КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue
DOI 10.28925/2663-4023.2025.30.986
УДК 004.056.5

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

МЕТОД РОЗРАХУНКУ РІВНЯ КІБЕРЗАХИСТУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Анотація. У сучасному світі, де динамічно зростає кількість та складність кіберзагроз, особливо спрямованих на стратегічні активи держави, виникає гостра необхідність у розробленні ефективних, гнучких та адаптивних механізмів оцінювання поточного рівня кіберзахисту. З огляду на цю потребу, було проведено аналіз існуючих підходів до оцінювання рівня кіберзахисту. Серед них виділяють моделі, засновані на зрілості, ризиках та відповідності. Результати аналізу встановили, що жоден з цих підходів не є повністю універсальним або достатнім для комплексної оцінки об'єктів критичної інформаційної інфраструктури в умовах національного законодавчого поля. Зокрема, підходи, що базуються лише на відповідності, можуть не враховувати реальні ризики, а підходи, що базуються на зрілості, часто є надто суб'єктивними. Для усунення цих системних недоліків було запропоновано гібридний підхід. Цей підхід забезпечує інтеграцію найкращих характеристик попередніх моделей, поєднуючи об'єктивність перевірки відповідності, гнучкість та орієнтованість на процес оцінки зрілості, пріоритезацію, що ґрунтується на оцінці ризиків. На основі гібридного підходу було розроблено метод розрахунку рівня кіберзахисту об'єктів критичної інформаційної інфраструктури. Компонентом цього методу є впровадження вагових коефіцієнтів для різних систем критеріїв. Для визначення цих вагових коефіцієнтів, що мають забезпечити об'єктивне відображення експертного знання, було обрано метод аналізу ієрархій. Запропонований метод дозволяє трансформувати якісні характеристики (наприклад, бінарні відповіді «так/ні») у єдиний кількісний показник. Цей показник розраховується в стандартизованому діапазоні від 0 до 1, що полегшує порівняння та моніторинг. Отримане числове значення далі інтерпретується за п'ятирівневою шкалою зрілості (від "Початковий" до "Оптимізований"), що надає чітке уявлення про необхідні кроки для покращення. Таким чином, розроблений метод є ієрархічним, багатокритеріальним та адаптивним до актуального українського законодавства у сфері кіберзахисту та кібербезпеки. В подальших дослідженнях планується проведення експериментального дослідження та верифікація методу на трьох об'єктах критичної інфраструктури паливно-енергетичного сектору, а також порівняння отриманих результатів за допомогою авторського програмного забезпечення та двох інших інструментів.

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

ВСТУП

У сучасному світі, що характеризується стрімкою цифровізацією та посиленою залежністю від інформаційних технологій, кіберзахист критичної інформаційної інфраструктури набуває статусу ключового пріоритету для національної безпеки та економічної стабільності. Об'єкти критичної інформаційної інфраструктури (ОКІІ), що включають енергетичні, транспортні, фінансові системи та мережі водопостачання, є основою для функціонування суспільства. Постійно зростаюча кількість і складність

кіберзагроз [1], [2], здатних завдати не лише значних економічних збитків, а й спричинити фізичну шкоду та дестабілізувати функціонування держави, вимагає розроблення ефективних та адаптивних механізмів оцінювання рівня кіберзахисту.

Постановка проблеми. Актуальним науковим і практичним завданням є створення обґрунтованого методу розрахунку рівня кіберзахисту ОКІІ. Існуючі підходи, що ґрунтуються на зрілості, ризиках чи відповідності стандартам, мають певні обмеження, які роблять їх недостатньо універсальними для застосування в динамічних умовах сучасних кіберзагроз. Тому, для забезпечення комплексної та об'єктивної оцінки, необхідним є розроблення гібридного підходу, що поєднує переваги кожного з них і враховує специфічні реалії ОКІІ в Україні.

Аналіз останніх досліджень і публікацій. Провівши детальний аналіз існуючих методів розрахунку рівня кіберзахисту, виявлено наступне.

Для розрахунку рівня кіберзахисту використовують різні підходи. Наприклад, предметом робіт як інституційних розробників, що створили моделі CMMI (Software Engineering Institute) [3] та C2M2 (Міністерство енергетики США) [4], так і науковців, які зробили значний внесок в адаптацію цих підходів, зокрема Уоттс Хамфрі, Мартін Кляйн і Майкл Л. Масі [5-6], а також українських дослідників Худинцева М. М. та Палажченка І. Л. [7] є дослідження методів оцінки зрілості кіберзахисту.

Дослідження методів оцінки кіберзахисту на основі ризиків здійснювалося провідними інституціями, зокрема National Institute of Standards and Technology (NIST), розробником фреймворку NIST Cybersecurity Framework, version 2.0 (NIST CSF 2.0). [8], та International Organization for Standardization (ISO), автором стандарту ISO/IEC 27005 [9]. Значний внесок у розвиток цього підходу також зробили науковці, серед яких Гері Стоунбернер, Джек Джонс, Майкл Паттон, Мансур Алалі [10-13]. Грунтовне дослідження щодо методів на основі ризиків здійснив український дослідник Гончар С.Ф. [14].

Методи оцінки, засновані на відповідності, розробляються передусім такими міжнародними організаціями, як International Organization for Standardization (ISO) (видавник стандарту ISO/IEC 27001) [15]. На національному рівні нормативну базу створюють державні органи, зокрема Кабінет Міністрів України та Державна служба спеціального зв’язку та захисту інформації України. Наукові дослідження в цій галузі зосереджені на аналізі та вдосконаленні існуючих стандартів.

Отже, можна згрупувати методи для оцінювання рівня кіберзахисту за такими характеристиками:

1. На основі зрілості;
2. На основі ризиків;
3. На основі відповідності.

