної на вирішальну умову виживання бізнесу. Зокрема, за даними звітів 2023–2024 рр., понад 60–80 % організацій зафіксували інциденти інформаційної безпеки (ІБ), пов'язані з ХО, серед причин яких, домінували неправильні конфігурації та помилки в управлінні доступом (IAM). Звідсіля виникла об'єктивна суперечність між необхідністю забезпечення високої якості обслуговування (QoS) та вимогою гарантування надійності й конфіденційності даних в ХМС. Це, відповідно, потребує синтезу нових, гнучких та ефективних методів розподілу обчислювальних потужностей із вбудованими механізмами безпеки ХМС. Дослідження в напрямі підвищення ефективності та захищеності ХМС активно ведуться вже декілька десятиріч.

Вагомий внесок у розбудову теоретичних та практичних засад ХО, а також методів розподілу ресурсів ХМС зробили численні закордонні вчені. Зокрема, фундаментальні питання класифікації моделей розподілу ресурсів ХМС, забезпечення енергоефективності та масштабованості висвітлено у роботах Saidi K., Hioual O., Siam A., Senthilkumar G., Tamilarasi K., Velmurugan N. та Periasamy J. K. Проблематику планування задач та автономного управління навантаженням досліджували Rabaaoui S., Hachicha H., Zagrouba E., Jabber S. A., Hashem S. H. та Jafer S. H., закцентував переважно увагу на економічних метриках та QoS. Систематизації стратегій алокації ресурсів та

аналізу програмно-конфігурованих мереж присвячені роботи Kareem Awad W., Mohamed A., Vergara J., Botero J. та Fletscher L. Окремий пласт досліджень, спрямований на використання методів штучного інтелекту в завдання прогнозування навантаження та управління ХМС, представлено у доробку Lekkala C., Ashawa M. та Manzoor M. F. Завдання багатозмінного управління та оптимізації SLA розглядали Gong S., Madni S. H. H., Li C. та Li L. Y., які сформували базис для розуміння економічної ефективності ХМС. Специфіку забезпечення безпеки у ХМС та інтеграцію захисних механізмів у процеси управління ресурсами досліджували такі науковці, як Parast F. K., Sindhav C., Saxena D., Singh A. K., Han J., Zang W. та Liu L. Значний вплив на розвиток теоретико-ігрових підходів до кібербезпеки та моделювання взаємодії «атакуючий–порушник» мають роботи Wilczyński A., Jebalia M., Xu X., Yu H., Ait Temghart A., а також концептуальні розробки архітектури самозахисту (SECURE) авторства Gill S. S. та Buyya R. Різні аспекти контейнерної безпеки та захисту даних аналізували Jarkas O., Feng D., Aldhyani T. H. та Alkahtani H. Серед вітчизняних науковців, які зробили суттєвий внесок у розв'язання задач оптимізації ресурсів та захисту інформації в комп'ютерних системах, зокрема ХМС, відзначимо Дорогого Я. Ю., який розглядав розподіл ресурсів критичної інфраструктури, та Волка М. О., Курочкіна В. С. і Запорожченка А. П., які запропонували гібридні методи управління ХМС. Питаннями первинного виділення ресурсів та застосуванням методу аналізу ієрархій займалися Гребенюк Д. С. та Давидов В. В. Також серед українських науковців вагоме місце займають праці Петровської І. Ю., Кучука Г. А., Панченка В. І. та Філоненко А. М., присвячені методам розподілу ресурсів при наданні хмарних послуг та забезпеченню збалансованості навантаження ХМС. Проблематика кібербезпеки хмарних обчислень, аналіз загроз та розробка засобів захисту знайшли відображення у роботах Ковалюк О. А., Лучика С. Д., Шевченка В. В., Бобренка В. В. та Гуди А. І. Критерії вибору та оцінювання якості хмарних сервісів досліджували Закаляк Р. Ф., Андрощук О., Голобородько М., Кондратенко Ю. та Литовченко Г. Окремі аспекти захисту інформації, застосування ігрових моделей та стохастичного моделювання ризиків розглядалися у працях Михайліва В. І., Кобевка А. Т., Тимченка О. В., Шабали Є., Корнійчука Б., Стефурака О. Р., Тихонова Ю. О., Лаптєва О. А., Зозулі С. А., Павлова І. М. та Толюпи С. В.

Попри значний обсяг наукових напрацювань, більшість релевантних підходів розглядають питання продуктивності ХМС та безпеки ізольовано або застосовують статичні моделі ризиків, що не дозволяє ефективно протидіяти варіативним загрозам ХМС. Відсутність комплексної моделі, яка б поєднувала багатокритеріальну оптимізацію, гнучку оцінку ризиків та апарат кооперативної взаємодії захисників, обумовила потребу проведення даного дослідження та підтвердило його актуальність для подальшого розвитку технологій захисту ХМС.

