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

старшого дослідника за спеціальністю 122 «Комп'ютерні науки»
Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова
НАН України, доктора технічних наук
Гончара Сергія Феодосійовича
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.

В умовах триваючої повномасштабної збройної агресії рф проти України та інтенсифікації гібридних загроз, захист об'єктів критичної інформаційної інфраструктури (ОКІІ) набув статусу одного з вирішальних чинників національної безпеки. Сучасні ОКІІ функціонують як складні багаторівневі кіберфізичні системи, що робить їх чутливими до випереджальних та високотехнологічних кібератак.

Здобувачка у дисертаційній роботі зазначає, що прийняття Закону України № 4336-IX від 27.03.2025 та постанови Кабінету Міністрів України від 31 грудня 2025 року № 1799 «Про затвердження Порядку оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури» сформувало базову суб'єктну структуру оцінювання стану кіберзахисту.

Проте вивчення зазначених нормативних актів показує, що вони мають переважно рамковий характер. Наразі існує виражена методологічна прогалина: прийняті документальні порядки позбавлені математично обґрунтованого, формалізованого й відтворюваного інструментарію кількісного обчислення рівня кіберзахисту. Традиційні підходи до аудиту спираються на статичні чек-листи, бінарне оцінювання, не враховують рівень зрілості управлінських і технологічних процесів, а також супроводжуються високим ступенем суб'єктивізму та невизначеності у «сірих зонах» на межах рівнів захищеності.

Крім того, існуючі універсальні міжнародні та регіональні стандарти (ISO/IEC 27001, NIST CSF 2.0) не охоплюють повною мірою специфіку 24 секторів критичної інфраструктури України і не враховують загроз воєнного стану. Подолання зазначеної методологічної прогалини вимагає залучення фундаментального апарату комп'ютерних наук – зокрема теорії нечітких множин, багатокритеріального аналізу (методу аналізу ієрархій), теорії прийняття рішень та системного моделювання. З огляду на це, розроблення методів та моделей оцінювання стану кіберзахисту ОКІІ є ***актуальним науково-прикладним завданням у галузі комп'ютерних наук***.

Метою дисертаційного дослідження Юдіної Діани Олексіївни є удосконалення процесу управління кіберзахистом ОКІІ, що полягає у досягненні високої точності та оперативності оцінювання показників кіберзахисту на основі розробленого комплексу гібридних моделей, нечітких методів та багатокритеріального аналізу.

Дисертаційна робота виконана у межах науково-дослідної теми Науково-дослідної лабораторії протидії кіберзагрозам в авіаційній галузі Державного університету «Київський авіаційний інститут» на тему «Методи, моделі та програмні засоби управління інцидентами кібербезпеки в критичній інфраструктурі держави» (державний реєстраційний номер 0125U000624).

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

Наукові положення, висновки та рекомендації, сформульовані в дисертаційній роботі Юдіної Д.О., є належно обґрунтованими та характеризуються високим ступенем достовірності. Достовірність результатів забезпечена коректною математичною постановкою задач, застосуванням апробованого математичного апарату теорії множин, теорії нечітких множин, методу аналізу ієрархій (MAI) Т. Сааті, системного аналізу та теорії прийняття рішень. Теоретичні моделі узгоджуються з проведеними експериментальними дослідженнями на об’єктах паливно-енергетичного сектору критичної інфраструктури, де показник узгодженості експертних суджень склав CR = 0,05, що свідчить про високу репрезентативність. Результати підтверджені актами впровадження в Адміністрації Державної служби спеціального зв'язку та захисту інформації України, Державному науково-дослідному інституті технологій кібербезпеки та захисту інформації, Державному університеті «Київський авіаційний інститут», свідоцтвом про реєстрацію авторського права на твір № 145206.

Наукова новизна одержаних результатів полягає у розв’язанні актуального наукового завдання з розробки методів та моделей оцінювання стану кіберзахисту ОКІІ. До найбільш суттєвих нових наукових результатів належать:

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 пріоритезації 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

Дисертаційна робота Юдіної Д.О. викладена на 187 сторінках друкованого тексту, з яких 143 сторінки становить основний зміст. Робота містить анотацію українською та англійською мовами, перелік умовних скорочень, вступ, чотири розділи, загальні висновки, список використаних джерел із 103 найменувань та 5 додатків. У тексті наведено 20 рисунків та 13 таблиць.

У вступі обґрунтовано актуальність теми, сформульовано мету, задачі, об’єкт, предмет та методи дослідження, викладено наукову новизну, практичне значення отриманих результатів, наведено дані про апробацію, публікації та зв’язок із науковими темами.

У першому розділі проведене поглиблене науково-методологічне дослідження існуючих підходів до оцінювання стану кіберзахисту ОКІІ. Проведено класифікацію методів за трьома напрямами: процедурні (на основі зрілості – CMMI, C2M2), перевірочні (на основі відповідності – ISO/IEC 27001, NIST SP 800-53) та аналітичні (на основі ризиків – FAIR, CISA CPGs). Здійснено компаративний аналіз міжнародних рамок (NIST CSF 2.0, EUCS ENISA, NIS 2 Directive) та проаналізовано процес гармонізації національного законодавства (Закон України № 4336-IX, постанови Кабінету Міністрів України від 19.06.2019 № 518, від 31.12.2025 № 1799, наказ Адміністрації Держспецзв'язку від 30.01.2026 № 75). Доведено, що пряме відтворення міжнародних стандартів без врахування умов воєнного стану та специфіки 24 секторів критичної інфраструктури створює ризики «паперової безпеки». Проаналізовано математичний апарат агрегування даних і обґрунтовано вибір методу аналізу ієрархій (MAI) для формалізації вагових коефіцієнтів.

