КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.31.1083
УДК 004.056.5

Юдіна Діана Олексіївна
аспірант факультету комп'ютерних наук та технологій
Державний університет "Київський авіаційний інститут", Київ, Україна
ORCID: 0000-0002-1277-8771
diana.yudina22@gmail.com

Юдін Дмитро Олексійович
студент факультету прикладної математики
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна
ORCID: 0009-0002-9946-494X
yudin.dmytro@lll.kpi.ua

МЕТОДИКА РОЗРАХУНКУ РІВНЯ КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Анотація. У статті розв'язано актуальне науково-практичне завдання щодо створення уніфікованого інструменту для кількісного розрахунку рівня кіберзахисту об'єктів критичної інформаційної інфраструктури (ОКІІ). Було обґрунтовано актуальність дослідження, зумовлену безпрецедентним зростанням кількості кібератак (на 74% у 2025 році порівняно з 2024 роком) та зміною їхнього вектора у бік систем SCADA. Наголошено на відсутності в Україні інструменту, який би дозволив операторам об'єктивно оцінити свій рівень кіберзахисту, а регуляторам — здійснювати ефективний моніторинг та аудит стану кіберзахисту. Згруповано існуючі методики за трьома характеристиками: процедурні, перевірочні та аналітичні. Визначено, що жодна з них не є повністю універсальною для умов повномасштабної війни, що зумовило потребу в розробці гібридного підходу. Результати дослідження представляють деталізовану методику, яка використовує попередньо розроблений метод розрахунку рівня кіберзахисту ОКІІ. Методика інтегрує сім систем критеріїв: Управління (GV), Ідентифікація ризиків кібербезпеки (ID), Кіберзахист (PR), Виявлення кіберінцидентів (DE), Реагування на кіберінциденти (RS) та Відновлення стану кібербезпеки (RC) та Секторальна складова (SE). Для врахування ризик-орієнтованого підходу застосовано метод аналізу ієрархій (MAI), що дозволяє через попарні порівняння визначити вагові коефіцієнти для кожного напряму захисту. Описано процедуру збору даних через трикомпонентний підхід: інспекцію документації, інтерв'ювання та технічне тестування, що мінімізує суб'єктивність оцінювання. Також наведено результати практичного застосування методики на об'єктах паливно-енергетичного сектору та проведено порівняльний аналіз розробленого авторського програмного забезпечення із двома міжнародними аналогами, який довів вищу точність авторської методики завдяки адаптації до національного законодавства та можливості індивідуального налаштування ваг. Ідентифіковано, що найбільш критичними прогалинами є системи з високою вагою та низьким рівнем реалізації. Практична цінність роботи полягає у створенні дорожньої карти для керівництва ОКІІ щодо пріоритезації інвестицій у безпеку. Перспективи подальших досліджень спрямовані на автоматизацію визначення цільового рівня кіберзахисту для проведення аналізу прогалин.

Ключові слова: кіберзахист; критична інфраструктура; об'єкти критичної інфраструктури; об'єкти критичної інформаційної інфраструктури; метод розрахунку; методика розрахунку; вагові коефіцієнти.

© Д.О. Юдіна, Д.О. Юдін, 2025

ВСТУП

Актуальність розробки методики розрахунку рівня кіберзахисту об’єктів критичної інформаційної інфраструктури (ОКІІ) обумовлена сукупністю чинників, що загрожують національній безпеці та стійкості держави.

По-перше, аналітичні звіти Ради національної безпеки і оборони України (РНБО) та Державної служби спеціального зв’язку та захисту інформації України (Держспецзв’язку) [1, 2] вказують, що рф та її сателіти (КНР, КНДР) використовують кібератаки як інструмент для дестабілізації, здійснення кібершпигунських операцій та завдання прямої шкоди об’єктам критичної інфраструктури (ОКІ). Геополітична напруженість стала прямим каталізатором нових загроз для державного та приватного секторів [1].

По-друге, спостерігається безпрецедентне кількісне та якісне зростання кібератак. За офіційними даними національної команди реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA (національний CSIRT), за перше півріччя 2025 року було опрацьовано 3018 кіберінцидентів, що демонструє кількісне зростання на 74% порівняно з аналогічним періодом 2024 року (1739 кіберінцидентів) [3, 4]. Найпоширенішими типами кіберінцидентів, що фіксуються національним CSIRT є: Розповсюдження шкідливого програмного забезпечення (ШПЗ), Фішинг, Зараження ШПЗ, Компрометація облікового запису та Компрометація системи [3].

По-третє, змінився вектор атак, що призводить до прямих безпекових та економічних збитків. Атаки дедалі частіше спрямовуються не лише на IT-інфраструктуру (кібершпигунство, викрадення даних), але й на операційні технології (ОТ). Це несе загрозу фізичного пошкодження обладнання та припинення надання життєво важливих послуг (електрика, зв'язок, водопостачання). Прикладом катастрофічних наслідків є кібератака на одного з національних операторів мобільного зв’язку – Київстар у грудні 2023 року [1].

По-четверте, актуальним залишається питання методичного забезпечення: за наявності нормативної бази оператори критичної інфраструктури позбавлені механізму для кількісного оцінювання власного рівня кіберзахисту. Чинна нормативно-правова база (зокрема, Закони України «Про критичну інфраструктуру», «Про основні засади забезпечення кібербезпеки України» та постанова Кабінету Міністрів України від 19.06.2019 № 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури») покладає на власників ОКІІ відповідальність за забезпечення належного рівня захисту. Однак на практиці відсутній уніфікований інструмент, який би дозволив операторам критичної інфраструктури об'єктивно оцінити свій поточний стан кіберзахисту, а регуляторам – здійснювати ефективний моніторинг та аудит.

Таким чином, розробка запропонованої методики є необхідним кроком для впровадження алгоритму кількісного оцінювання, що дозволяє структурувати процес аудиту та забезпечити перехід до вимірюваного управління станом кіберзахисту ОКІІ в умовах динамічного середовища загроз.

Постановка проблеми. Актуальне наукове та практичне завдання полягає у створенні обґрунтованої, уніфікованої методики для кількісного розрахунку інтегрального рівня кіберзахисту ОКІІ. Існуючі підходи до розрахунку кіберзахисту, що традиційно ґрунтуються на аналізі зрілості, оцінці ризиків чи верифікації відповідності стандартам, мають певні функціональні обмеження. Ці обмеження виявляються у їхній недостатній універсальності та нездатності комплексно враховувати українську

секторальну специфіку ОКІІ, необхідність обґрунтування інвестицій (ризиковий підхід) і, водночас, забезпечувати стандартизований аудит (підхід відповідності).

В [6] було розроблено модель розрахунку рівня кіберзахисту об'єктів критичної інфраструктури, в [7] проведено модифікацію запропонованої моделі та в [5] розроблено метод розрахунку рівня кіберзахисту об'єктів критичної інформаційної інфраструктури. На основі розроблених моделі та методу пропонується методика розрахунку рівня кіберзахисту об'єктів критичної інформаційної інфраструктури. Актуальність методики розрахунку рівня кіберзахисту зумовлена її здатністю забезпечити практичне застосування моделі, викладеної в [6, 7] та методу, викладеного в [5]. Запропонована методика перетворює абстрактні модель та метод на послідовний та деталізований алгоритм. Вона забезпечує відтворюваність результатів незалежно від виконавця, що є критично важливим для моніторингу динаміки кіберзахисту. Отримані на основі методики кількісні показники слугують науково-обґрунтованою основою для ідентифікації слабких місць системи, ефективного розподілу ресурсів та формування стратегії підвищення рівня кіберзахисту. Таким чином, методика є не лише інструментом вимірювання, але й основою для проактивного управління ризиками.

Призначення: Методика призначена для фахівців з кібербезпеки ОКІ.

Об'єкт оцінювання: стан кіберзахисту ОКІІ.

Аналіз останніх досліджень і публікацій. Для розрахунку рівня кіберзахисту використовують підходи з різними характеристиками: на основі зрілості, на основі ризиків та на основі відповідності.

Дослідженнями методів оцінки зрілості кіберзахисту займаються зокрема Software Engineering Institute (модель CMMI) [8], Міністерство енергетики США (модель C2M2) [9], а також окремі науковці, які адаптують створені підходи, зокрема Уоттс Хамфрі, Мартін Кляйн і Майкл Л. Масі [10-11], а також українські дослідники Худинцев М. М. та Палажченко І. Л. [12].

Дослідження методів оцінки кіберзахисту на основі ризиків є предметом робіт як провідних інституцій, зокрема National Institute of Standards and Technology (NIST), розробника фреймворку NIST Cybersecurity Framework, version 2.0 (NIST CSF 2.0). [13], та International Organization for Standardization (ISO), видавника стандарту ISO/IEC 27005 [14], так і науковців, які зробили значний внесок у розвиток цього підходу, серед яких Гері Стоунбернер, Джек Джонс, Майкл Паттон, Мансур Алалі [15-19], а також українського дослідника Гончара С.Ф. [20].

Розрахунок рівня кіберзахисту методами, орієнтованими на відповідність, переважно регулюється міжнародними структурами. Серед них виділяється International Organization for Standardization (ISO), яка є видавником стандарту ISO/IEC 27001 [21]. В Україні створенням національної нормативної бази займаються державні органи влади, зокрема Кабінет Міністрів України та Держспецзв'язку. Наукові дослідження у цій сфері концентруються на поглибленому вивченні та модернізації чинних регулятивних вимог.

В [5] здійснено аналіз методів оцінки рівня кіберзахисту за вказаними характеристиками, який показав, що жоден з існуючих методів не є повністю універсальним. Таким чином в [5] було розроблено авторський метод, який є гібридним і передбачає інтеграцію критеріїв відповідності з гнучкими показниками зрілості (для стратегічного планування), а також включає ризик-орієнтований підхід. Разом з тим, зазначений метод враховує секторальну специфіку ОКІІ та динамічний характер загроз.

Незважаючи на обґрунтованість розробленого методу, він залишається концептуальним, оскільки не містить прикладного інструменту, необхідного для його практичного застосування. Зокрема, відсутня чітка методична база, що включає

послідовність операцій, стандартизовані інструменти та конкретні показники для оцінки та впровадження.

До прикладу, розглянемо існуючі методики розрахунку стану кіберзахисту.

У роботі [21] український науковець Володимир Шиповський дослідив підходи до розрахунку рівня кіберзахисту інформаційних систем. З трьох підходів один є програмним застосунком «Стандарт оцінки кібербезпеки інформаційних технологій» (CSET) від Національного інституту стандартів та технологій (NIST) США, другий – міжнародним стандартом «Оцінка рівня кібербезпеки на основі заходів забезпечення безпеки інформації» (ISO/IEC 27001) від Міжнародної організації зі стандартизації (ISO), третій – «Методологією секторальної оцінки кібербезпеки» від Європейського агентства з кібербезпеки (ENISA). В межах нашого дослідження розглянемо третій варіант – «Методологію секторальної оцінки кібербезпеки» (SCSA Methodology) [22]. Перевагою конкретної методології є те, що вона дозволяє здійснити оцінку кібербезпеки в рамках конкретного сектору критичної інфраструктури, допомагає визначити необхідний рівень гарантії для ІКТ-продуктів та є орієнтованою на ризики. Водночас, застосування цієї методології потребує застосування значних ресурсів та глибокої експертизи, а також узгодження з чинними національними регуляторними базами.