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

Напрям дисертаційного дослідження безпосередньо пов'язаний з реалізацією доктрини інформаційної безпеки України, Стратегії інформаційної безпеки та Стратегії кібербезпеки України. Дисертаційна робота виконана відповідно до планів наукової і науково-технічної діяльності Київського столичного університету імені Бориса Грінченка в рамках науково-дослідної роботи: «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (№0122U200483, КСУБГ, м. Київ).

Мета дисертаційного дослідження полягає в підвищенні ефективності та безпеки функціонування хмарних систем шляхом розробки методу кооперативно-еволюційного розподілу обчислювальних ресурсів.

У відповідності до поставленої мети для вирішення наукового завдання в роботі визначено та розв'язано такі *часткові* ***завдання***:

– проаналізувати попередні дослідження з проблематики дисертації, методи та моделі управління ресурсами в хмарних системах, виявити їхні обмеження щодо врахування варіативних ризиків безпеки та обґрунтувати необхідність розробки нового методу розподілу ресурсів ХМС;

– розробити багатокритеріальну оптимізаційну модель розподілу ресурсів ХМС яка дозволить знаходити множину Парето-оптимальних рішень;

– удосконалити теоретико-ігрову модель взаємодії «порушник-захисник» в ХМС;

– розробити метод кооперативно-еволюційного розподілу обчислювальних ресурсів, який поєднає інструментарій еволюційної оптимізації (NSGA-II / NSGA-III) з апаратом кооперативних ігор для формування узгоджених стратегій захисту та отримання синергетичного ефекту у вигляді коаліційної вигоди від взаємодії захисників;

– експериментально дослідити ефективність запропонованого методу шляхом імітаційного моделювання, оцінити якість отриманих рішень за метриками Hypervolume (HV), зворотна генераційна відстань 'Inverted Generational Distance' (IGD), Spacing та розробити рекомендації щодо його практичного впровадження в платформи оркестрації ХМС.

Об'єктом дослідження є процеси розподілу обчислювальних ресурсів у хмарних системах.

Предметом дослідження є методи та моделі оптимізації розподілу ресурсів хмарних систем з урахуванням критеріїв безпеки, продуктивності, вартості та коаліційної взаємодії захисників.

Методи дослідження.

Теоретико-методологічну основу дисертаційної роботи склав системний підхід, який поєднав методи системного аналізу, математичного моделювання та штучного інтелекту. Для розв'язання поставлених завдань використано: методи системного аналізу та узагальнення – для дослідження специфіки

архітектурних моделей хмарних систем (IaaS, PaaS, SaaS тощо), систематизації існуючих методів та моделей в завданні управління ресурсами ХМС та виявлення їхніх обмежень щодо врахування релевантних кіберзагроз; апарат теорії ігор, зокрема, антагоністичні та кооперативні ігри – для формалізації конфліктної взаємодії між підсистемою захисту та порушником політики інформаційної безпеки, а також для моделювання коаліційної співпраці захисників із використанням вектору Шеплі для розподілу вигоди; методи теорії ймовірностей та стохастичного моделювання – для математичного опису параметра агресивності атак $\lambda(t)$ та розрахунку функції ризику для вузлів ХМС; методи багатокритеріальної оптимізації та еволюційні алгоритми – для синтезу методу CoopEvo-CloudSec, зокрема, алгоритми NSGA-II та NSGA-III, застосовано для пошуку множини Парето-оптимальних рішень у просторі чотирьох критеріїв – безпека, продуктивність, вартість, коаліційна вигода; методи імітаційного моделювання та методи математичної статистики – для проведення обчислювальних експериментів, оцінювання якості отриманих рішень за метриками HV, IGD, Spacing та підтвердження статистичної значущості переваг розробленого методу CoopEvo-CloudSec порівняно з чинними аналогами.

Наукова новизна одержаних результатів полягає в подальшому розвитку теоретичних і практичних методів та методів оптимізації розподілу обчислювальних ресурсів хмарних систем для підвищення безпеки:

1. Вперше запропонований та математично обґрунтований метод кооперативно-еволюційного розподілу обчислювальних ресурсів (CoopEvo-CloudSec) у хмарних системах з урахуванням ризиків для їхньої безпеки, та якій вирізняється від наявних, інтеграцією критерію коаліційної взаємодії захисників безпосередньо у еволюційний процес пошуку рішень на базі алгоритмів багатокритеріальної оптимізації NSGA-II/NSGA-III, залежно від часових обмежень, що дозволяє сформувати узгоджені стратегії захисту та відповідну проводити реконфігурацію ресурсів ХМС.