Методи на основі зрілості оцінюють рівень зрілості процесів в організації. Вони допомагають визначити поточний стан кіберзахисту та спланувати його розвиток.

Ці методи оцінюють не просто наявність заходів кіберзахисту, а рівень зрілості процесів в організації. Вони допомагають визначити поточний стан кіберзахисту та спланувати його розвиток. Прикладами таких методів є C2M2 та CMMI. В цих методах оцінка здійснюється за багатоступеневою шкалою (наприклад, від 0 до 5), де кожен рівень відповідає певному ступеню розвитку процесів, від хаотичного до оптимізованого. Перевагами цих методів є комплексний погляд на кіберзахист як на процес, а не одноразову дію. Однак, їхні результати часто є суб'єктивними і не завжди відображають реальну стійкість до актуальних кіберзагроз, особливо в умовах специфічних для України викликів.

Методи на основі ризиків зосереджені на виявленні та оцінці ризиків, пов'язаних з інформаційними активами. Їхня мета — пріоритезувати заходи захисту так, щоб зменшити найбільші ризики. Прикладами таких методів є NIST CSF 2.0, CISA Cybersecurity Performance Goals (CPGs) [16]. В основі цих методів лежить ідентифікація активів, загроз та вразливостей, після чого розраховується рівень ризику (як добуток імовірності реалізації загрози та її потенційного впливу). Ключовою перевагою є прямий зв'язок з бізнес-цілями організації та можливість оптимізації витрат. Однак, кількісна оцінка ризиків часто є складною і залежить від експертних суджень, що може призвести до невідповідностей.

Методи на основі відповідності ґрунтуються на перевірці відповідності організації вимогам нормативно-правових актів, стандартів та політик. Прикладами таких методів є ISO/IEC 27001, а також національні вимоги, такі як Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури, затверджені постановою Кабінету Міністрів України від 19.06.2019 № 518 [17]. В таких методах оцінюється, чи впроваджено необхідні заходи, що передбачені документами. Зазвичай це перевіряється бінарним шляхом: «так» або «ні». Ці методи забезпечують дотримання законодавства, проте вони не гарантують реального рівня захищеності, оскільки наявність документа чи політики не завжди означає їх ефективне виконання.

Таблиця 1

Порівняльна таблиця методів оцінки рівня кіберзахисту

Характеристика	На основі відповідності	На основі ризиків	На основі зрілості
Мета оцінки	Досягнення нормативних вимог.	Мінімізація ризиків для бізнесу.	Мінімізація ризиків для бізнесу.
Гнучкість	**Низька**. Критерії фіксовані та не адаптуються до змін.	**Висока**. Фокусується на унікальних ризиках конкретного об'єкта.	**Середня**. Потребує адаптації моделі, але дозволяє гнучке планування.
Орієнтація	**Нормативно-орієнтований**. Головне — дотримання законів і стандартів.	**Бізнес-орієнтований**. Зв'язок між заходами та їхнім впливом на бізнес.	**Процесно-орієнтований**. Головне — ефективність управління та внутрішніх процесів.
Дескриптивність	**Низька**. Оцінка бінарна («виконано»/»не виконано»).	**Висока**. Детальний опис загроз, вразливостей і наслідків.	**Висока**. Докладна характеристика поточного та бажаного стану.
Суб’єктивність	**Низька**. Критерії чіткі, а результати перевіряються.	**Висока**. Залежить від експертних оцінок імовірності та впливу.	**Середня**. Може бути суб'єктивною, але використовує чіткі критерії для рівнів зрілості.
Використовувані дані	Чек-листи, аудити, наявність документів.	Дані про загрози, вартість активів, результати сканування вразливостей.	Інтерв'ю, опитування, аналіз політик та процедур.

В табл. 1 здійснено порівняння методів оцінки рівня кіберзахисту за такими характеристиками: мета оцінки, гнучкість, орієнтація, дескриптивність, суб’єктивність та використовувані дані.

Аналіз показав, що жоден з існуючих методів не є повністю універсальним. Методи на основі зрілості та ризиків можуть бути суб'єктивними, тоді як методи на основі

відповідності не враховують реальну ефективність. З огляду на специфіку українських реалій та постійно зростаючі кіберзагрози, існує потреба в розробці нового, гібридного методу. Цей підхід має поєднувати об'єктивні критерії відповідності з гнучкими показниками зрілості для стратегічного планування та інтегрувати ризик-орієнтований підхід для фокусування на найбільш критичних загрозах, що є особливо актуальним в сучасних умовах. Метод має враховувати секторальну специфіку ОКІІ та динамічний характер загроз.

В роботі [18] було розроблено модель оцінювання стану кіберзахисту ОКІІ.

Ключовими компонентами моделі є:

Множина систем критеріїв (*SC*): Модель оперує сімома системами критеріїв, шість з яких відповідають вимогам постанови Кабінету Міністрів України від 29 грудня 2021 року № 1426 [19] (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.

Підмножини критеріїв (*SCi*): 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 [20]. 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 [21, табл. 4].

Таким чином, в моделі враховано підхід на основі відповідності. Щоб врахувати ризик-орієнтований підхід та відобразити неоднаковий вплив різних систем критеріїв на загальний рівень захищеності, пропонується ввести вагові коефіцієнти. Модель представляє кінцевий результат оцінювання у вигляді єдиного кількісного показника в діапазоні від 0 до 1, який інтерпретується за п'ятирівневою відсотковою шкалою, узгодженою з міжнародними моделями зрілості (наприклад, NIST CSF, CMMI).