Іншою популярною методикою для розрахунку стану кіберзахисту можна вважати NIST SP 800-53A [23], яка є методичним посібником до основного каталогу контролів NIST SP 800-53 [24]. Документ надає деталізовані та конкретні процедури для кожного контролю, використовує три різні методи оцінки (інспектування документації, інтерв'ювання персоналу та тестування середовищ). Водночас, документ є надзвичайно об'ємним, застосування методики у повному обсязі є ресурсомістким та вимагає спеціальних знань від оцінювачів, а також не адаптований під національну термінологічну базу.

У разі використання міжнародних стандартів серії ISO, методикою є ДСТУ ISO 19011:2019 [25]. Стандарт є універсальним посібником, який використовується для аудиту будь-якої системи, розробленої на основі стандартів серії ISO. У контексті кіберзахисту ДСТУ ISO 19011:2019 використовується як методична основа для проведення аудитів на відповідність ДСТУ ISO/IEC 27001:2023 [26]. Документ чітко визначає принципи аудиту та надає покрокову методику. Поряд із перевагами, стандарт характеризується певною змістовною обмеженістю: він встановлює лише регламент аудиторської діяльності, не пропонуючи деталізованої технічної бази контрольних показників, що вимагає додаткового залучення фахівців з відповідною технічною компетенцією. Також стандарт вимагає створення та підтримки комплексної програми аудиту, не гарантує якості системи управління.

Методика FAIR (Factor Analysis of Information Risk) [27] є провідним аналітичним підходом до оцінки кіберризиків, що забезпечує їхнє кількісне вимірювання у фінансовому еквіваленті. Основна перевага FAIR полягає у декомпозиції складної проблеми ризику на вимірювані фактори (ймовірність взаємодії загрози, вразливість, масштаб втрат), що дозволяє керівництву приймати обґрунтовані бізнес-рішення щодо інвестицій у кібербезпеку, оскільки результати представлені мовою грошових одиниць. Водночас, ключові недоліки методики пов'язані з потребою у достовірних історичних даних для проведення точного аналізу та необхідністю залучення висококваліфікованих аналітиків, здатних коректно оцінювати діапазони ймовірності та масштабу втрат.

Методика оцінки відповідності вимогам PCI DSS (Payment Card Industry Data Security Standard) [28] забезпечує високий та стандартизований рівень безпеки у всій екосистемі платіжних систем, оскільки методика надає чіткі 12 основних вимог та

детальні перевірочні процедури для кожного контролю, забезпечуючи одноманітний підхід до аудиту. Ключові недоліки методики пов'язані з її ресурсомісткістю та фокусом на мінімальних вимогах, а також до необхідності високих фінансових витрат на щорічний аудит незалежними аудиторами для великих організацій.

Методика CMMI (Capability Maturity Model Integration) [29], яка часто використовується як основа для оцінки зрілості кібербезпеки (наприклад, C2M2 є адаптацією її принципів), є процедурною методикою, що надає структурований шлях вдосконалення процесів організації шляхом переходу через п'ять рівнів зрілості: від початкового до оптимізованого. Основна перевага CMMI полягає у забезпеченні чіткої дорожньої карти для послідовного підвищення якості, передбачуваності та ефективності процесів (включаючи процеси безпеки), що дозволяє керівництву приймати обґрунтовані рішення про інвестиції на основі досягнутого рівня зрілості. Проте, ключові недоліки CMMI включають її високу вартість впровадження та сертифікації, значне документаційне навантаження та ризик того, що організація може зосередитися виключно на досягненні рівня зрілості (що є бюрократичним показником) замість реальної адаптації та покращення бізнес-результатів.

Отже, можна згрупувати методики розрахунку рівня кіберзахисту за такими характеристиками:

1. Процедурні методики (на основі фреймворків та стандартів);
2. Перевірочні методики (на основі аудиту та відповідності);
3. Аналітичні методики (на основі кількісної оцінки ризиків).

Таблиця 1

Порівняльна таблиця методик розрахунку рівня кіберзахисту

Методики розрахунку рівня кіберзахисту	Процедурні методики	Перевірочні методики	Аналітичні методики
SCSA Methodology [22]	+	-	+
NIST SP 800-53A [23]	-	+	-
ДСТУ ISO 19011:2019 [25]	-	+	-
Методика FAIR [27]	-	-	+
Методика оцінки відповідності вимогам PCI DSS [28]	-	+	-
Методика CMMI [29]	+	-	-

В табл. 1 здійснено порівняння методик розрахунку рівня кіберзахисту за такими характеристиками: методики на основі фреймворків та стандартів, методики на основі аудиту та відповідності, аналітичні методики.

Аналіз показав, що жодна з розглянутих методик не є універсальною. Процедурні методики надають детальний алгоритм для побудови та вдосконалення системи кіберзахисту, однак мають високе документаційне навантаження. Перевірочні методики забезпечують об’єктивність та відповідність зовнішнім вимогам, але є ресурсомісткими і фокусуються на мінімально необхідних контролях. Аналітичні методики вимагають значної кількості достовірних даних. З огляду на специфіку українських реалій, враховуючи повномасшабне вторгнення рф, збільшення кількості кібератак на ОКІ та необхідність швидко і якісно оцінити стан кіберзахисту ОКІІ, існує потреба в розробці гібридної методики, яка б інтегрувала переваги кожного з підходів, дозволяючи одночасно оцінювати зрілість процесів, верифікувати відповідність стандартам та обґрунтовувати рішення щодо безпеки на основі кількісних ризиків.

З цією метою для розробки методики обрано метод, розроблений в [5], який поєднує об'єктивні критерії відповідності з гнучкими показниками зрілості для стратегічного планування та інтегрує ризик-орієнтований підхід для фокусування на найбільш критичних загрозах. Метод включає всі необхідні компоненти: оцінку зрілості, верифікацію відповідності (об'єктивні критерії) та ризик-орієнтований підхід, що є необхідним для комплексної оцінки стану кіберзахисту. Крім того, застосування вагових коефіцієнтів є необхідним елементом для відображення неоднакового впливу різних систем критеріїв і, відповідно, врахування ризик-орієнтованого підходу в остаточному кількісному показнику. Фіналізація розрахунку у вигляді єдиного кількісного показника в діапазоні від 0 до 1 з подальшою інтерпретацією за п'ятирівневою шкалою зрілості (узгодженою з NIST CSF та CMMI), забезпечує безпосередній зв'язок між виконанням контролів (відповідність), якістю процесів (зрілість) та економічною доцільністю (ризики), що робить метод логічно завершеним та цільовим для побудови прикладної гібридної методики оцінки кіберзахисту ОКІІ.

Отже, **метою** роботи є розробка гібридної методики для кількісного розрахунку інтегрального рівня кіберзахисту ОКІІ.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

З метою практичної реалізації теоретичних положень, викладених у попередніх роботах [5-7], та для вирішення проблеми відсутності уніфікованого прикладного інструменту, було розроблено гібридну методику кількісного розрахунку інтегрального рівня кіберзахисту ОКІІ. Розроблена методика являє собою послідовний алгоритм, який перетворює багатокритеріальний метод на алгоритм, забезпечуючи обов'язкову інтеграцію функціональних підходів: оцінки відповідності (об'єктивні критерії), оцінки зрілості (стратегічне планування) та ризик-орієнтованого підходу (за допомогою вагових коефіцієнтів).

Методика структурована у п’ять послідовних етапів, які дозволяють перейти від збору первинних даних до формування єдиного кількісного показника, готового до інтерпретації та управлінського використання.

Структура та етапи методики

Етап 1. Підготовка та визначення обсягу оцінювання

Цей етап методики полягає у формалізації обсягу, меж та критеріїв оцінювання.

1.1. Формування команди

Першочергово визначається склад експертної робочої групи, яка відповідатиме за проведення оцінювання та збір даних. До групи включаються фахівці з кіберзахисту ОКІІ, представники керівництва ОКІІ, а також може бути запрошений зовнішній експерт. Серед членів робочої групи визначаються окремі відповідальні за збір первинної документації, проведення інтерв’ю з персоналом ОКІІ, а також за верифікацію технічних даних.

1.2. Визначення середовища оцінювання

Після формування робочої групи, здійснюється визначення та формалізація середовища оцінювання. Процедура визначення середовища передбачає наступні варіанти:

- Оцінка загальної інформаційно-комунікаційної системи (ІКС) ОКІІ, яка включає всі ІТ- та ОТ-компоненти, які забезпечують надання життєво важливих послуг.

- Оцінка окремих сегментів ІКС ОКІІ. Допускається виділення окремих ІКС або їх сегментів. Це застосовується у випадках, коли певні системи мають специфічні регуляторні або технічні вимоги щодо кіберзахисту (наприклад, системи обробки фінансових даних, сегменти автоматизованих систем управління технологічними процесами тощо).

Після визначення середовища оцінювання формується документ, де визначено зафіксовані межі оцінювання, а також причини виділення окремих ІКС або їх сегментів.

1.3. Актуалізація критеріїв оцінювання

Актуалізація здійснюється з метою узгодженості критеріїв оцінювання з регуляторними вимогами. На цьому етапі здійснюється перевірка чинності та актуальності національної нормативно-правової бази, що включає:

Закони України «Про основні засади забезпечення кібербезпеки України», «Про критичну інфраструктуру», «Про захист інформації в інформаційно-комунікаційних системах»;

постанови Кабінету Міністрів України від 19.06.2019 № 518 «Про затвердження Загальних вимог з кіберзахисту об’єктів критичної інфраструктури», від 18.06.2025 № 712 «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем», від 09.10.2020 № 943 «Деякі питання об’єктів критичної інформаційної інфраструктури», від 29.12.2021 № 1426 «Про затвердження Положення про організаційно-технічну модель кіберзахисту», від 26.11.2025 № 1533 «Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози», від 24.03.2023 № 257 «Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури»;

накази Адміністрації Держспецзв’язку від 29.05.2023 № 463 «Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами», від 14.09.2024 № 505 «Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту при використанні технології хмарних обчислень та Методичних рекомендацій щодо оцінки відповідності хмарних послуг рівням безпеки (впевненості)», від 30.08.2023 № 773 «Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту систем електронного документообігу», спільний наказ Служби безпеки України та Адміністрації Держспецзв’язку від 19.12.2024 № 627/772 «Деякі питання розробки, затвердження та погодження планів захисту об’єктів критичної інфраструктури за проектною загрозою національного рівня «кібератака/кіберінцидент».

Враховуючи функціональні відмінності ОКІІ, методика передбачає можливість адаптації уніфікованої системи критеріїв до галузевої специфіки оцінюваного сектору критичної інфраструктури, тому обов’язково здійснюється перевірка чинності та актуальності секторальних нормативних документів (наприклад, наказ Міністерства енергетики України від 05.08.2024 № 285 «Про затвердження Методики оцінювання стану кібербезпеки електричних мереж та практик кібербезпеки електричних мереж», постанова Правління Національного банку України від 12.08.2022 № 178 «Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України» тощо).