2. Вперше запропонована багатокритеріальна оптимізаційна модель розподілу ресурсів ХМС, яка, на відміну від відомих, враховує чотири суперечливі критерії – ризик, продуктивність, вартість та, вперше, коаліційну вигоду від взаємодії захисників, що дозволило математично формалізувати задачу пошуку множини Парето-оптимальних рішень в умовах мультиагентної протидії кіберзагрозам.

3. Вдосконалена теоретико-ігрова модель конфліктної взаємодії «атакуючий-захисник», яка, на відміну від чинних, містить параметр агресивності $\lambda(t)$, який описує варіативність інтенсивності атак у часі, що дозволило врахувати стохастичну або еволюційну природу ризику та застосувати механізм розрахунку виграшу коаліції на основі вектора Шеплі для формування узгоджених стратегій захисту ХМС.

Практичне значення одержаних результатів полягає у розробці та програмній реалізації на мові програмування Python (IDE PyCharm) з використанням бібліотек Pymoo методу CoopEvo-CloudSec та відповідного програмного комплексу, який дозволяє підвищити стійкість хмарних систем (ХМС) до релевантних кіберзагроз без втрати продуктивності системи. Розроблений програмний модуль CoopEvo-CloudSec Engine на відміну від стандартних планувальників, дозволяє знаходити компромісні рішення між безпекою, вартістю та часом виконання завдань в ХМС. Експериментально підтверджено, що використання модифікованого алгоритму на базі алгоритму NSGA-II) дозволяє покращити якість фронту Парето за показником HV на 25,2% порівняно з базовим алгоритмом NSGA-II (значення 1,11 проти 0,89). Це забезпечує адміністраторам ХМС ширший та якісніший вибір стратегій захисту. Доведено експериментально зростання різноманітності рішень (метрика Diversity) до рівня 1,23 (проти 0,268 у базових методах), що дає можливість обрати оптимальні конфігурації підсистеми захисту ХМС. Розроблено архітектурну схему інтеграції методу CoopEvo-CloudSec, включаючи модулі Risk Analyzer та Policy Adapter, яка сумісна з платформами Kubernetes та OpenStack, що дозволило під час впровадження (акти впровадження наведено в Додатках В і Г) використати розроблений метод CoopEvo-CloudSec як алгоритмічно-програмну надбудову над наявними оркестраторами без необхідності зміни їх ядра, забезпечив підтримку прийняття рішень на основі даних телеметрії SIEM/EDR систем.

Апробація результатів дисертації.

Основні теоретичні та практичні результати були представлені та обговорені в ході ряду наукових конференцій:

1. Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS), 2023.
2. 14-ї Всеукраїнської науково-практичної конференції «Актуальні проблеми управління інформаційною безпекою держави», 2023.

Публікації.

Основні результати дисертації висвітлено у 7 наукових публікаціях, із них 4 – одноосібні, 3 – у співавторстві: 5 статей (з них 1 у співавторстві) у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України; 2 публікації (з них усі у співавторстві), у яких додатково висвітлено результати дисертації. Наукові результати дисертації повною мірою висвітлено у наукових публікаціях.

Особистий внесок здобувача.

Дисертація є самостійною науковою працею, в якій висвітлено власні ідеї і розробки автора, що дозволили вирішити поставлені завдання. Робота містить теоретичні та методичні положення і висновки, сформульовані здобувачем особисто. Використані в дисертації ідеї, положення чи гіпотези інших авторів мають відповідні посилання і використані лише для

підкріплення ідей здобувача. Безпосередньо автором розроблено новий метод (CoopEvo-CloudSec) кооперативно-еволюційного розподілу ОбР у ХМС з урахуванням безпекового ризику, багатокритеріальну оптимізаційну модель розподілу ресурсів ХМС, удосконалену теоретико-ігрову модель конфліктної взаємодії «атакуючий–захисник», програмні модулі та архітектурну схему інтеграції методу CoopEvo-CloudSec, включаючи модулі Risk Analyzer та Policy Adapter.

Наукові статті, опубліковані у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України:

1. **Цирканюк, Д.**, & Соколов, В. (2024). Методика розслідування інцидентів інформаційної безпеки. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(26)*, 140–154. https://doi.org/10.28925/2663-4023.2024.26.675

2. **Цирканюк, Д.** (2025). Модель розподілу обчислювальних задач у хмарній інфраструктурі з урахуванням продуктивності, вартості та безпеки. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(28)*, 619–632. https://doi.org/10.28925/2663-4023.2025.28.836

3. **Цирканюк, Д.** (2025). Розширена гібридна модель з урахуванням ризиків та кооперативних стратегій захисту хмарного середовища. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(29)*, 909–929. https://doi.org/10.28925/2663-4023.2025.29.970