У другому розділі розроблено гібридну ієрархічну модель системи показників кіберзахисту ОКІІ. Модель базується на семи функціональних системах критеріїв: «Управління» (31 критерій), «Ідентифікація» (21 критерій), «Кіберзахист» (22 критерії), «Виявлення» (11 критеріїв), «Реагування» (13 критеріїв), «Відновлення» (8 критеріїв) та авторська «Секторальна складова» (від 3 до 5 критеріїв для кожного з 24 секторів критичної інфраструктури, усього 91 галузевий критерій). Також у розділі розроблено математичну модель нечіткої інтерпретації результатів оцінювання на основі теорії нечітких множин. Застосовано лінгвістичну змінну «Стан кіберзахисту» (CSL) та 5 еталонних трапецієподібних нечітких чисел LR-типу для формалізації станів захищеності (від «Початкового» до «Оптимізованого»).

У третьому розділі розроблено метод оцінювання стану кіберзахисту ОКІІ. Запропоновано багаторівневу дискретну шкалу квантифікації якісних характеристик (1,0 – виконання повністю; 0,5 – частково; 0,2 – заплановано; 0 – не виконано / не застосовується). Описано процедуру розрахунку вагових

коефіцієнтів систем критеріїв за методом MAI T. Сааті. Обґрунтовано каскадний спосіб інтеграції детермінованого розрахунку та нечіткої інтерпретації з обчисленням нормалізованого індексу впевненості (ECI) та використанням асоціативних правил для діагностики «сірих зон».

У четвертому розділі наведено опис розробленого комп'ютерного застосунку «Програмний компонент оцінювання рівня кіберзахисту ОКІІ». Наведено результати експериментальних досліджень на об'єкті паливно-енергетичного сектору критичної інфраструктури за участю групи з 7 експертів. Експеримент підтвердив високу точність, збіжність та оперативність роботи методу.

Зміст дисертації є повністю завершеним, характеризується внутрішньою єдністю та логічною послідовністю викладу. Фактів академічного плагіату, самоплагіату, фабрикації чи фальсифікації даних не виявлено.

4. Оприлюднення результатів дисертаційної роботи

Основні теоретичні та практичні результати дисертаційного дослідження відображено у 8 наукових публікаціях. Серед них: 7 наукових статей у провідних фахових виданнях України зі спеціальності 122 «Комп'ютерні науки» (у тому числі 3 статті одноосібні, а 3 статті опубліковані з грифом обмеження доступу «Для службового користування»); 1 публікація у матеріалах міжнародної науково-технічної конференції IEEE ATIT 2024 (м. Львів), що індексується у міжнародній наукометричній базі Scopus.

Практична реалізація підтверджується Свідоцтвом про реєстрацію авторського права на твір № 145206 від 06.04.2026 та трьома актами впровадження.

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

Оцінюючи позитивно дисертаційну роботу Юдіної Д.О., вважаю за необхідне вказати на такі дискусійні питання та зауваження:

1. У другому розділі при математичній формалізації еталонних станів кіберзахисту на основі нечітких чисел LR-типу параметри лівої та правої меж

носіїв чисел обрано з однакових коефіцієнтів симетрії. Доцільно було б надати додаткове обґрунтування варіативності коефіцієнта зближеності залежно від категорії критичності ОКІІ (I, II, III чи IV категорія).

2. У розробленому методі оцінювання (Розділ 3) для формалізації виконання заходів використовується дискретна шкала, де значення 0,2 присвоюється за наявності затвердженого плану та бюджетування. Проте у роботі детально не регламентовано граничний часовий термін виконання такого плану, після перевищення якого показник має обнулятися.

3. У четвертому розділі експериментальну перевірку розробленого методу та моделі проведено на прикладі об’єкта паливно-енергетичного сектору критичної інфраструктури. Робота виграла б від наведення порівняльного аналізу експериментальних даних для об’єктів інших секторів (наприклад, сектору цифрових технологій чи транспорту і пошти).

4. При визначенні вагових коефіцієнтів систем критеріїв за методом аналізу ієрархій в ілюстративному розрахунку використано класичну 9-бальну шкалу Т. Сааті. Було б доцільно надати аналіз стабільності вагових коефіцієнтів при використанні нечітких або логарифмічних модифікацій даної шкали.

6. Висновки по дисертаційній роботі

Зазначені зауваження мають переважно дискусійний та рекомендаційний характер, не впливають негативно на наукову цінність роботи і не применшують вагомості отриманих здобувачкою результатів.

Дисертаційна робота Юдіної Діани Олексіївни є завершеною кваліфікаційною працею, у якій отримано нові обґрунтовані наукові результати, що у сукупності вирішують актуальне науково-прикладне завдання щодо вдосконалення процесів оцінювання стану кіберзахисту ОКІІ.

Дисертаційна робота «Методи та моделі оцінювання стану кіберзахисту об’єктів критичної інформаційної інфраструктури» 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 від 12 січня 2022 р. № 44 (зі змінами). З огляду на це, 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:
заступник директора з науково-технічної роботи
Інституту проблем моделювання в енергетиці
ім. Г.Є. Пухова НАН України
доктор технічних наук Сергій ГОНЧАР