Після визначення актуальних вимог нормативно-правової бази України забезпечується включення до фінальної системи критеріїв усіх функціональних груп, які передбачені гібридним методом:

Критерії відповідності – до цієї групи включаються множина систем критеріїв (*SC*), яка містить сім систем критеріїв, шість з яких відповідають вимогам постанови Кабінету Міністрів України від 29 грудня 2021 року № 1426 [30] (Управління (GV), Ідентифікація ризиків кібербезпеки (ID), Кіберзахист (PR), Виявлення кіберінцидентів (DE), Реагування на кіберінциденти (RS) та Відновлення стану кібербезпеки (RC)). Додатково включено сьому систему критеріїв — Секторальна складова (SE), що враховує специфіку конкретної галузі, наприклад, паливно-енергетичного сектору. Кожна з семи систем критеріїв містить певну кількість деталізованих критеріїв. Ці критерії сформовані у відповідності до наказу Адміністрації Держспецзв'язку № 54 від 30.01.2025 [31]. Наприклад, система критеріїв Управління (GV) включає 31 критерій, Ідентифікація ризиків кібербезпеки (ID) – 21, Кіберзахист (PR) – 22, Виявлення кіберінцидентів (DE) – 11, Реагування на кіберінциденти (RS) – 13 та Відновлення стану кібербезпеки (RC) – 8. Система критеріїв Секторальна складова (SE) є індивідуальною для кожного сектора критичної інфраструктури і складається з різної кількості критеріїв [7, табл. 4].

Критерії зрілості – ці критерії необхідні для представлення результатів методики у вигляді єдиного інтегрального кількісного показника, який відображає поточний рівень кіберзахисту ОКІІ. Ці критерії інтерпретуються за шкалою в діапазоні від 0 до 1 [7, табл. 2].

Критерії ризиків – ці критерії використовуються для розробки вагових коефіцієнтів w_i шляхом проведення попарних порівнянь систем критеріїв (SC_i) за методом аналізу ієрархій (MAI) [5, 32]. Ці критерії ґрунтуються на експертній оцінці критичності активів ОКІІ та ймовірності/впливу загроз, характерних для даного сектора критичної інфраструктури.

Підсумок етапу 1: перший етап розробленої методики є підготовчим та методологічно ключовим для забезпечення валідності та релевантності подальшої оцінки. На цьому етапі відбувається формування експертної групи та розподіл ролей. Здійснюється чітке визначення середовища оцінювання, яке може охоплювати загальну ІКС або цільове виділення окремих ІКС/сегментів. Паралельно відбувається актуалізація та адаптація системи критеріїв, яка є суттю гібридного методу: до неї включаються критерії відповідності (на основі [31]), критерії зрілості та критерії ризиків. Секторальна адаптація забезпечує необхідну релевантність оцінки до унікальних вимог галузі.

Етап 2. Збір первинних даних та оцінка відповідності

Цей етап методики забезпечує збір та верифікацію даних для подальшого кількісного розрахунку інтегрального рівня кіберзахисту та застосування вагових коефіцієнтів.

Для мінімізації суб'єктивності та забезпечення відтворюваності результатів, для збору даних використовується набір стандартизованих оціночних інструментів. До них відносяться структуровані анкети, опитувальники та чек-листи, які безпосередньо корелюють з критеріями відповідності, визначеними на Етапі 1.

Важливим компонентом збору даних є верифікація достовірності, що має усунути потенційні викривлення, спричинені суб'єктивністю або неповнотою інформації. Пропонується здійснювати верифікацію зібраних даних за допомогою трикомпонентного підходу, який описано у [23]. Цей підхід забезпечує об'єктивність первинної оцінки, оскільки вимагає підтвердження на трьох рівнях:

- інспекція: перевірка наявності формальних доказів (політик, процедур, журналів, конфігураційних файлів), що підтверджує документальне впровадження критерію;
- інтерв'ювання: обговорення з профільним персоналом ОКІ для оцінки розуміння та усвідомленого застосування впроваджених заходів;

- тестування: активна перевірка операційної ефективності та коректності функціонування критерію в реальному середовищі (наприклад, технічна перевірка конфігурацій, оцінка механізмів автентифікації). Рівень тестування застосовний тільки до тих критеріїв, які є технічними або організаційно-технічними.

Фінальним завданням етапу 2 є перетворення якісних характеристик стану кіберзахисту на бінарні показники. Це досягається шляхом фіксування відповідей на критерії відповідності у форматі «так» (критерій впроваджено) або «ні» (критерій не впроваджено), що є основою для подальшою математичної формалізації.

Підсумок етапу 2: другий етап розробленої методики формує набір нормалізованих дискретних значень, які відображають первинний (незважений) рівень кіберзахисту ОКІІ.

Етап 3. Визначення вагових коефіцієнтів

Цей етап є ключовим для забезпечення ризик-орієнтованого підходу в розробленій методиці, оскільки він дозволяє відобразити неоднаковий вплив різних систем критеріїв на загальний стан кіберзахисту ОКІІ та сфокусувати увагу на найбільш критичних загрозах.

Для кількісної формалізації експертних оцінок щодо критичності активів та ймовірності загроз обґрунтовано застосовано метод аналізу ієрархій (MAI), який дозволяє перетворити якісні експертні знання у нормовані кількісні вагові показники [5].

MAI передбачає, що експертна група здійснює попарне порівняння систем критеріїв ОКІІ (наприклад, «Ідентифікація ризиків кібербезпеки» та «Реагування на кіберінциденти») за стандартизованою фундаментальною шкалою Сааті, що передбачає значення від 1 до 9.

Оскільки оцінювання проводиться групою незалежних експертів, ключовим етапом є агрегація індивідуальних суджень для досягнення консенсусу. Кожен експерт формує свою власну матрицю попарних порівнянь A_k. Для отримання єдиної агрегованої матриці A_{agr} застосовується принцип об'єднання індивідуальних суджень, що зберігає властивість оберненості матриці.

Консолідація оцінок здійснюється шляхом розрахунку геометричного середнього для кожного елемента серед усіх експертів:

$$\overline{a_{ij}} = (\prod_{k=1}^{N} a_{ij,k})^{1/N} \quad (1),$$

де N — загальна кількість експертів;

$a_{ij,k}$ — судження k-го експерта щодо порівняння критерію i та j.

На основі отриманої агрегованої матриці A_{agr} здійснюється математичний розрахунок вектора пріоритетів (w) за виразом:

$$w_i = \frac{1}{n}\sum_{j=1}^{n} A'_{ij} \quad (2),$$

де n – загальна кількість критеріїв, що порівнюються;

A'_{ij} – позначення елемента нормалізованої агрегованої матриці, де i - номер рядка, j - номер стовпця.

Цей вектор, після верифікації його узгодженості (де $CR \leq 0.1$), слугує нормалізованим ваговим коефіцієнтом для відповідної системи критеріїв у формулі розрахунку інтегрального показника.

Підсумок етапу 3: результатом цього етапу є набір зважених коефіцієнтів w_i, що забезпечує пряму кореляцію між ідентифікованими критичними ризиками ОКІІ та методологічною значимістю кожної системи критеріїв у розрахунку інтегрального показника рівня кіберзахисту.

Етап 4. Кількісний розрахунок інтегрального показника рівня кіберзахисту

На цьому етапі забезпечується консолідація даних про відповідність та ризик-орієнтованих вагових коефіцієнтів у єдиний кількісний показник.

1. Для визначення первинного (незваженого) рівня кіберзахисту ОКІІ необхідно визначити середнє арифметичне за кожною системою критеріїв.

Для цього введемо множину з семи системи критеріїв, яка охоплює окремі критерії, і відобразимо її як:

$$SC = \{\cup_{i=1}^{n} SC_i\} = \{SC_1, SC_2, SC_3, SC_4, SC_5, SC_6, SC_7\} = \{SE, GV, ID, PR, DE, RS, RC\}, \quad (3),$$

де $SC_1 = SE =$ "Секторальна складова", $SC_2 = GV =$ "Управління", $SC_3 = ID =$ "Ідентифікація ризиків кібербезпеки", $SC_1 = PR =$ "Кіберзахист", $SC_1 = DE =$ "Виявлення кіберінцидентів", $SC_1 = RS =$ "Реагування на кіберінциденти", $SC_1 = RC =$ "Відновлення стану кібербезпеки".

Кожен з зазначених систем критеріїв характеризується підмножиною критеріїв:

$$SC = \left\{\bigcup_{i=1}^{n}\left\{\bigcup_{j=1}^{k_i} SC_{ij}\right\}\right\} =$$

$$\left\{\{SC_{11}, SC_{12} \dots SC_{1k_1}\}, \{SC_{21}, SC_{22} \dots SC_{2k_2}\} \dots \{SC_{i1}, SC_{i2} \dots SC_{ik_n}\}\right\} \quad (4),$$

де SC_{ij} – j-ий критерій i-ої системи критеріїв.

Наприклад, з урахуванням [7, табл. 3], а також взявши до уваги, що ми, до прикладу, розглядаємо ОКІІ фінансового сектору [7, табл. 4] вираз (4) запишемо як:

$$SC = \left\{\bigcup_{i=1}^{n}\left\{\bigcup_{j=1}^{k_i} SC_{ij}\right\}\right\} =$$

$$\begin{Bmatrix}\{SC_{1.1}, SC_{1.2} \dots SC_{1.4}\}, \{SC_{2.1}, SC_{2.2} \dots SC_{2.31}\}, \{SC_{3.1}, SC_{3.2} \dots SC_{3.21}\}, \{SC_{4.1} \dots SC_{4.22}\}, \\ \{SC_{4.1}, SC_{4.2} \dots SC_{4.22}\}, \{SC_{5.1}, SC_{5.2} \dots SC_{5.11}\}, \{SC_{6.1}, SC_{6.2} \dots SC_{6.13}\}, \{SC_{7.1} \dots SC_{7.8}\}\end{Bmatrix} \quad (5)$$

Після введення систем та підмножин критеріїв розрахуємо первинний рівень кіберзахисту:

$$SA_{SC} = \frac{\sum_{i=1}^{n} SA_{SC_i}}{n} = \frac{\sum_{i=1}^{n} \frac{\sum_{j=1}^{k} SC_{ij}}{k}}{n} = \frac{SA_{SC_1} + SA_{SC_2} + SA_{SC_3} + SA_{SC_4} + SA_{SC_5} + SA_{SC_6} + SA_{SC_7}}{7} \quad (6),$$

де SA_{SC_i} – середнє арифметичне системи критеріїв SC_i.

Таким чином, значення, отримане, застосувавши вираз (6), є середнім арифметичним всіх систем критеріїв і відповідає первинному рівню кіберзахисту ОКІІ. Отриманий показник, завдяки перетворенню якісних характеристик стану кіберзахисту на бінарні показники («Так» = 1, «Ні» = 0) буде знаходитись у діапазоні від 0 до 1.

2. Для визначення інтегрального показника рівня кіберзахисту ОКІІ необхідно дані, отримані після застосування MAI [5], поєднати з показником первинного рівня кіберзахисту. Для цього застосуємо:

$$SA_{SC}^{w} = \sum_{i=1}^{n} w_i * SA_{SC_i} \quad (7),$$

де SA_{SC}^{w} – інтегральний показник рівня кіберзахисту ОКІІ;

w_i – ваговий коефіцієнт для i-ї системи критеріїв (*SCi).*

Підсумок етапу 4: завдяки використанню нормалізованих значень SA_{SC_i} та w_i кінцевий інтегральний показник SA_{SC}^{w} завжди знаходиться у стандартизованому діапазоні від 0 до 1. Це забезпечує можливість об'єктивного порівняння результатів оцінювання ОКІІ між собою, а також моніторингу динаміки рівня захисту протягом часових інтервалів.