Отже, **метою** роботи є розробка гібридного методу розрахунку рівня кіберзахисту ОКІІ на основі раніше запропонованої автором моделі розрахунку рівня кіберзахисту ОКІ. Для досягнення мети роботи необхідно розробити додаткові вагові коефіцієнти для системи критеріїв, розробити і описати метод розрахунку рівня кіберзахисту ОКІІ.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

1. Розробка додаткових вагових коефіцієнтів для системи критеріїв

Для досягнення адекватного та репрезентативного оцінювання необхідно запровадити вагові коефіцієнти для системи критеріїв. Оскільки різні системи критеріїв мають неоднаковий вплив на загальний стан захищеності ОКІІ, неможливо трактувати усі системи як рівнозначні. Це призведе до викривлення загальної оцінки та хибних висновків щодо реального рівня кіберзахисту ОКІІ.

Етап 1. Оскільки критерії являють собою набір дихотомічних питань, для забезпечення їх кількісної характеристики та подальшого математичного аналізу пропонується застосовувати бінарне кодування. У цьому форматі кожній позитивній відповіді («Так») присвоюється числове значення «1», тоді як кожна негативна відповідь

(«Ні») отримує значення «0». Такий підхід дозволяє трансформувати якісні характеристики у числовий формат, забезпечуючи можливість статистичної обробки та подальшого інтегрального оцінювання стану досліджуваних параметрів.

Етап 2. Для підвищення аналітичної цінності результатів оцінювання, отриманих на основі набору дихотомічних питань, пропонується ввести вагові коефіцієнти для кожної системи критеріїв. Цей підхід дозволить відобразити різний ступінь впливу кожної групи питань на загальну оцінку стану кіберзахисту, забезпечуючи більш точну та об'єктивну інтерпретацію агрегованих даних.

З метою забезпечення гібридності методу розрахунку рівня кіберзахисту пропонується застосувати метод оцінки ризиків, здатний оперувати ваговими коефіцієнтами.

В [14] автор монографії виділяє наступні методи оцінювання ризиків: Brainstorming, Delphi method, HAZOP, SWIFT, HACCP, Fault tree analysis, Event tree analysis, Monte Carlo simulation, Байєсовські мережі, LOPA, Consequence/probability matrix, MCDA тощо. Зазначені методи оцінювання ризиків можна згрупувати за підходом до оцінювання ризиків:

Експертні методи (Brainstorming, Delphi method) ефективні для ідентифікації загроз та збору експертних думок, але не містять вбудованих механізмів для формалізованого розрахунку вагових коефіцієнтів. Їхні результати мають переважно описовий характер і можуть бути використані як початкові дані для інших, більш структурованих методів.

Методи аналізу процесів (HAZOP, SWIFT, HACCP) призначені для систематичного дослідження робочих процесів з метою виявлення відхилень та потенційних небезпек. Вони зосереджені на причинно-наслідкових зв’язках усередині системи, але не передбачають механізмів для зважування різних факторів ризику.

Методи причинно-наслідкового аналізу (Fault tree analysis, Event tree analysis) дозволяють моделювати логічні зв’язки між подіями. Вони надають кількісні оцінки ймовірності збою, але не є інструментом для введення суб'єктивних вагових коефіцієнтів, що відображають пріоритети.

Кількісні та математичні методи (Monte Carlo simulation, Байєсовські мережі, LOPA) базуються на строгих математичних та статистичних моделях. Вони оперують імовірностями та числовими даними, забезпечуючи високу об'єктивність, але не мають механізму для врахування суб'єктивних вагових коефіцієнтів, що можуть відображати важливість критеріїв для конкретної організації.

Методи порівняння (MAI, Consequence/probability matrix, MCDA) ґрунтуються на зіставленні різних варіантів або оцінок за певними критеріями, що допомагає прийняти рішення.

Було проведено аналіз існуючих розповсюджених методів оцінки ризиків (табл. 2) за такими критеріями:

- Наявність механізму для встановлення ваг (МВ);
- Гнучкість (ГН) – здатність методу використовувати різні типи даних для визначення ваг (як якісні, так і кількісні дані);
- Зменшення суб'єктивності (ЗС) – здатність мінімізувати упередженість експертів при встановленні ваг.
- Простота інтерпретації результатів (ПІ);
- Придатність для прийняття рішень (ПР) – можливість використання результатів роботи методу для вибору оптимального рішення.

Таблиця 2

Порівняльна таблиця методів оцінки ризиків

Група методів	Метод	МВ	ГН	ЗС	ПІ	ПР
Експертні методи	Brainstorming	-	+	-	+/-	-
	Delphi method	-	+	+	+/-	-
Методи аналізу процесів	HAZOP	-	+	+	+	+
	SWIFT	-	+	+/-	+	+
	HACCP	-	+	+	+	+
Методи причинно-наслідкового аналізу	Fault tree analysis	-	+/-	+	+	+
	Event tree analysis	-	+/-	+	+	+
Кількісні та математичні методи	Monte Carlo simulation	-	-	+	+	+
	Байєсовські мережі	-	+	+	+/-	+
	LOPA	-	-	+	+	+
Методи порівняння	Аналізування ієрархій (MAI)	+	+	+	+	+
	Consequence/probability matrix	-	+	-	+	+
	MCDA	+	+	-	+	+

Аналіз існуючих методів оцінки ризиків, виконаний в табл. 2, показав, що запропонованим критеріям у більшості відповідають методи групи «Методи порівняння», оскільки вони безпосередньо спрямовані на порівняння та зважування різних критеріїв.

З огляду на необхідність розроблення вагових коефіцієнтів пропонується розглянути методи порівняння детальніше.

MAI: Цей метод дозволяє експертам встановлювати пріоритети для різних критеріїв шляхом попарних порівнянь. Ці порівняння перетворюються на числові значення (вагові коефіцієнти), що відображають відносну важливість кожного критерію. MAI допомагає структуровано оцінити, наприклад, важливість різних аспектів кіберзахисту (як-от конфіденційність даних, доступність сервісів) та об'єктивно порівняти їх.

