Голові разової спеціалізованої вченої ради Національного університету «Київський авіаційний інститут»

д.т.н., проф. Одарченку Роману Сергійовичу
пр. Любомира Гузара 1, м. Київ, 03058, Україна

ВІДГУК
ОФІЦІЙНОГО ОПОНЕНТА
доцента кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка
кандидата технічних наук
Мирутенко Лариси Вікторівни
на дисертаційну роботу Юдіної Діани Олексіївни
на тему «Методи та моделі оцінювання стану кіберзахисту об'єктів критичної інформаційної інфраструктури»,
представлену на здобуття наукового ступеня доктора філософії
за спеціальністю 122 – Комп'ютерні науки
галузі знань 12 – Інформаційні технології

1. Актуальність та мета дослідження

Стрімка еволюція загрозового середовища та кіберфізична природа сучасних об'єктів критичної інформаційної інфраструктури (ОКІІ) вимагають відходу від разових аудитів до побудови алгоритмізованих систем безперервної оцінки кіберстійкості. У сучасних умовах ведення мережево-центричної війни та систематичного застосування складних цілеспрямованих атак (APT) традиційні прескриптивні методики не спроможні адекватно оцінювати динаміку безпекового стану кіберфізичних систем, які поєднують IT-сегменти з промисловими контролерами (ICS/SCADA).

Прийняття новітнього законодавчого масиву в Україні (Закон № 4336-IX від 27.03.2025 р., Постанова КМУ № 1799 від 31.12.2025 р.) закріпило обов'язковість систематичного контролю за станом кіберзахисту. Проте з точки зору комп'ютерних наук ключовою нерозв'язаною проблемою залишається відсутність алгоритмічного апарату. Існуючі комплаєнс-моделі є

суто дескриптивними та позбавленими математично обґрунтованої здатності опрацьовувати невизначеність експертних даних.

У цьому контексті дисертаційне дослідження Юдіної Д.О., спрямоване на математичне формалізування процесу обчислення рівня кіберзахисту ОКІ шляхом створення гібридних декомпозиційних моделей, застосування багатокритеріального аналізу та нечіткої фазифікації, є надзвичайно ***актуальним завданням спеціальності 122 «Комп'ютерні науки»***.

Метою дослідження є удосконалення процесу управління кіберзахистом ОКІІ, що полягає в досягненні високої точності та оперативності оцінювання показників кіберзахисту на основі розробленого комплексу моделей і методів.

2. Ступінь обґрунтованості наукових положень та результатів, їх достовірності та новизни

Наукові положення, сформульовані у дисертаційній роботі, є обґрунтованими. Достовірність здобутих результатів базується на системній строгості математичних виведень, коректному застосуванні теорії графів, теорії множин, методу аналізу ієрархій (MAI) Т. Сааті та апарату трапецієподібних нечітких чисел LR-типу. Теоретичні моделі підтверджені обчислювальними експериментами за участю експертної групи, а також впровадженнями у профільних державних установах та свідоцтвом про реєстрацію авторського права на твір № 145206.

Наукова новизна результатів дослідження:

Вперше:

- розроблено гібридну ієрархічну модель системи показників кіберзахисту ОКІІ, яка, на відміну від існуючих, базується на ієрархічній декомпозиції семи функціональних систем критеріїв (шість з яких гармонізовано з міжнародним фреймворком NIST CSF 2.0, а сьома – «Секторальна складова»), що дозволило вперше в межах єдиного оціночного циклу врахувати специфічні вимоги 24 галузей критичної інфраструктури України;

- обґрунтовано метод багатокритеріального оцінювання стану кіберзахисту, який відрізняється від відомих інтеграцією процедури перевірки нормативної відповідності з механізмом попарних порівнянь для пріоритизації захисних заходів, що забезпечило можливість формалізувати неоднаковий вплив різних систем захисту на інтегральний рівень безпеки об'єкта.

Удосконалено:

- математичну модель нечіткої інтерпретації стану кіберзахисту, яка, на відміну від традиційних підходів, використовує нечіткі числа LR-типу трапецієподібної форми та розрахунок індексу впевненості, що дало змогу підвищити точність оцінювання у межових зонах між рівнями захищеності;
- процедуру формування якісних висновків щодо стану кіберзахисту шляхом впровадження апарату асоціативних правил до результатів фазифікації інтегрального показника, що дозволило констатувати поточний рівень захищеності та здійснювати прогнозування стійкості системи до дестабілізуючих впливів.

Отримала подальший розвиток:

- класифікація рівнів зрілості процесів кіберзахисту, яка відрізняється врахуванням факторів воєнного стану та динамічної природи атак, що дозволило диференціювати стан захищеності об'єктів за уточненою п'ятирівневою шкалою.

3. Оцінка змісту дисертації, її завершеності, дотримання принципів академічної доброчесності

Дисертація Юдіної Д.О. є цілісним, глибоким і завершеним науковим дослідженням. Загальний обсяг становить 187 сторінок. Структура включає анотацію, вступ, 4 розділи, висновки, список використаних джерел та 5 додатків. Робота містить 20 рисунків та 13 таблиць.