Етап 5. Інтерпретація результатів та стратегічне планування

На цьому завершальному етапі забезпечується узгодження між математичним розрахунком інтегрального показника SA_{SC}^{w} та потребами управління кіберзахистом ОКІІ.

Першочергово отриманий показник SA_{SC}^{w} переводиться у п'ятирівневу шкалу інтерпретації результатів поточного рівня кіберзахисту ОКІІ [7, табл. 2].

Припустимо, що в ході дослідження SA_{SC}^{w} = 0,63. Таким чином, використавши шкалу, отримуємо результат – визначений/середній рівень кіберзахисту. Отриманий результат дає керівництву ОКІІ чітке розуміння фактичного рівня зрілості системи кіберзахисту ОКІІ.

На основі деталізації оцінок (SA_{SC_i} та їхніх вагових коефіцієнтів w_i) ідентифікуються найбільш критичні прогалини у захисті, які мають найбільший вплив на зниження інтегрального показника. Використання вагових коефіцієнтів w_i дозволяє пріоритезувати інвестиції та ресурси. Рекомендується спрямовувати зусилля на вдосконалення тих систем критеріїв, які мають низький рівень SA_{SC_i}, але високий ваговий коефіцієнт w_i.

Після цього розробляється стратегічний план (дорожня карта), спрямований на переведення ідентифікованих слабких місць в ІКС ОКІІ на вищий рівень зрілості протягом наступного звітного періоду.

Підсумок етапу 5: методологічним виходом цього етапу є звіт про оцінювання та план підвищення рівня кіберзахисту, що забезпечує зворотний зв'язок і закладає основи для наступного циклу оцінювання.

Апробація результатів дослідження

Апробацію розробленої методики розрахунку рівня кіберзахисту ОКІІ здійснено з метою підтвердження її практичної застосовності, достовірності та об'єктивності результатів.

Для розрахунку рівня кіберзахисту ОКІІ обрано дані, отримані від операторів критичної інфраструктури в рамках проведення у 2023 році Огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом. З метою кращої візуалізації результатів досліджено об'єкти паливно-енергетичного сектору критичної інфраструктури. З урахуванням вимог законодавства України щодо захисту інформації з обмеженим доступом, використано деперсоніфіковані дані.

1. Апробація методики розрахунку рівня кіберзахисту ОКІІ

Розглянемо детально кожен з етапів реалізації запропонованої методики розрахунку рівня кіберзахисту ОКІІ.

Етап 1. Підготовка та визначення обсягу оцінювання

1. Формування команди – до складу групи, що здійснювала розрахунок рівня кіберзахисту та визначала вагові коефіцієнти, увійшли провідні фахівці з кібербезпеки та представники керівництва ОКІІ. У якості зовнішнього експерта було запрошено фахівця Адміністрації Держспецзв'язку, як представника центрального органу виконавчої влади, що забезпечує формування та реалізацію державної політики у сфері кіберзахисту, та фахівця Державного центру кіберзахисту Держспецзв'язку, як представника оперативного підрозділу із забезпечення кіберзахисту.

2. Визначення середовища оцінювання – середовищами оцінювання на кожному ОКІІ було обрано загальні ІКС ОКІІ, які не включають ОТ-компоненти. Межі оцінювання зафіксовано в Схемному рішенні ІКС.

3. Актуалізація критеріїв оцінювання

У якості критеріїв відповідності до основних шести систем критеріїв було додано сьому, що включає питання, викладені у Таблиці 2. Таким чином, було визначено всі критерії відповідності, що відображені у виразі (3).

Таблиця 2

Представлення підмножин критеріїв системи «Секторальна складова (SE)»

Назва сектору критичної інфраструктури	Назва підмножини критеріїв	Критерії
Паливно-енергетичний сектор	SE_{PE} = «Секторальна складова паливно-енергетичного сектору»	PE_1 – «Чи проведено всебічну оцінку вашого ОКІ відповідно до наказу Міненерго від 10.09.2024 № 338 «Про затвердження Порядку огляду стану кібербезпеки паливно-енергетичного сектору критичної інфраструктури»?»; PE_2 – «Чи проведено оцінювання стану кібербезпеки електричних мереж, відповідно до наказу Міненерго від 05.08.2024 № 285 «Про затвердження Методики оцінювання стану кібербезпеки електричних мереж та практик кібербезпеки електричних мереж»?»; PE_3 – «Чи існують механізми обміну інформацією про кіберзагрози з іншими суб'єктами енергетичної галузі?»; PE_4 – «Чи може ваш ОКІ ефективно відновити нормальну роботу енергетичних систем після масштабної кібератаки, спрямованої на виведення з ладу критичної інфраструктури?»; PE_5 – «Чи проходить операційний персонал, що працює з ОТ-системами, спеціалізоване навчання з кібербезпеки, яке враховує особливості та ризики промислових систем?»

Таким чином, за підсумками етапу 1 Методики було сформовано експертну групу та розподілено її ролі, визначено середовище оцінювання та адаптовано систему критеріїв під вимоги специфічного паливно-енергетичного сектору критичної інфраструктури.

Етап 2. Збір первинних даних та оцінка відповідності

На цьому етапі експертною групою було здійснено анкетування профільного персоналу ОКІ для оцінки розуміння та усвідомленого застосування впроваджених заходів кіберзахисту, перевірено всі наявні на ОКІІ політики, плани, журнали та конфігураційні файли, а також за допомогою зовнішнього експерта з Державного центру кіберзахисту Держспецзв'язку здійснено тестування на проникнення, що дозволило зімітувати дії зловмисника для виявлення та експлуатації критичних вразливостей, таким чином забезпечивши об'єктивну оцінку функціональної відповідності.

Експертною групою за результатами інтерв'ювання, тестування та інспекції було формалізовано якісні характеристики по кожному критерію. Таким чином, кожному критерію було присвоєно бінарний показник:

«1» (Так) – критерій впроваджено та верифіковано;

«0» (Ні) – критерій не впроваджено або не підтверджено його операційну ефективність.

Етап 3. Визначення вагових коефіцієнтів

Експертною групою було сформовано нормалізовану матрицю розрахунку важливості систем критеріїв.

При побудові нормалізованої матриці розрахунку важливості систем критеріїв на основі MAI, залучення множини експертів вимагає застосування процедур агрегації індивідуальних суджень. Таким чином, кожен експерт сформував індивідуальну матрицю попарних порівнянь, які було перевірено на узгодження шляхом розрахунку відношення узгодженості (*CR*). Судження, для яких показник *CR* перевищував порогове значення ($CR \leq 0.1$), були переглянуті експертами для забезпечення логічної транзитивності.

Після отримання узгоджених матриць попарних порівнянь, було застосовано агрегацію індивідуальних суджень (з використанням виразу (1)). Таким чином, було отримано нормалізовану матрицю розрахунку важливості на основі суджень всіх експертів (Таблиця 3).

Таблиця 3

Нормалізована матриця розрахунку важливості

Важливість	SE	GV	ID	PR	DE	RS	RC
SE	1/23 = 0.0435	0.25/8.75 = 0.0286	0.333/3.582 = 0.0930	0.2/11.2 = 0.0179	0.25/5.416 = 0.0461	0.25/6.583 = 0.0380	0.5/12 = 0.0417
GV	4/23 = 0.1739	1/8.75 = 0.1143	0.333/3.582 = 0.0930	2/11.2 = 0.1786	1/5.416 = 0.1846	1/6.583 = 0.1519	0.5/12 = 0.0417
ID	3/23 = 0.1304	3/8.75 = 0.3429	1/3.582 = 0.2792	3/11.2 = 0.2679	2/5.416 = 0.3693	3/6.583 = 0.4557	4/12 = 0.3333
PR	5/23 = 0.2174	0.5/8.75 = 0.0571	0.333/3.582 = 0.0930	1/11.2 = 0.0893	0.5/5.416 = 0.0923	0.5/6.583 = 0.0759	1/12 = 0.0833
DE	4/23 = 0.1739	1/8.75 = 0.1143	0.5/3.582 = 0.1396	2/11.2 = 0.1786	1/5.416 = 0.1846	0.333/6.583 = 0.0506	3/12 = 0.2500
RS	4/23 = 0.1739	1/8.75 = 0.1143	0.333/3.582 = 0.0930	2/11.2 = 0.1786	0.333/5.416 = 0.0615	1/6.583 = 0.1519	2/12 = 0.1667
RC	2/23 = 0.0870	2/8.75 = 0.2286	0.25/3.582 = 0.0698	1/11.2 = 0.0893	0.333/5.416 = 0.0615	0.5/6.583 = 0.0759	1/12 = 0.0833

Після чого було застосовано вираз (2) і отримано вагові коефіцієнти:

w(SE) = 0.0441
w(GV) = 0.1340
w(ID) = 0.3112
w(PR) = 0.1012
w(DE) = 0.1559
w(RS) = 0.1357
w(RC) = 0.1136

Отримані вагові коефіцієнти було перевірено на узгодженість, визначено, що відношення узгодженості *CR*=0,05, що є меншим за допустимий поріг (0,1).

Етап 4. Кількісний розрахунок інтегрального показника рівня кіберзахисту

1. Першочергово розраховано первинний рівень кіберзахисту. Для цього здійснено розрахунок виразу (5) з урахуванням визначених критеріїв (для системи критеріїв SE = «Секторальна складова» - Табл. 2, для систем критеріїв GV = «Управління», ID = «Ідентифікація ризиків кібербезпеки», PR = «Кіберзахист», DE = «Виявлення кіберінцидентів», RS = «Реагування на кіберінциденти», RC = «Відновлення стану кібербезпеки» - [Табл. 3, 7]).

$$SC = \left\{ \bigcup_{i=1}^{n} \left\{ \bigcup_{j=1}^{k_i} SC_{ij} \right\} \right\} =$$

$$\left\{\begin{matrix}\{SC_{1.1}, SC_{1.2} \dots SC_{1.5}\}, \{SC_{2.1}, SC_{2.2} \dots SC_{2.31}\}, \{SC_{3.1}, SC_{3.2} \dots SC_{3.21}\}, \{SC_{4.1} \dots SC_{4.22}\}, \\ \{SC_{5.1}, SC_{5.2} \dots SC_{5.11}\}, \{SC_{6.1}, SC_{6.2} \dots SC_{6.13}\}, \{SC_{7.1} \dots SC_{7.8}\}\end{matrix}\right\} \quad (8)$$

Після цього розраховано первинний рівень кіберзахисту, використавши (6):

$$SA_{SC} = \frac{SA_{SC_1} + SA_{SC_2} + SA_{SC_3} + SA_{SC_4} + SA_{SC_5} + SA_{SC_6} + SA_{SC_7}}{7}$$
$$= \frac{0{,}890 + 0{,}310 + 0{,}440 + 0{,}920 + 0{,}300 + 0{,}750 + 0{,}710}{7} = \frac{4{,}320}{7}$$
$$= 0{,}617$$

Таким чином, отримане значення є середнім арифметичним всіх систем критеріїв і відповідає первинному рівню кіберзахисту ОКІІ.