MCDA: Цей метод дозволяє приймати рішення, враховуючи декілька критеріїв одночасно. Кожен критерій може мати свій ваговий коефіцієнт, який відображає його важливість для організації. MCDA використовує ці ваги для розрахунку загального рейтингу кожної альтернативи. Проте, MCDA не має вбудованого механізму для перевірки узгодженості ваг.

Consequence/probability matrix: У класичному варіанті цього методу ваги не використовуються. Однак, у більш досконалих версіях можна застосовувати вагові коефіцієнти для коригування оцінки. Наприклад, можна надати більшу вагу певним наслідкам (наприклад, втраті критично важливих даних) порівняно з іншими (наприклад, незначними збоями). Це дозволяє точніше визначити, які ризики є найпріоритетнішими для організації. Однак, такий метод є надмірно спрощеним, оскільки він зводить всі критерії до двох параметрів, що може призвести до низької точності та суб’єктивності.

Отже, провівши аналіз, пропонується використовувати метод аналізу ієрархій з експертними оцінками попарних порівнянь для визначення вагових коефіцієнтів.

Етап 2.1. Побудова ієрархії:

На рис. 1 показано побудова ієрархії оцінювання стану кіберзахисту ОКІІ.

Перший рівень (верхній) – це визначення мети розробки вагових коефіцієнтів систем критеріїв. Отже, мета – оцінювання стану кіберзахисту ОКІІ.

Другий рівень (середній) – це критерії/атрибути, що використовуються у оцінці: Складність впровадження, Відповідність регуляторним вимогам, Швидкість досягнення результату, Потреба у специфічних фахівцях, Потреба у постійному оновленні.

Третій рівень (нижній) представляє альтернативні рішення (субкритерії), які будуть порівнюватися між собою на цьому рівні відносно загальної мети, а саме множини систем Секторальна складова (SE), Управління (GV), Ідентифікація (ID), Забезпечення захисту (PR), Виявлення (DE), Реагування (RS), Відновлення (RC).

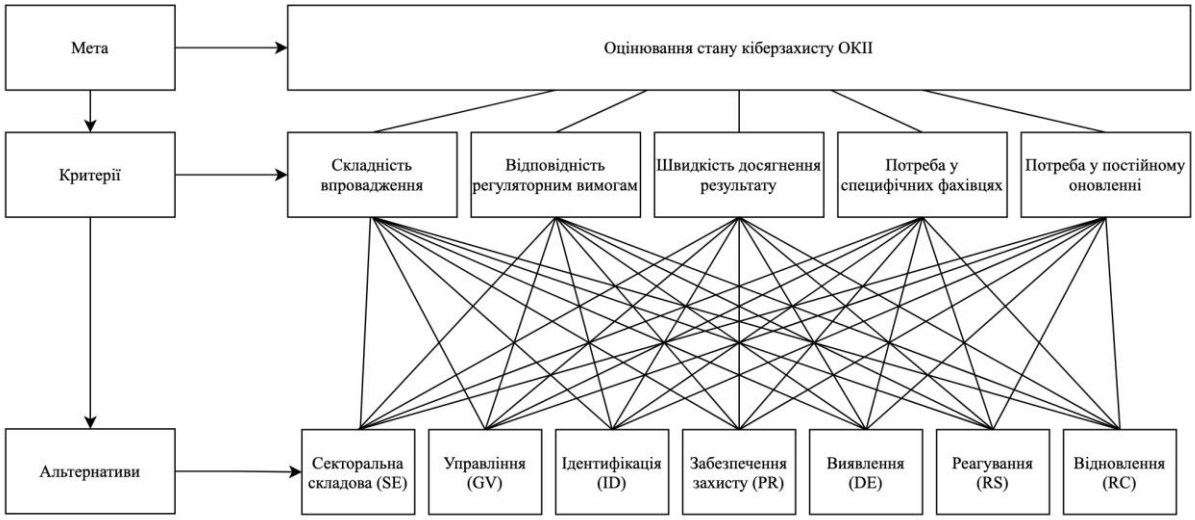

Рис. 1. Ієрархія оцінювання стану кіберзахисту ОКІІ

Етап 2.2. Проведення попарних порівнянь експертами.

На даному кроці для ілюстрації застосування методу аналізу ієрархій у контексті визначення вагових коефіцієнтів для систем критеріїв, парні порівняння виконано автором. Важливо підкреслити, що ці порівняння є демонстраційними і слугують прикладом реалізації механізму зважування, який інтегровано до програмного забезпечення для проведення самостійних оцінок користувачами. При цьому для кількісного визначення переваг одного критерію над іншим використовувалася (та інтегрована в програмне забезпечення) фундаментальна шкала Сааті [22], що передбачає значення від 1 до 9, де 1 - однакова важливість; 3 - помірна перевага; 5 - сильна перевага; 7 - дуже сильна перевага; 9 - абсолютна перевага; парні числа (2, 4, 6, 8) - проміжні значення; зворотні значення (1/3, 1/5) - для відображення зворотної переваги.

Отже, автор оцінив відносну важливість та переваги елементів на кожному рівні ієрархії за допомогою спеціальних матриць парних порівнянь.

Етап 2.3. Формування матриці порівнянь та розрахунок вагових коефіцієнтів:

В Таблиці 3 представлено нормалізовану матрицю розрахунку важливості кожної альтернативи за критерієм «Складність впровадження» за допомогою шкали Сааті за формулою:

$$A'_{ij} = \frac{A_{ij}}{\sum_{k=1}^{n} A_{kj}}$$

де A'_{ij} – позначення елемента нормалізованої матриці, де і - номер рядка, j - номер стовпця;

A_{ij} – оригінальний елемент матриці на позиції (i,j).