У першому розділі виконано детальний критичний огляд існуючого науково-методичного апарату. Проведено порівняльний аналіз стандартів ISO/IEC 27001, NIST CSF 2.0, ENISA EUCS, CISA CPGs та норм NIS 2 Directive. Доведено відсутність у чинних комплаєнс-підходах математично

обґрунтованих алгоритмів обробки нечітких експертних суджень і обґрунтовано вибір методу аналізу ієрархій як інструменту зважування.

У другому розділі наведено теоретико-множинний опис розробленої гібридної ієрархічної моделі, що об'єднує 6 систем критеріїв за NIST CSF 2.0 та 7-му систему – «Секторальну складову». Деталізовано 106 базових і 91 галузевий критерій. Розроблено математичну модель нечіткої фазифікації для лінгвістичної змінної CSL («Стан кіберзахисту») із побудовою трапецієподібних функцій належності LR-типу.

У третьому розділі викладено алгоритм методу оцінювання: сформовано дискретну шкалу оцінювання, наведено матриці попарних порівнянь для обчислення вагових коефіцієнтів систем та деталізовано каскадну інтеграцію кількісного розрахунку із системою нечіткого виведення.

У четвертому розділі описано архітектуру розробленого програмного забезпечення. Наведено результати експериментальної валідації методу на об'єкті паливно-енергетичного сектору (за участю 7 експертів). Наведено підсумкові профілі у вигляді пелюсткових діаграм і структурованих звітів.

Робота характеризується високим рівнем наукової сумлінності. Фактів плагіату, фабрикацій, фальсифікацій чи інших порушень академічної доброчесності не виявлено. Авторські публікації та внесок співавторів відображені коректно.

4. Оприлюднення результатів дисертаційної роботи

Основні результати дослідження оприлюднено у 8 наукових працях. Серед них: 7 статей у фахових виданнях України зі спеціальності 122 «Комп'ютерні науки» (3 статті — одноосібні, 3 — у виданні з грифом «ДСК»); 1 праця у матеріалах міжнародної конференції IEEE ATIT 2024, що індексується в міжнародній наукометричній базі Scopus. Отримано свідоцтво про реєстрацію авторського права № 145206 від 06.04.2026 та 3 акти впровадження.

5. Дискусійні питання та зауваження щодо змісту дисертаційної роботи і її окремих положень

Визнаючи високу наукову та практичну цінність дисертаційного дослідження Юдіної Д.О., вважаю за необхідне висловити наступні зауваження та дискусійні моменти:

1. У третьому розділі при розрахунку вагових коефіцієнтів методом аналізу ієрархій припускається лінійна незалежність критеріїв. Проте в реальних кіберфізичних системах ОКІ між системами захисту (наприклад, «Detect» та «Respond») існують синергетичні та нелінійні зв'язки. Доцільно було б розглянути використання мережевих процесів для врахування зворотного зв'язку.

2. При обчисленні матриць попарних порівнянь для розширеної множини з 106 базових та 91 галузевих критеріїв виникає значне обчислювальне та когнітивне навантаження на експертів. У роботі недостатньо розкрито алгоритми декомпозиції, які запобігають зростанню показника неузгодженості.

3. У розробленому програмному забезпеченні збереження сесій оцінювання виконується у файлах JSON. Для захисту аудиторських даних об'єктів критичної інфраструктури (зокрема з обмеженим доступом) доцільно було б передбачити використання зашифрованих баз даних (наприклад, SQLCipher) із розмежуванням прав доступу.

4. У тексті четвертого розділу бракує опису модульних автоматизованих тестів (Unit Tests), які б підтверджували стабільність функціонування ядра нечіткого виведення при граничних і некоректних вхідних даних.

5. В основному тексті дисертації трапляються поодинокі описки в математичних індексах у розділі 2 та стилістичні огріхи в підписах до рисунків.

6. Висновки по дисертаційній роботі

Зазначені зауваження мають зауважувально-дискусійний характер і не знижують наукової цінності та обґрунтованості результатів дисертаційного дослідження.

Дисертаційна робота Юдіної Діани Олексіївни є завершеною, цілісною та самостійною науковою працею, у якій отримано нові обґрунтовані наукові результати, що розв'язують актуальне науково-прикладне завдання галузі комп'ютерних наук.

За обсягом, актуальністю, новизною та практичною значимістю дисертаційна робота «Методи та моделі оцінювання стану кіберзахисту об'єктів критичної інформаційної інфраструктури» повністю відповідає вимогам пунктів 6–8 «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого постановою КМУ від 12 січня 2022 р. № 44 (зі змінами). Її авторка, Юдіна Діана Олексіївна, заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 122 – Комп'ютерні науки (галузь знань 12 – Інформаційні технології).

Офіційний опонент:
доцент кафедри кібербезпеки та захисту інформації
Київського національного університету
імені Тараса Шевченка
кандидат технічних наук, доцент Лариса МИРУТЕНКО

ПІДПИС Мирутенко Л.
ЗАСВІДЧУЮ
ПРОРЕКТОР З НАУКОВОЇ РОБОТИ
ОКСАНА ...НСЬКА