2. Розраховано інтегральний показник рівня кіберзахисту ОКІІ. Для цього застосовано вираз (7):

$$SA_{SC}^{w} = \sum_{i=1}^{n} w_i * SA_{SC_i}$$
$$= (0{,}0441 * 0{,}890) + (0{,}1340 * 0{,}310) + (0{,}3112 * 0{,}440) + (0{,}1012 * 0{,}920)$$
$$+ (0{,}1559 * 0{,}300) + (0{,}1357 * 0{,}750) + (0{,}1136 * 0{,}710) = 0{,}54$$

Етап 5. Інтерпретація результатів та стратегічне планування

Переводимо отриманий показник 0,54 у п’ятирівневу шкалу інтерпретації результатів поточного рівня кіберзахисту ОКІІ [7, табл. 2] і отримуємо результат – визначений/середній рівень кіберзахисту.

На основі деталізації оцінок ідентифіковано найбільш критичні прогалини у захисті.

Найвищу вагу має система критеріїв «Ідентифікація ризиків кібербезпеки (ID)», при цьому її первинний рівень кіберзахисту становить 0,44.

Найнижчий первинний рівень кіберзахисту (0,3) зафіксовано у системі критеріїв «Виявлення кіберінцидентів (DE)». Хоча вага в цій системі критеріїв не є критичною, такий показник свідчить про наявність системних проблем з реалізацією відповідних заходів.

Ще однією слабкою ланкою є система критеріїв «Управління (GV)» з оцінкою первинного рівня кіберзахисту у 0,31 і вагою 0,134, що вказує на початковий рівень зрілості процесів управління ризиками.

Таким чином, необхідно першочергово звернути увагу керівництва ОКІІ на покращення критеріїв в цих системах.

На завершення етапу 5 експертною групою розробляється дорожня карта, спрямована на покращення виявлених прогалин і переведення ідентифікованих слабких місць в ІКС ОКІІ на вищий рівень зрілості.

Практична апробація розробленої гібридної методики на базі об’єктів паливно-енергетичного сектору підтвердила її функціональну придатність. Результати засвідчили, що методика забезпечує послідовний, алгоритмізований та відтворюваний процес оцінювання. Чіткий розподіл на етапи (від збору первинних даних до інтегрального розрахунку) мінімізує процедурні помилки. Використання MAI для визначення вагових коефіцієнтів w_i дозволило трансформувати суб’єктивні експертні судження у математично узгоджені показники ваг. Перевірка відношення узгодженості доводить логічну транзитивність оцінок та забезпечує ризик-орієнтований підхід, де

пріоритет надається найбільш вагомим системам критеріїв. Отриманий інтегральний показник слугує кількісною метрикою для вищого керівництва. Деталізація результатів дозволяє ідентифікувати слабкі місця не лише за абсолютним значенням успішності, а й за ступенем їхнього впливу на загальну кіберстійкість ІКС.

Перевагами розробленої методики є висока роздільна здатність, оскільки методика надає точне цифрове значення, що дозволяє фіксувати навіть незначні зміни стану кібербезпеки в динаміці; поєднання об'єктивного інструментального контролю з експертними зважуваннями дозволяє забезпечити збалансовану оцінку, яка враховує як технічний стан, так і стратегічну важливість процесів; можливість інтеграції додаткових підмножин критеріїв робить методику гнучкою до специфічних вимог законодавства або галузевих стандартів.

Водночас в розробленій методиці наявні певні обмеження. По-перше, залежність від компетентності експертної групи, оскільки попри використання MAI для контролю узгодженості, початкове формування матриць попарних порівнянь залишається чутливим до рівня кваліфікації залучених фахівців. По-друге, ефективність методики безпосередньо залежить від достовірності вхідної інформації (приховування інцидентів або надання неповних конфігураційних журналів може призвести до штучного завищення інтегрального показника).

2. Експериментальне дослідження методики

З метою всебічного аналізу та порівняння існуючих підходів до оцінки рівня кіберзахисту ОКІІ паливно-енергетичного сектору, було здійснено послідовну оцінку загального стану кіберзахисту трьох ОКІІ (ОКІІ 1, ОКІІ 2 та ОКІІ 3) за допомогою трьох різних програмних забезпечень:

1. «Інструмент оцінки кібербезпеки (CSET®) / The Cyber Security Evaluation Tool (CSET®)» [33]. Це програмне забезпечення є продуктом Управління кібербезпеки та інфраструктурної безпеки США (Cybersecurity & Infrastructure Security Agency, CISA) та було адаптовано ДержНДІ технологій кібербезпеки для застосування в українських реаліях.
2. «Інструмент самооцінки». Даний інструмент розроблений Національним інститутом стандартів і технологій США (National Institute of Standards and Technology, NIST) і також адаптований ДержНДІ технологій кібербезпеки.
3. Авторське програмне забезпечення. Це інструмент, розроблений безпосередньо в межах даного експериментального дослідження, що втілює запропоновану модель розрахунку рівня кіберзахисту.

Отримані результати, представлені у вигляді графіків, демонструють відмінності та спільні риси в оцінках, наданих кожним інструментом. Це дозволяє порівняти їхню чутливість, повноту охоплення та інтерпретацію рівня кіберзахисту для конкретних ОКІІ.

На рисунках 1-3 представлено результати оцінки рівня кіберзахисту для ОКІІ 1, ОКІІ 2 та ОКІІ 3, отримані за допомогою ПЗ CSET®.

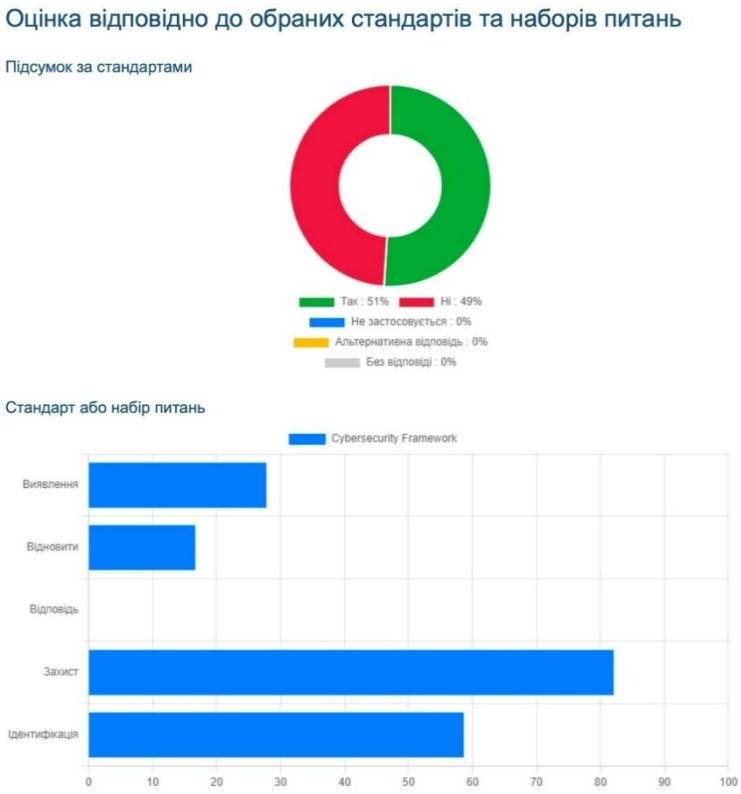

Рис. 1. Результати оцінки рівня кіберзахисту ОКІІ 1 за допомогою CSET®

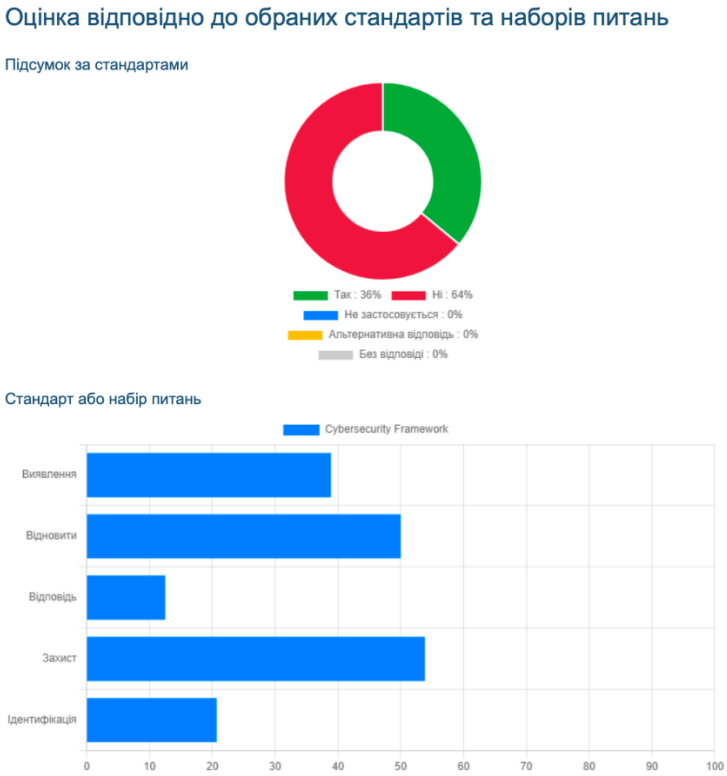

Рис. 2. Результати оцінки рівня кіберзахисту ОКІІ 2 за допомогою CSET®

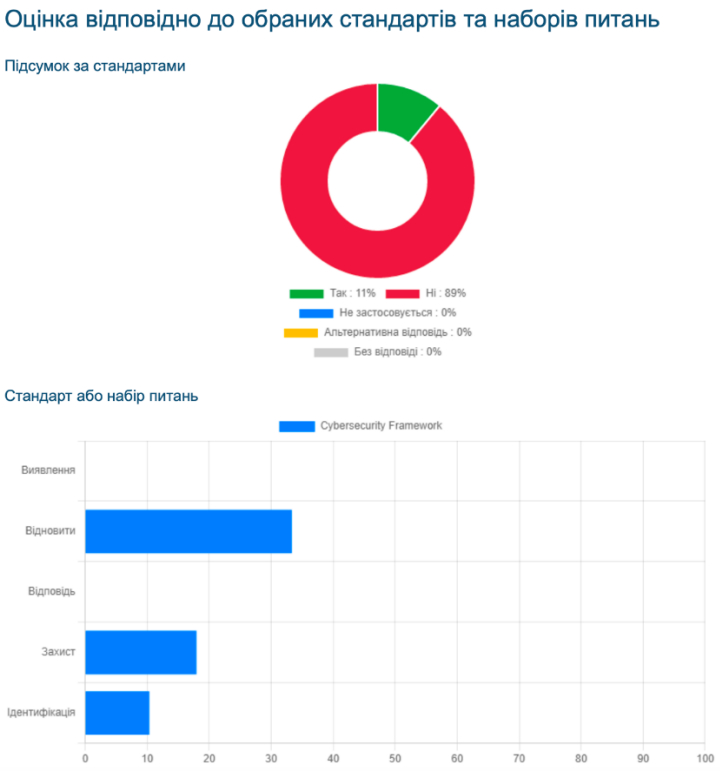

Рис. 3. Результати оцінки рівня кіберзахисту ОКІІ 3 за допомогою CSET®

На рисунках 4-6 представлено результати оцінки рівня кіберзахисту для ОКІІ 1, ОКІІ 2 та ОКІІ 3, отримані за допомогою «Інструменту самооцінки» NIST.