Таблиця 3

Нормалізована матриця розрахунку важливості

Важливість	**SE = «Секторальна складова»**	**GV = «Управління»**	**ID = «Ідентифікація ризиків кібербезпеки»**	**PR = «Кіберзахист»**	**DE = «Виявлення кіберінцидентів»**	**RS = «Реагування на кіберінциденти»**	**RC = «Відновлення стану кібербезпеки»**
SE = «Секторальна складова»	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 = «Управління»	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 = «Ідентифікація ризиків кібербезпеки»	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 = «Кіберзахист»	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 = «Виявлення кіберінцидентів»	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 = «Реагування на кіберінциденти»	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 = «Відновлення стану кібербезпеки»	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

Для отримання вагових коефіцієнтів застосуємо формулу:

$$w_i = \frac{1}{n}\sum_{j=1}^{n} A'_{ij}$$

де n – загальна кількість критеріїв, що порівнюються.

Таким чином, отримуємо 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

$$\sum w(SE), w(GV), w(ID), w(DE), w(PR), w(RS), w(RC) = 0{,}9957$$

Етап 2.4. Перевірка узгодженості

Для перевірки на однорідність суджень та оцінок автора необхідно розрахувати зважену суму для кожної альтернативи:

SE = «Секторальна складова»: 0.3311

GV = «Управління»: 0.9648

ID = «Ідентифікація ризиків кібербезпеки»: 2.3224

PR = «Кіберзахист»: 0.7568

DE = «Виявлення кіберінцидентів»: 1.2103

RS = «Реагування на кіберінциденти»: 1.0312

RC = «Відновлення стану кібербезпеки»: 0.7685

Після чого розраховується λ_{max} = 7.396, індекс узгодженості CI = 0.066 та випадковий індекс RI = 1,32.

Відношення узгодженості $CR = \frac{CI}{RI} = \frac{0{,}273}{1{,}32} = 0{,}050.$

Вагові коефіцієнти (вектор пріоритетів):

SE («Секторальна складова»): 0.0441

GV («Управління»): 0.1340

ID («Ідентифікація ризиків кібербезпеки»): 0.3112

PR («Кіберзахист»): 0.1012

DE («Виявлення кіберінцидентів»): 0.1559

RS («Реагування на кіберінциденти»): 0.1357

RC («Відновлення стану кібербезпеки»): 0.1136

Відношення узгодженості (CR): 0.050 (5.0%)

Отже, CR = 0.050 є значно меншим за допустимий поріг 0.10 (10%). Це означає, що матриця попарних порівнянь є узгодженою, і судження, закладені в неї, є достатньо послідовними.

Використаємо (6) в [18] з урахуванням вагових коефіцієнтів для отримання зваженого середнього:

$$SA_{SC}^{w} = \sum_{i=1}^{n} w_i \left(\frac{\sum_{j=1}^{k_i} SC_{ij}}{k_i} \right), \quad (1)$$

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

При чому, оскільки модель, розроблена в [18] використовує шкалу в діапазоні від 0 до 1, то після введення вагових коефіцієнтів фінальний результат роботи моделі має бути в діапазоні [0, 1].

Таким чином, модель, розроблена в [18] модифікована для підвищення її функціональності, шляхом розроблення вагових коефіцієнтів для систем критеріїв, що дозволяє моделі більш точно відображати реальний рівень кіберзахисту.

2. Розробка методу розрахунку рівня кіберзахисту ОКІІ

Запропонований метод розрахунку рівня кіберзахисту ОКІІ (схема реалізації відображена на рис. 2) реалізується в такі етапи: 1) визначення множини системи критеріїв, яка охоплює групи заходів із кіберзахисту (*SC*); 2) визначення підмножини критеріїв (*SCi*); 3) формування деталізованих заходів із кіберзахисту у вигляді показників критеріїв; 4) введення вагових коефіцієнтів для системи критеріїв; 5) введення кількісних характеристик для формалізації результату; 6) визначення рівня кіберзахисту ОКІІ у вигляді кількісного показника; 7) складання звіту-графіку представлення результатів рівня кіберзахисту ОКІІ.