4. **Цирканюк, Д.** (2025). Метод багатокритеріальної оптимізації безпеки хмарних обчислень на основі модифікованого алгоритму NSGA-II. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(30)*, 692–714. https://doi.org/10.28925/2663-4023.2025.30.983

5. **Цирканюк, Д.** (2025). Метод CoopEvo-CloudSe для оптимізації обчислювальних ресурсів хмарних систем для підвищення безпеки. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(31)*, 872–887. https://doi.org/10.28925/2663-4023.2025.31.1077

Наукові публікації, у яких додатково висвітлено результати дисертації:

1. Shevchenko, S., Zhdanova, Y., Dreis, Y., Kyrychok, R., & **Tsyrkaniuk, D.** (2023). Protection of Information in Telecommunication Medical Systems based on a Risk-Oriented Approach. In *Cybersecurity Providing in Information and Telecommunication Systems* (Vol. 3421, pp. 158–167). (Scopus).

2. Гулак Г. М., Скітер І. С., Гулак Є. Г., & **Цирканюк Д. А.** (2023). Базові засади побудови центру кібербезпеки об'єктів ядерної енергетики. In *14-а Всеукраїнська науково-практична конференція «Актуальні проблеми управління інформаційною безпекою держави»* (pp. 262–266).

Структура та обсяг дисертації.

Дисертація складається зі вступу, трьох розділів, висновків, списку використаних джерел із 156 найменування на 18 сторінках і4 додатків. Загальний обсяг роботи становить 242 сторінки серед яких 149 сторінок основного тексту, 22 рисунків і 31 таблиця.

Оцінка мови та стилю дисертації.

Дисертація написана науковою українською мовою. Стиль викладу матеріалу логічний і послідовний. Зміст роботи повністю висвітлює результати наукових досліджень. Текст роботи має смислову цілісність, послідовність і завершеність, що забезпечує легкість і доступність сприйняття матеріалу.

Дотримання здобувачем академічної доброчесності в дисертації та наукових публікаціях, в яких висвітлено наукові результати дисертації.

На підставі вивченого тексту дисертації і наукових публікацій, результатів автоматизованої перевірки на плагіат та їх експертної оцінки, встановлено, що дисертація і наукові публікації виконані самостійно, не містять академічного плагіату, фальсифікації, фабрикації.

Відповідність дисертації вимогам, що представляються до дисертацій на здобуття ступеня доктор філософії.

Дисертація Цирканюк Діани Андріївни на тему «Методи та моделі оптимізації розподілу обчислювальних ресурсів хмарних систем для підвищення безпеки» є завершеним науковим дослідженням, в якому отримано нові обґрунтовані результати. Дисертацію виконано на достатньо високому рівні, її результати мають наукову новизну і практичну значимість. Основні положення дисертації опубліковані в наукових фахових виданнях і міжнародних виданнях, що входять до наукометричних баз Scopus та Web of Science Core Collection та оприлюднювались на міжнародних науково-практичних конференціях. Дисертаційне дослідження відповідає обраній темі, розкриває її суть та підтверджує, що автором повністю вирішено поставлені у роботі завдання.

Рішення:

1. Дисертація Цирканюк Д.А., на тему «Методи та моделі оптимізації розподілу обчислювальних ресурсів хмарних систем для підвищення безпеки», подана на здобуття ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека, є завершеною, самостійною роботою, що містить науково обґрунтовані результати, актуальність, наукову новизну, теоретичне та практичне значення і відповідає пп. 6–9 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 від 12.01.2022 №44 (зі змінами),

наказу Міністерства освіти і науки України від 12.01.2017 №40 «Про затвердження Вимог до оформлення дисертації», затвердженого Міністерством юстиції України 03.02.2017 за №155/30023.

2. Дисертація Цирканюк Діани Андріївни та наукові публікації, у яких висвітлено наукові результати дисертації, виконано на належному науковому рівні з дотриманням академічної доброчесності.

3. Цирканюк Діана Андріївна на високому рівні оволоділа методологією наукової діяльності, набула теоретичних знань, відповідних умінь, навичок та компетентностей. Здобувач вільно володіє матеріалом.

4. Рекомендувати дисертацію Цирканюк Д.А., на тему «Методи та моделі оптимізації розподілу обчислювальних ресурсів хмарних систем для підвищення безпеки» до публічного захисту у разовій спеціалізованій вченій раді для присудження Цирканюк Д.А. ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека.

Голова –
кандидат технічних наук, доцент
завідуючий кафедри інформаційної
та кібернетичної безпеки
імені професора Володимира Бурячка
Київського столичного університету
імені Бориса Грінченка Павло СКЛАДАННИЙ

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА Код ЄДРПОУ 45307955 ВЛАСНИЙ ПІДПИС Складанного П. ПОСВІДЧУЮ Провід. фах. В.К. Л. Мамітько