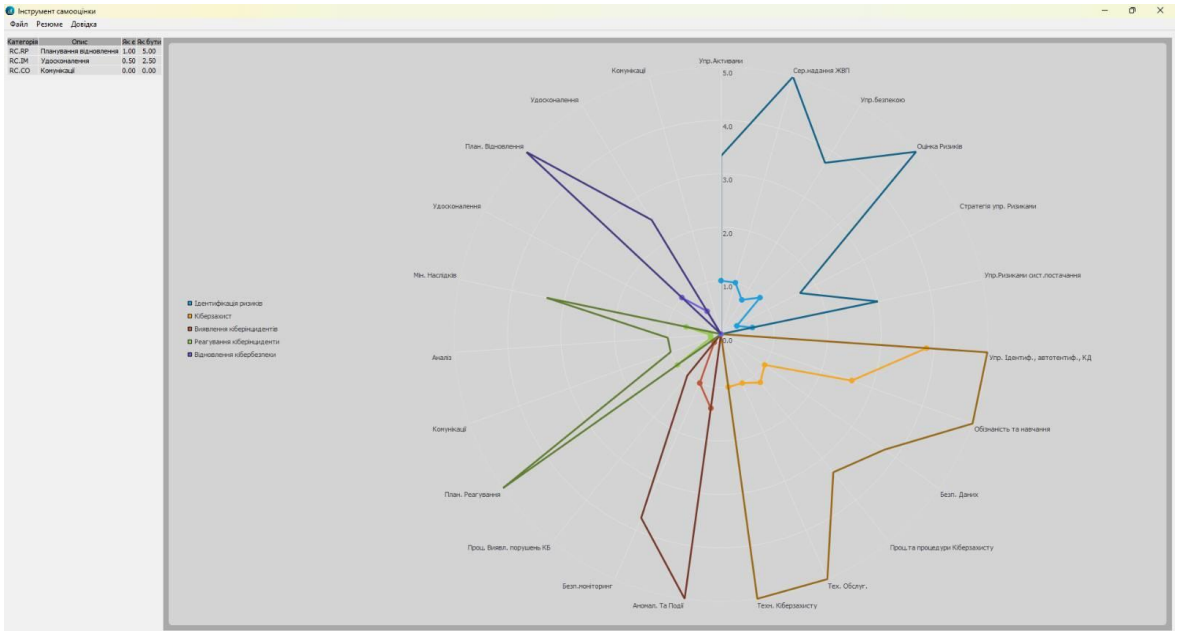

Рис. 4. Результати оцінки рівня кіберзахисту ОКІІ 1 за допомогою «Інструменту самооцінки» NIST

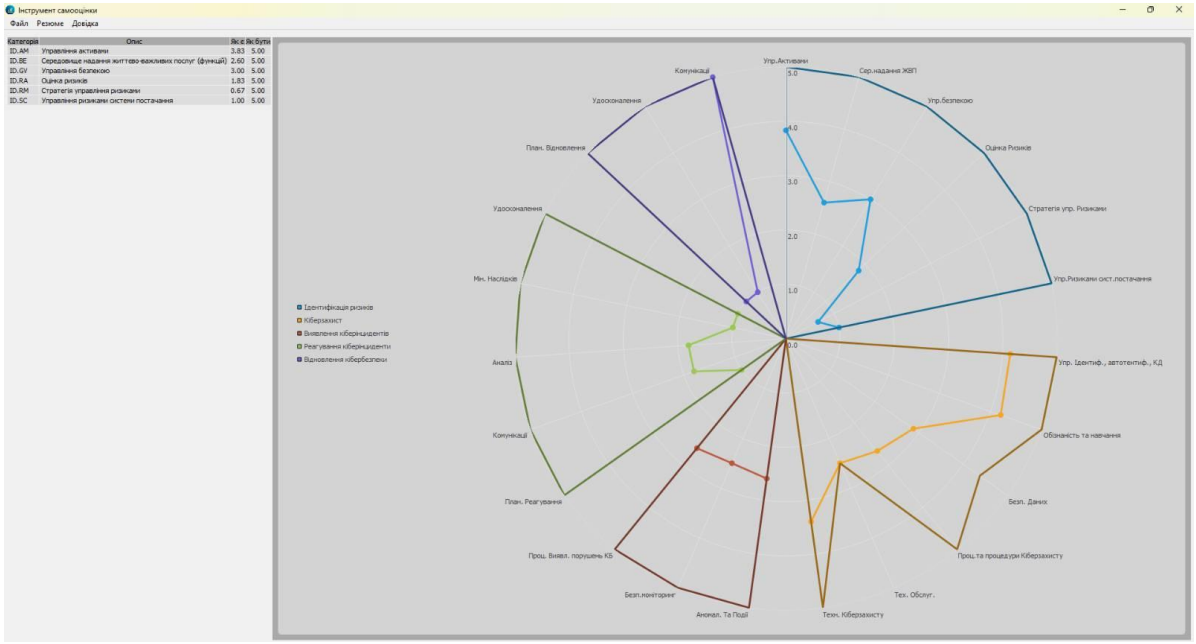

Рис. 5. Результати оцінки рівня кіберзахисту ОКІІ 2 за допомогою «Інструменту самооцінки» NIST

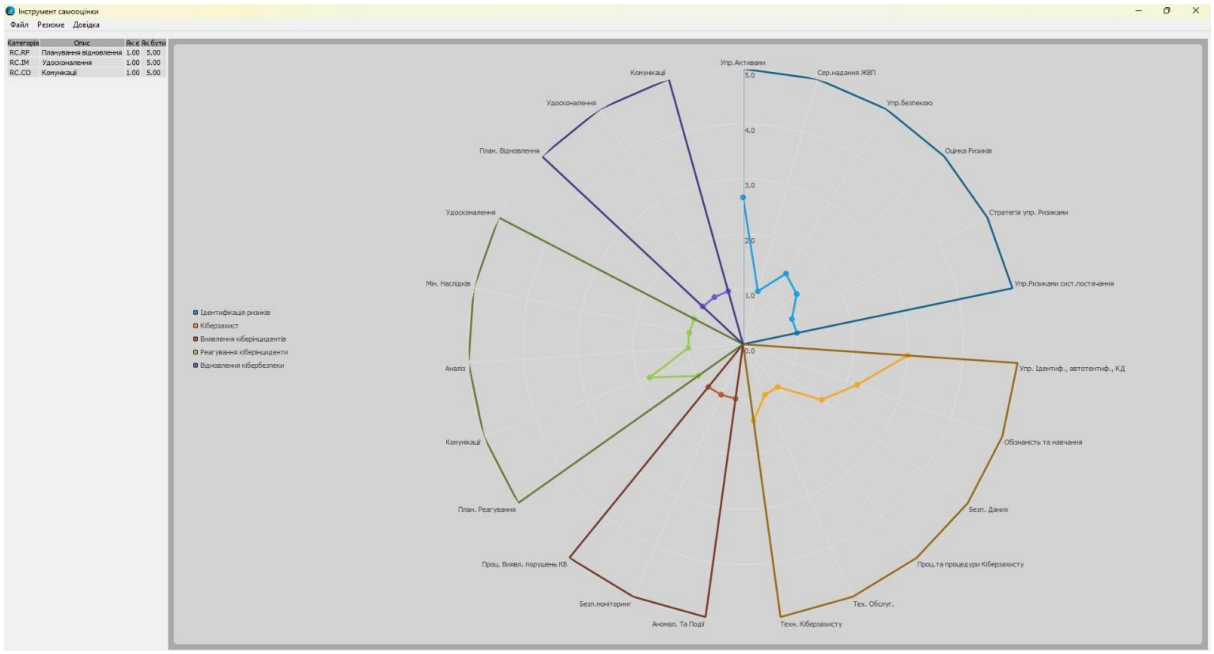

Рис. 6. Результати оцінки рівня кіберзахисту ОКІІ 3 за допомогою «Інструменту самооцінки» NIST

На рисунках 7-9 представлено результати оцінки первинного рівня кіберзахисту для ОКІІ 1, ОКІІ 2 та ОКІІ 3, отримані за допомогою авторського програмного забезпечення.

ISSN 2663 - 4023

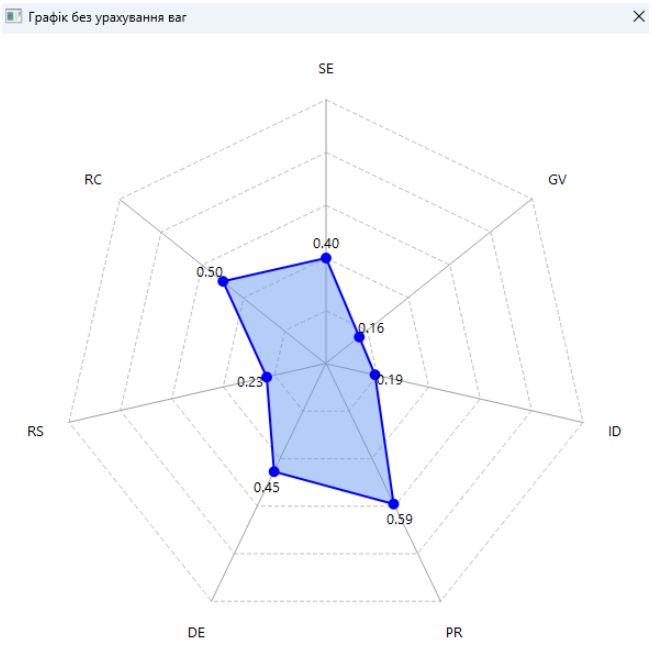

Рис. 7. Результати розрахунку первинного рівня кіберзахисту ОКІІ 1 (без врахування вагових коефіцієнтів)

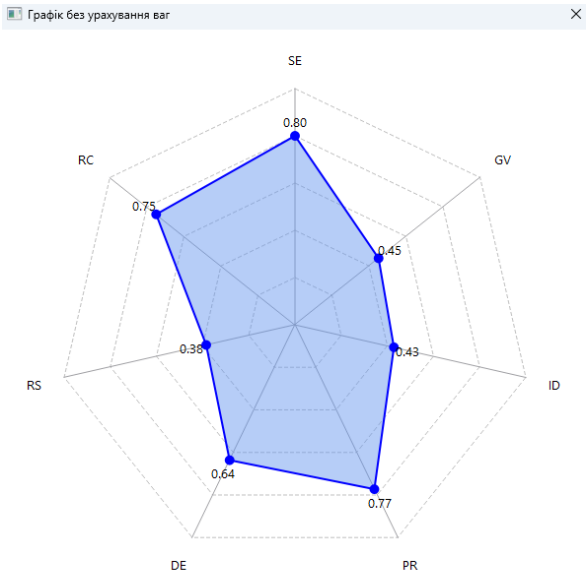

Рис. 8. Результати розрахунку первинного рівня кіберзахисту ОКІІ 2 (без врахування вагових коефіцієнтів)