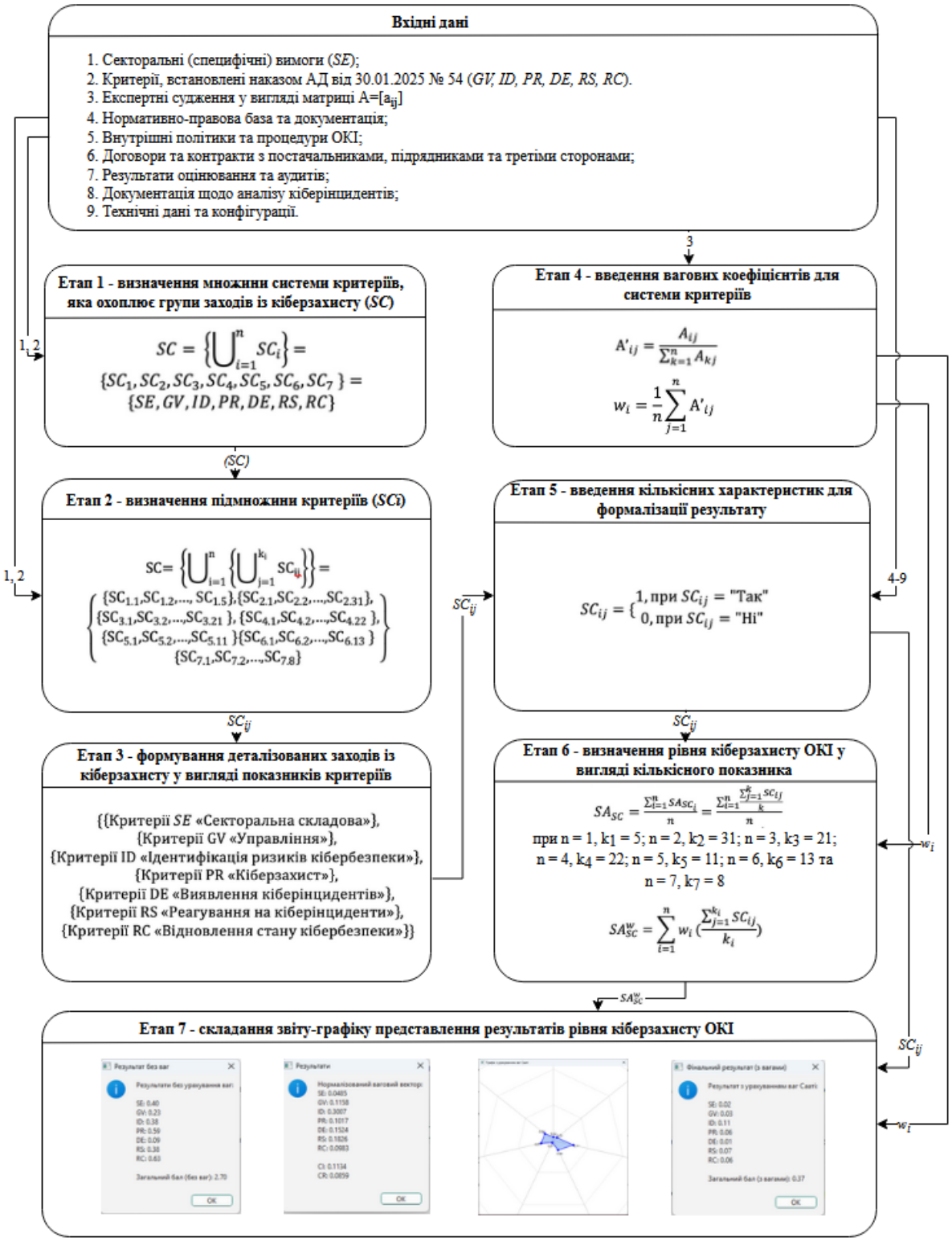

Рис. 2. Схема реалізації методу розрахунку рівня кіберзахисту

Робота методу ґрунтується на таких принципах:

- Принцип ієрархічності: структура методу побудована за ієрархічним принципом, що дозволяє проводити оцінювання від загального рівня (систем критеріїв) до конкретних деталей (окремих критеріїв).

- Принцип багатокритеріального аналізу: оцінка рівня кіберзахисту не ґрунтується на одному показнику, а є результатом комплексного аналізу багатьох критеріїв. Це дозволяє отримати більш повне та об'єктивне уявлення про стан захищеності.
- Принцип адаптивності та релевантності: метод адаптовано до актуального українського законодавства, він враховує секторальну специфіку ОКІІ та дозволяє коригувати вагові коефіцієнти, що забезпечує його гнучкість та відповідність конкретним потребам.
- Принцип кількісної формалізації: якісні характеристики (відповіді «Так/Ні») перетворюються на кількісні значення (1/0), що робить можливим їх математичний аналіз та отримання числового результату.

Вхідними параметрами для роботи методу є:

- Секторальні (специфічні) вимоги;
- Критерії, встановлені наказом Адміністрації Держспецзв'язку № 54 від 30.01.2025 [20];
- Експертні судження у вигляді матриці;
- Нормативно-правова база та документація;
- Внутрішні політики та процедури ОКІІ;
- Договори та контракти з постачальниками, підрядниками та третіми сторонами;
- Результати оцінювання та аудитів;
- Документація щодо аналізу кіберінцидентів;
- Технічні дані та конфігурації (мережеві схеми та архітектура безпеки, конфігурації систем захисту, дані про резервне копіювання, інформація про системи управління доступом, журнали та системи моніторингу).

Вихідними даними роботи методу є:

- Кількісний показник рівня кіберзахисту ОКІІ без урахування вагових коефіцієнтів;
- Кількісний показник рівня кіберзахисту ОКІІ з урахуванням вагових коефіцієнтів;
- Графік представлення результатів рівня кіберзахисту ОКІІ без урахування вагових коефіцієнтів;
- Графік представлення результатів рівня кіберзахисту ОКІІ з урахуванням вагових коефіцієнтів;
- Узагальнений звіт про рівень кіберзахисту ОКІІ з якісною оцінкою.

Послідовність роботи методу:

Етап 1. Визначення множини системи критеріїв, яка охоплює групи заходів із кіберзахисту (*SC*)

$$SC = \left\{\bigcup_{i=1}^{n} SC_i\right\} = \{SC_1, SC_2, SC_3, SC_4, SC_5, SC_6, SC_7\} = \{SE, GV, ID, PR, DE, RS, RC\}$$

де $SC_i \subseteq SC (i = \overline{1,n})$ – ідентифікатор відповідної системи критеріїв.

Етап 2. Визначення підмножини критеріїв (*SCi*)

$$SC = \left\{\bigcup_{i=1}^{n} \left\{\bigcup_{j=1}^{k_i} SC_{ij}\right\}\right\} = \{\{SC_{1.1}, SC_{1.2}, \ldots, SC_{1.h}\}, \{SC_{2.1}, SC_{2.2}, \ldots, SC_{2.31}\}, \{SC_{3.1}, SC_{3.2}, \ldots, SC_{3.21}\}, \{SC_{4.1}, SC_{4.2}, \ldots, SC_{4.22}\}, \{SC_{5.1}, SC_{5.2}, \ldots, SC_{5.11}\} \{SC_{6.1}, SC_{6.2}, \ldots, SC_{6.13}\} \{SC_{7.1}, SC_{7.2}, \ldots, SC_{7.8}\}\}$$

де для множини критеріїв SC_1 при n = 1, k_1 = h, де h = 3, або 4, або 5 (залежно від вибору SE) та для множин критеріїв $SC_2, SC_3, SC_4, SC_5, SC_6$ та SC_7, при n = 2, k_2 = 31; n = 3, k_3 = 21; n = 4, k_4 = 22; n = 5, k_5 = 11; n = 6, k_6 = 13 та n = 7, k_7 = 8.