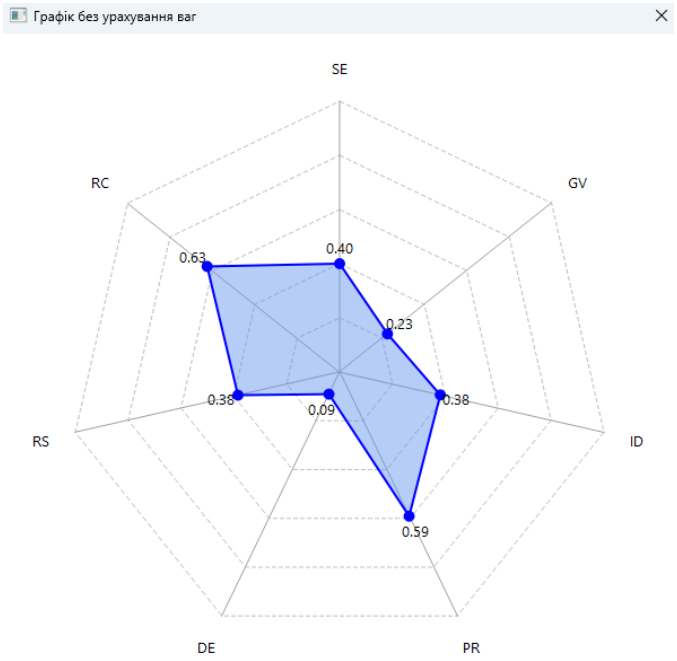

Рис. 9. Результати розрахунку первинного рівня кіберзахисту ОКІІ 3 (без врахування вагових коефіцієнтів)

На рисунках 10-12 представлено результати оцінки інтегрального рівня кіберзахисту для ОКІІ 1, ОКІІ 2 та ОКІІ 3, отримані за допомогою авторського програмного забезпечення.

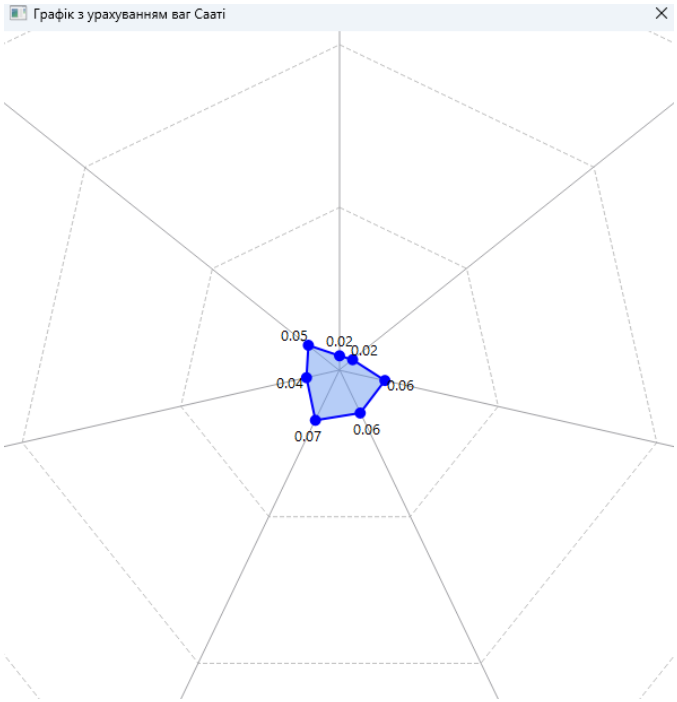

Рис. 10. Результати оцінки інтегрального рівня кіберзахисту ОКІІ 1 за допомогою авторського ПЗ

Загальний рівень кіберзахисту ОКІІ 1 – 0,31, що відповідно до [7, табл. 2] відповідає показнику – в процесі формування / низький рівень.

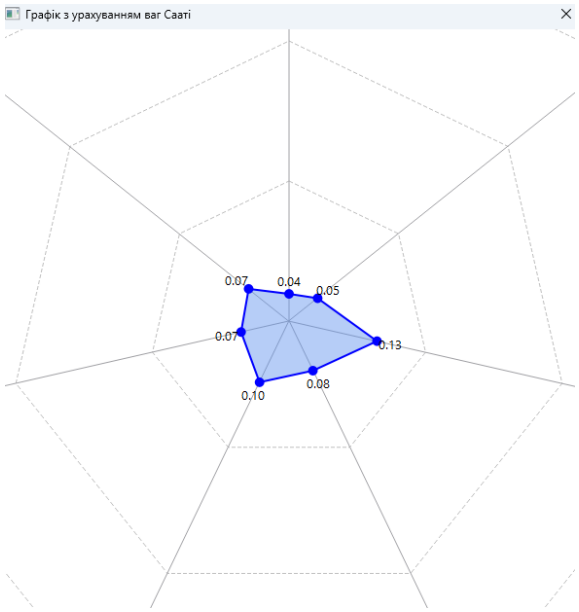

Рис. 11. Результати оцінки інтегрального рівня кіберзахисту ОКІІ 2 за допомогою авторського ПЗ

Загальний рівень кіберзахисту ОКІІ 2 – 0,54, що відповідно до [7, табл. 2] відповідає показнику – визначений / середній рівень.

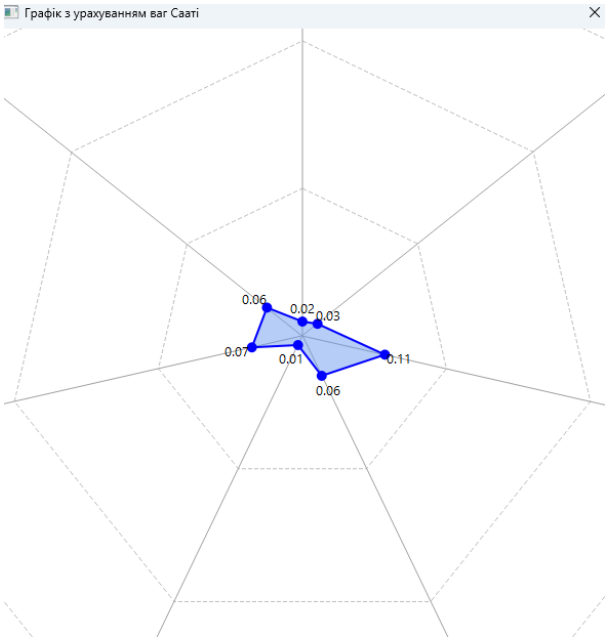

Рис. 12. Результати оцінки інтегрального рівня кіберзахисту ОКІІ 3 за допомогою авторського ПЗ

Загальний рівень кіберзахисту ОКІІ 3 – 0,37, що відповідно до [7, табл. 2] відповідає показнику – в процесі формування / низький рівень.

Таким чином, за результатами проведеного аналізу встановлено переваги авторського програмного забезпечення над інструментами, розробленими NIST та CISA, за наступними параметрами:

1) Повна адаптація до українського законодавства, що забезпечує релевантність оцінки нормативно-правовому полю України.

2) Розширений набір груп порівняння (критеріїв), що дозволяє отримати більш деталізовану та всеохоплюючу оцінку.

3) Безпосереднє врахування секторальної специфіки ОКІ, що підвищує точність оцінки для паливно-енергетичного сектору.

4) Інтегрована можливість внесення користувачем вагових коефіцієнтів, що дозволяє налаштовувати модель під конкретні пріоритети та особливості оцінюваного об'єкта.

Водночас, слід зазначити, що поточна версія авторського ПЗ фокусується виключно на розрахунку фактичного (поточного) рівня кіберзахисту ОКІІ, не передбачаючи функціоналу для визначення бажаного (цільового) рівня.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У роботі вирішено актуальне науково-практичне завдання щодо створення уніфікованого інструменту для об’єктивного розрахунку рівня кіберзахисту ОКІІ в умовах інтенсифікації кіберзагроз. Було розроблено гібридну методику кількісного розрахунку інтегрального рівня кіберзахисту ОКІІ, яка базується на поєднанні трьох функціональних підходів: оцінки відповідності нормативним вимогам, визначення рівня зрілості процесів та застосування ризик-орієнтованого зважування за допомогою MAI. Крім того, було експериментально підтверджено переваги авторського підходу над міжнародними аналогами, зокрема у частині повної адаптації до українського законодавчого поля, врахування секторальної специфіки та можливості динамічного налаштування пріоритетів через вагові коефіцієнти. Запропонована методика та розроблене на її основі програмне забезпечення можуть бути використані як операторами критичної інфраструктури, так і регуляторами та суб’єктами забезпечення кібербезпеки. Головною перевагою розробленої методики є здатність перетворювати якісні характеристики на точні цифрові показники, що дозволяє відстежувати прогрес. Разом з тим, методика має певні обмеження: вона залишається чутливою до рівня експертної кваліфікації при попарному порівнянні критеріїв та вимагає високого ступеня достовірності вхідних даних для уникнення штучного завищення результатів.

Продовженням даного дослідження стане розширення функціональних можливостей методики, зокрема розробка математичного апарату для автоматизованого визначення бажаного (цільового) рівня кіберзахисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Апарат Ради національної безпеки і оборони України. (2025). *Річний аналітичний огляд (жовтень 2023 – вересень 2024)*. https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20250109/Year%20in%20review_UKR_upd.pdf
2. State Service of Special Communications and Information Protection of Ukraine. (2025). *WAR AND CYBER: Three years of struggle and lessons for global security. Analytical report*. https://cip.gov.ua/services/cm/api/attachment/download?id=69131