Етап 3. Формування деталізованих заходів із кіберзахисту у вигляді показників критеріїв

Для множин критеріїв $SC_2, SC_3, SC_4, SC_5, SC_6$ та SC_7 деталізовані заходи кіберзахисту сформовані у відповідності до наказу Адміністрації Держспецзв'язку № 54 від 30.01.2025 [20]. Для множини критеріїв SC_1 деталізовані заходи кіберзахисту є індивідуальними для кожного сектора критичної інфраструктури і складаються з різної кількості критеріїв [21, табл. 4].

Етап 4. Введення вагових коефіцієнтів для системи критеріїв

Див. Етап 2 пункту 1. «Розробка додаткових вагових коефіцієнтів для системи критеріїв» Розділу «Основна частина дослідження»).

Етап 5. Введення кількісних характеристик для формалізації результату

Див. Етап 1 пункту 1. «Розробка додаткових вагових коефіцієнтів для системи критеріїв» Розділу «Основна частина дослідження»).

Етап 6. Визначення рівня кіберзахисту ОКІІ у вигляді кількісного показника

Використовуючи (4), (5), (6) та (7) в [18]).

Етап 7. Складання звіту-графіку представлення результатів рівня кіберзахисту ОКІІ.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У роботі було проведено аналіз методів оцінювання рівня кіберзахисту, який показав, що жоден з існуючих підходів не є універсальним. Виявлено, що ефективний метод має поєднувати елементи аналізу відповідності, ризиків і зрілості, а також враховувати секторальну специфіку ОКІІ і динамічний характер загроз. Крім того, проведений аналіз методів оцінки ризиків засвідчив, що метод аналізу ієрархій є найбільш придатним для розроблюваного підходу.

На основі отриманих результатів було розроблено метод розрахунку рівня кіберзахисту ОКІІ, який є адаптивним, багатоцільовим та орієнтованим на практичне застосування в умовах динамічних кіберзагроз, що є особливо актуальним для України.

Продовженням даного дослідження стане проведення експериментального дослідження розробленого методу на трьох ОКІ паливно-енергетичного сектору. Результати, отримані за допомогою авторського програмного забезпечення, будуть порівняні з оцінками, наданими двома іншими інструментами, для підтвердження ефективності методу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. (2025). *Річний звіт системи виявлення вразливостей і реагування на кіберінциденти.* https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006
2. Рада національної безпеки і оборони України. (2024). *Річний аналітичний огляд (жовтень 2023 – вересень 2024).* https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20250109/Year%20in%20review_UKR_upd.pdf?fbclid=IwY2xjawI-fZRleHRuA2FlbQIxMAABHcaZdkgcVIlSJ0eGnBO78x5xRCDcoBwcJ1GKrT4SAVS5reEAtY5u8ssd4w_aem_0xN1oMO3-toIy6vpuA27mA

3. CMMI Institute. (2023). *Capability Maturity Model Integration (CMMI) for Development, Version 3.0.* https://cmmiinstitute.com/cmmi
4. 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
5. W. S. Humphrey. (1989). *Managing the software process*. Reading, Addison-Wesley, MA, 1989.
6. Klein, M., & Masi, M. (1993). *The Capability Maturity Model, Version 1.1*. IEEE Software.
7. Khudyntsev, M., & Palazhchenko, I. (2024). *Cybersecurity Maturity Models for Cybersecurity assessment in critical infrastructure*. ISSN: 2411-4049. Екологічна безпека та природокористування, вип. 4 (52), 2024.
8. National Institute of Standards and Technology. (2024) *NIST Cybersecurity Framework, version 2.0.* https://www.nist.gov/cyberframework
9. ISO/IEC. (2022). *27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks*
10. Stoneburner, G., Goguen A., Feringa A. (2002). *Risk Management Guide for Information Technology Systems (NIST Special Publication 800-30)*.
11. Freund J, Jones J. (2014). *Measuring and Managing Information Risk: A FAIR Approach.* United States: Butterworth-Heinemann. ISBN-13:978-0124202313.
12. Patton, Michael Quinn (2002). *Qualitative Research and Evaluation Methods. 3 ed*. SagePublications.
13. Mansour Alali, Ahmad Almogren, Mohammad Mehedi Hassan etc. (2018). *Improving risk assessment model of cyber security using fuzzy logicinference system*. Computers & Security, № 74.
14. Гончар, С. Ф. (2019). *Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури: монографія*. К.: Альфа Реклама. 176 с. ISBN 978-966-288-263-6
15. ISO/IEC. (2022). *27001:2022. Information technology — Security techniques — Information security management systems — Requirements.*
16. Cybersecurity and Infrastructure Security Agency. (2023). *CISA Cybersecurity Performance Goals*. https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf
17. Кабінет Міністрів України. (2019). *Постанова від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури».*
18. Юдіна, Д. (2025). *Модель розрахунку рівня кіберзахисту об'єктів критичної інфраструктури*. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», *4*(28), 586–598. https://doi.org/10.28925/2663-4023.2025.28.829
19. Кабінет Міністрів України. (2021). *Постанова від 29.12.2021 № 1426 «Про затвердження Положення про організаційно-технічну модель кіберзахисту».*
20. 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».*
21. Юдіна, Д. (2025). Модифікація моделі розрахунку рівня кіберзахисту об'єктів критичної інформаційної інфраструктури. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1*(29), 818–836. https://doi.org/10.28925/2663-4023.2025.29.943
22. Vargas, Luis L.; Saaty, Thomas L. (2001). *Models, Methods, Concepts & Applications of the Analytic Hierarchy Process*. Boston: Kluwer Academic. ISBN 0-7923-7267-0

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue

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

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

Abstract. In today's world, where the number and complexity of cyber threats, especially those targeting strategic state assets, are growing rapidly, there is an urgent need to develop effective, flexible, and adaptive mechanisms for assessing the current level of cyber security. In view of this need, an analysis of existing approaches to assessing the level of cyber security was conducted. Among them are models based on maturity, risk, and compliance. The results of the analysis showed that none of these approaches is completely universal or sufficient for a comprehensive assessment of critical information infrastructure objects in the context of the national legislative field. In particular, approaches based solely on compliance may not take into account real risks, while approaches based on maturity are often too subjective. To address these systemic shortcomings, a hybrid approach was proposed. This approach integrates the best features of previous models, combining the objectivity of compliance testing, the flexibility and process orientation of maturity assessment, and risk-based prioritization. Based on the hybrid approach, a method for calculating the level of cyber protection of critical information infrastructure objects was developed. A component of this method is the introduction of weighting coefficients for different criteria systems. To determine these weighting coefficients, which should ensure an objective reflection of expert knowledge, the hierarchy analysis method was chosen. The proposed method allows qualitative characteristics (e.g., binary "yes/no" answers) to be transformed into a single quantitative indicator. This indicator is calculated in a standardized range from 0 to 1, which facilitates comparison and monitoring. The resulting numerical value is further interpreted on a five-level maturity scale (from "Initial" to "Optimized"), which provides a clear idea of the steps needed for improvement. Thus, the developed method is hierarchical, multi-criteria, and adaptable to current Ukrainian legislation in the field of cyber protection and cyber security. In further research, it is planned to conduct an experimental study and verify the method on three critical infrastructure objects in the fuel and energy sector, as well as to compare the results obtained using the author's software and two other tools.

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

REFERENCES

1. State Cyber Protection Center of the State Service of Special Communications and Information Protection of Ukraine. (2025). *Annual report of the vulnerability detection and cyber incident response system*. https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006
2. National Security and Defense Council of Ukraine. (2024). *Annual analytical review (October 2023 – September 2024)*. https://www.rnbo.gov.ua/files/2024/
3. CMMI Institute. (2023). *Capability Maturity Model Integration (CMMI) for Development, Version 3.0*. https://cmmiinstitute.com/cmmi
4. 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
5. W. S. Humphrey. (1989). *Managing the software process.* Reading, Addison-Wesley, MA, 1989
6. Klein, M., & Masi, M. (1993). *The Capability Maturity Model, Version 1.1*. IEEE Software.

7. Khudyntsev, M., & Palazhchenko, I. (2024). *Cybersecurity Maturity Models for Cybersecurity assessment in critical infrastructure*. ISSN: 2411-4049. Environmental safety and environmental management, vol. 4 (52), 2024.
8. National Institute of Standards and Technology. (2024) *NIST Cybersecurity Framework, version 2.0.* https://www.nist.gov/cyberframework
9. ISO/IEC. (2022). *27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks*
10. Stoneburner, G., Goguen A., Feringa A. (2002). *Risk Management Guide for Information Technology Systems (NIST Special Publication 800-30)*.
11. Freund J, Jones J. (2014). *Measuring and Managing Information Risk: A FAIR Approach.* United States: Butterworth-Heinemann. ISBN-13:978-0124202313.
12. Patton, Michael Quinn (2002). *Qualitative Research and Evaluation Methods. 3 ed*. SagePublications.
13. Mansour Alali, Ahmad Almogren, Mohammad Mehedi Hassan etc. (2018). *Improving risk assessment model of cyber security using fuzzy logicinference system*. Computers & Security, № 74.
14. Honchar, S. F. (2019). *Cybersecurity risk assessment model of information systems of critical infrastructure facilities.* Monograph, Alpha Reklama. 176 p. ISBN 978-966-288-263-6
15. ISO/IEC. (2022). *27001:2022. Information technology — Security techniques — Information security management systems — Requirements.*
16. Cybersecurity and Infrastructure Security Agency. (2023). *CISA Cybersecurity Performance Goals*. https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf
17. Cabinet of Ministers of Ukraine. (2019). *Resolution No. 518 dated June 19, 2019 "On Approval of General Requirements for Cybersecurity of Critical Infrastructure Facilities"*.
18. Yudina, D. (2025). *Model for Calculating the Level of Cyber Security of Critical Infrastructure Facilities*. Electronic professional scientific publication “Cybersecurity: Education, Science, Technology,” 4(28), 586–598. https://doi.org/10.28925/2663-4023.2025.28.829
19. Cabinet of Ministers of Ukraine. (2021). *Resolution No. 1426 dated December 29, 2021 "On approval of the Regulations on the organizational and technical model of cybersecurity"*.
20. Administration of the State Service of Special Communications and Information Protection of Ukraine. (2025). *Order No. 54 dated January 30, 2025, “On Approval of Basic Cyber Security Measures and Methodological Recommendations for Implementing Basic Cyber Security Measures”*.
21. Yudina, D. (2025). *Modification of the Model for Calculating the Level of Cyber Security of Critical Infrastructure Facilities*. Electronic professional scientific publication “Cybersecurity: Education, Science, Technology,” *1*(29), 818–836. https://doi.org/10.28925/2663-4023.2025.29.943
22. Vargas, Luis L.; Saaty, Thomas L. (2001). *Models, Methods, Concepts & Applications of the Analytic Hierarchy Process*. Boston: Kluwer Academic. ISBN 0-7923-7267-0