3. Державна служба спеціального зв'язку та захисту інформації України. (2025). *Російські кібероперації: H1 '2025*. https://cip.gov.ua/services/cm/api/attachment/download?id=71278
4. Державна служба спеціального зв'язку та захисту інформації України. (2024). *Російські кібероперації: H2 '2024*. https://cip.gov.ua/services/cm/api/attachment/download?id=68769
5. Юдіна, Д. (2025). Метод розрахунку рівня кіберзахисту об'єктів критичної інформаційної інфраструктури. *Кібербезпека: освіта, наука, техніка*, *2*(30), 473–487. https://doi.org/10.28925/2663-4023.2025.30.986
6. Юдіна, Д. (2025). Модель розрахунку рівня кіберзахисту об'єктів критичної інфраструктури. *Кібербезпека: освіта, наука, техніка*, *4*(28), 586–598. https://doi.org/10.28925/2663-4023.2025.28.829
7. Юдіна, Д. (2025). Модифікація моделі розрахунку рівня кіберзахисту об'єктів критичної інформаційної інфраструктури. *Кібербезпека: освіта, наука, техніка*, *1*(29), 818–836. https://doi.org/10.28925/2663-4023.2025.29.943
8. CMMI Institute. (2023). *Capability Maturity Model Integration (CMMI) for Development, Version 3.0*. https://cmmiinstitute.com/cmmi
9. U.S. Department of Energy. (2022). *Cybersecurity Capability Maturity Model (C2M2), version 2.1*. https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf
10. Humphrey, W. S. (1989). *Managing the software process*. Addison-Wesley, MA.
11. Klein, M., & Masi, M. (1993). The Capability Maturity Model, Version 1.1. *IEEE Software*.
12. Khudyntsev, M., & Palazhchenko, I. (2024). Cybersecurity maturity models for cybersecurity assessment in critical infrastructure. *Екологічна безпека та природокористування*, *4*(52).
13. National Institute of Standards and Technology. (2024). *NIST Cybersecurity Framework, version 2.0*. https://www.nist.gov/cyberframework
14. ISO/IEC. (2022). *ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks*.
15. Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk management guide for Information Technology systems* (NIST Special Publication 800-30). National Institute of Standards and Technology.
16. Freund, J., & Jones, J. (2014). *Measuring and managing information risk: A FAIR approach*. Butterworth-Heinemann.
17. Patton, M. Q. (2002). *Qualitative research and evaluation methods* (3rd ed.). Sage Publications.
18. Alali, M., Almogren, A., Hassan, M. M., Razzak, I., & Alelaiwi, A. (2018). Improving risk assessment model of cyber security using fuzzy logic inference system. *Computers & Security*, *74*, 323–339.
19. Гончар, С. Ф. (2019). *Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури: монографія*. Альфа Реклама.
20. ISO/IEC. (2022). *ISO/IEC 27001:2022. Information technology — Security techniques — Information security management systems — Requirements*.
21. Шиповський, В. (2023). Система показників оцінювання кіберстійкості інформаційних систем об'єктів критичної інфраструктури. *Захист інформації*, *1*(25), 37–45. https://doi.org/10.18372/2410-7840.25.17597
22. European Union Agency for Cybersecurity (ENISA). (2021). *EU cybersecurity certification framework – Methodology for sectoral cybersecurity assessments*. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20SCSA%20Methodology.pdf
23. National Institute of Standards and Technology. (2014). *Assessing security and privacy controls in federal information systems and organizations: Building effective assessment plans* (NIST Special Publication 800-53A, Rev. 4).
24. National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations* (NIST Special Publication 800-53, Rev. 5).
25. ДП «УкрНДНЦ». (2019). *Настанови щодо проведення аудитів систем управління* (ДСТУ ISO 19011:2019; ISO 19011:2018, IDT).
26. ДП «УкрНДНЦ». (2023). *Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги* (ДСТУ ISO/IEC 27001:2023; ISO/IEC 27001:2022, IDT).
27. The FAIR Institute. (n.d.). *What is FAIR? Factor Analysis of Information Risk*. https://www.fairinstitute.org/fair-risk-management
28. PCI Security Standards Council. (2022). *Payment Card Industry Data Security Standard (PCI DSS) Requirement and Assessment Procedures, Version 4.0*.
29. CMMI Institute. (n.d.). *About CMMI Integration*. https://cmmiinstitute.com/cmmi

30. Кабінет Міністрів України. (2021). *Постанова від 29.12.2021 № 1426 «Про затвердження Положення про організаційно-технічну модель кіберзахисту»*. https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF
31. Адміністрація Державної служби спеціального зв'язку та захисту інформації України. (2025). *Наказ від 30.01.2025 № 54 «Про затвердження Базових заходів з кіберзахисту та Методичних рекомендацій щодо здійснення базових заходів з кіберзахисту»*.
32. Vargas, L. L., & Saaty, T. L. (2001). *Models, methods, concepts & applications of the Analytic Hierarchy Process*. Kluwer Academic.
33. Cybersecurity & Infrastructure Security Agency (CISA). (n.d.). *The Cyber Security Evaluation Tool (CSET)*. https://csirt.csi.cip.gov.ua/uk/pages/cset

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023

Yudina Diana
PhD student of the Faculty of Computer Science and Technology
State University "Kyiv Aviation Institute", Kyiv, Ukraine
ORCID: 0000-0002-1277-8771
diana.yudina22@gmail.com

Yudin Dmytro
Student of the Faculty of Applied Mathematics
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
ORCID: 0009-0002-9946-494X
yudin.dmytro@lll.kpi.ua

METHODOLOGY FOR CALCULATING THE LEVEL OF CYBERSECURITY OF CRITICAL INFORMATION INFRASTRUCTURE FACILITIES

Abstract. The article addresses a pressing scientific and practical challenge: the creation of a unified toolkit for the quantitative assessment of the security status of critical information infrastructure objects (CIIO). The relevance of the study is substantiated by an unprecedented increase in the number of cyberattacks (by 74% in 2025 compared to 2024) and a shift in their vector toward operational technologies. The research emphasizes the lack of transparent tools in Ukraine that would allow operators to objectively evaluate their posture and enable regulators to perform effective monitoring. Existing methodologies are grouped according to three characteristics: procedural, verification, and analytical. It is determined that none of them are fully universal under the conditions of full-scale war, necessitating the development of a hybrid approach. The research results present a developed five-stage methodology that transforms a multi-criteria theoretical method into a detailed algorithm. The methodology integrates seven systems of criteria: Governance (GV), Cybersecurity Risk Identification (ID), Cyber Protection (PR), Cyber Incident Detection (DE), Cyber Incident Response (RS), Cybersecurity Recovery (RC), and a Sectoral Component (SE). To incorporate a risk-oriented approach, the Analytic Hierarchy Process (AHP) is applied, allowing for the determination of weighting coefficients for each protection direction through pairwise comparisons. The data collection procedure is described through a three-component approach: documentation inspection, interviewing, and technical testing, which minimizes evaluation subjectivity. Furthermore, the results of the practical application of the methodology at fuel and energy sector facilities are provided. A comparative analysis of the developed proprietary software against two international analogs is conducted, proving the superior accuracy of the author's methodology due to its adaptation to national legislation and the possibility of individual weight adjustment. The study identifies that the most critical gaps are systems with high weighting coefficients and low implementation levels. The practical value of the work lies in creating a roadmap for CIIF management regarding the prioritization of security investments. Prospects for further research are aimed at automating the determination of the target cyber protection level for conducting gap analysis.

Keywords: cybersecurity; critical infrastructure; critical infrastructure facilities; critical information infrastructure facilities; method for calculation; methodology for calculation; weighting factors.

REFERENCES

1. Apparatus of the National Security and Defense Council of Ukraine. (2025). *Annual analytical review (October 2023 – September 2024)*. https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20250109/Year%20in%20review_UKR_upd.pdf
2. State Service of Special Communications and Information Protection of Ukraine. (2025). *WAR AND CYBER: Three years of struggle and lessons for global security. Analytical report*. https://cip.gov.ua/services/cm/api/attachment/download?id=69131

3. State Service of Special Communications and Information Protection of Ukraine. (2025). *Russian cyber operations: H1 '2025*. https://cip.gov.ua/services/cm/api/attachment/download?id=71278
4. State Service of Special Communications and Information Protection of Ukraine. (2024). *Russian cyber operations: H2 '2024*. https://cip.gov.ua/services/cm/api/attachment/download?id=68769
5. Yudina, D. (2025). Method for calculating the level of cyber protection of critical information infrastructure objects. *Cybersecurity: Education, Science, Technique*, 2(30), 473–487. https://doi.org/10.28925/2663-4023.2025.30.986
6. Yudina, D. (2025). Model for calculating the level of cyber protection of critical infrastructure objects. *Cybersecurity: Education, Science, Technique*, 4(28), 586–598. https://doi.org/10.28925/2663-4023.2025.28.829
7. Yudina, D. (2025). Modification of the model for calculating the level of cyber protection of critical information infrastructure objects. *Cybersecurity: Education, Science, Technique*, 1(29), 818–836. https://doi.org/10.28925/2663-4023.2025.29.943
8. CMMI Institute. (2023). *Capability Maturity Model Integration (CMMI) for Development, Version 3.0*. https://cmmiinstitute.com/cmmi
9. U.S. Department of Energy. (2022). *Cybersecurity Capability Maturity Model (C2M2), version 2.1*. https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf
10. Humphrey, W. S. (1989). *Managing the software process*. Addison-Wesley, MA.
11. Klein, M., & Masi, M. (1993). The Capability Maturity Model, Version 1.1. *IEEE Software*.
12. Khudyntsev, M., & Palazhchenko, I. (2024). Cybersecurity maturity models for cybersecurity assessment in critical infrastructure. *Environmental Safety and Natural Resources*, 4(52).
13. National Institute of Standards and Technology. (2024). *NIST Cybersecurity Framework, version 2.0*. https://www.nist.gov/cyberframework
14. ISO/IEC. (2022). *ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks*.
15. Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk management guide for Information Technology systems* (NIST Special Publication 800-30). National Institute of Standards and Technology.
16. Freund, J., & Jones, J. (2014). *Measuring and managing information risk: A FAIR approach*. Butterworth-Heinemann.
17. Patton, M. Q. (2002). *Qualitative research and evaluation methods* (3rd ed.). Sage Publications.
18. Alali, M., Almogren, A., Hassan, M. M., Razzak, I., & Alelaiwi, A. (2018). Improving risk assessment model of cyber security using fuzzy logic inference system. *Computers & Security*, 74, 323–339.
19. Honchar, S. F. (2019). *Risk assessment of cybersecurity of information systems of critical infrastructure objects: Monograph*. Alpha Reklama.
20. ISO/IEC. (2022). *ISO/IEC 27001:2022. Information technology — Security techniques — Information security management systems — Requirements*.
21. Shipovskyi, V. (2023). System of indicators for evaluating the cyber resilience of information systems of critical infrastructure objects. *Information Security*, 1(25), 37–45. https://doi.org/10.18372/2410-7840.25.17597
22. European Union Agency for Cybersecurity (ENISA). (2021). *EU cybersecurity certification framework – Methodology for sectoral cybersecurity assessments*. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20SCSA%20Methodology.pdf
23. National Institute of Standards and Technology. (2014). *Assessing security and privacy controls in federal information systems and organizations: Building effective assessment plans* (NIST Special Publication 800-53A, Rev. 4).
24. National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations* (NIST Special Publication 800-53, Rev. 5).
25. SE «Ukrmetrteststandart». (2019). *Guidelines for auditing management systems* (DSTU ISO 19011:2019; ISO 19011:2018, IDT).
26. SE «Ukrmetrteststandart». (2023). *Information security, cybersecurity and privacy protection. Information security management systems. Requirements* (DSTU ISO/IEC 27001:2023; ISO/IEC 27001:2022, IDT).
27. The FAIR Institute. (n.d.). *What is FAIR? Factor Analysis of Information Risk*. https://www.fairinstitute.org/fair-risk-management
28. PCI Security Standards Council. (2022). *Payment Card Industry Data Security Standard (PCI DSS) Requirement and Assessment Procedures, Version 4.0*.
29. CMMI Institute. (n.d.). *About CMMI Integration*. https://cmmiinstitute.com/cmmi

30. Cabinet of Ministers of Ukraine. (2021). *Resolution No. 1426 of December 29, 2021 «On approval of the Regulation on the organizational and technical model of cyber protection»*. https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF
31. Administration of the State Service of Special Communications and Information Protection of Ukraine. (2025). *Order No. 54 of January 30, 2025 «On approval of Basic cyber protection measures and Methodological recommendations for the implementation of basic cyber protection measures»*.
32. Vargas, L. L., & Saaty, T. L. (2001). *Models, methods, concepts & applications of the Analytic Hierarchy Process*. Kluwer Academic.
33. Cybersecurity & Infrastructure Security Agency (CISA). (n.d.). *The Cyber Security Evaluation Tool (CSET)*. https://csirt.csi.cip.gov.ua/uk/pages/cset

This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.