



DOI 10.28925/2663-4023.2025.29.837

УДК 004.056.55:681.3.06

Сидоренко Вікторія Миколаївна

к.т.н., доц., доцент кафедри комп'ютерних інформаційних технологій
Державний університет «Київський авіаційний інститут», Київ, Україна
ORCID ID: 0000-0002-5910-0837
v.sydorenko@ukr.net

МЕТОД ОЦІНЮВАННЯ СТІЙКОСТІ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

Анотація. У сучасних умовах зростання кількості та складності загроз питання оцінювання стійкості об'єктів критичної інформаційної інфраструктури (ОКІІ) набуває першочергового значення для національної безпеки держави. Вразливість інфраструктурних систем у поєднанні з міжсекторальними залежностями обумовлює необхідність застосування інтегрованих науково обґрунтованих підходів до оцінки ОКІІ та підвищення їхньої стійкості. У статті представлено інтегрований метод оцінювання стійкості ОКІІ, що поєднує багатовимірну систему індикаторів, методи нечіткого аналізу, уніфіковану нормалізацію змінних та категоризацію об'єктів згідно з чинними нормативними документами. Вперше в процес оцінювання інтегровано модель життєвого циклу стійкості (P–A–A–R), яка дозволяє здійснювати подвійний розрахунок категорії критичності: первинний — на основі інтегрального показника РКОКІ, та повторний — з урахуванням здатності системи прогнозувати, витримувати впливи, адаптуватися та відновлюватися. Експериментальне дослідження, проведене на прикладі трьох вимірів стійкості (економічного, соціального та безпекового), підтвердило пріоритетність безпекового аспекту й водночас довело значущість економічних і соціальних чинників у формуванні збалансованої системи. Результати роботи мають практичне значення для державних і приватних структур, що відповідають за захист критичної інфраструктури, оскільки створюють основу для стратегічного управління ризиками та розвитку адаптивних політик. Подальші дослідження будуть спрямовані на верифікацію методу у всіх вимірах стійкості для різних міст держави з метою підтвердження його універсальності та масштабованості.

Ключові слова: критична інфраструктура; об'єкти критичної інформаційної інфраструктури; кібербезпека; стійкість; оцінювання стійкості; нечіткий аналіз; управління ризиками; критичність; категорії критичності.

ВСТУП

Забезпечення стійкості об'єктів критичної інфраструктури (КІ) є одним із ключових завдань національної безпеки України. Сучасні умови характеризуються поєднанням різномірних загроз: від воєнних дій і терористичних актів до кібератак, природних катастроф і техногенних аварій. Уразливість КІ безпосередньо впливає на стабільність функціонування держави, безпеку населення та розвиток економіки.

Нормативно-правове забезпечення у цій сфері формується Законом України «Про критичну інфраструктуру» [1], який визначає правові та організаційні засади функціонування системи захисту КІ. Важливу роль відіграють також постанови Кабінету Міністрів України, зокрема №1109 «Деякі питання забезпечення безпеки та стійкості критичної інфраструктури» [2], №518 «Про затвердження критеріїв віднесення об'єктів до категорій критичності» [3] та інші підзаконні акти, що регламентують класифікацію об'єктів КІ (ОКІ), порядок управління ризиками та взаємодію державних і приватних структур.

В умовах глобалізації та зростання міжсекторальних залежностей окремі інциденти можуть мати ефект «доміно», поширюючись від одного сектора КІ до іншого. Це вимагає



системного підходу до оцінки ризиків та розробки методів підвищення стійкості, які враховують технічні, організаційні, кібернетичні, правові та соціальні чинники.

Актуальність теми обумовлюється тим, що формування ефективної системи захисту та стійкості КІ є передумовою збереження державності, підтримання життєдіяльності суспільства та інтеграції України у європейський та світовий безпековий простір.

Постановка проблеми. У сучасних умовах зростання кількості та складності загроз, що спрямовані на об'єкти критичної інформаційної інфраструктури (ОКІІ), обумовлює необхідність створення формалізованих підходів до оцінювання та підвищення їх стійкості. На практиці існує потреба у методиках, які дозволяють враховувати багатовимірний характер стійкості, включаючи технічні, організаційні, правові та соціальні аспекти, а також забезпечують можливість кількісного аналізу.

Складність проблеми полягає у різноманітності вихідних даних, наявності значної кількості індикаторів та залежностей між ними, а також у динамічному характері ризиків, що виникають внаслідок військових дій, кібератак, природних та техногенних катастроф. Традиційні методи управління ризиками не завжди здатні комплексно враховувати зазначені фактори та забезпечувати адаптивність системи у кризових умовах. У цих умовах постає необхідність у проведенні фундаментальних наукових досліджень, спрямованих на пошук ефективних підходів до оцінювання стійкості ОКІІ, що поєднують теоретичні основи та практичну придатність для використання у національній системі безпеки.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Забезпечення належного рівня захисту КІ є пріоритетним завданням держави, оскільки від її стійкості залежить безпека громадян, економічна стабільність та обороноздатність країни. Обґрунтування методів оцінювання стійкості ОКІІ потребує системного аналізу наукових праць і публікацій у цій сфері. Дослідження існуючих вітчизняних і зарубіжних підходів дозволить простежити основні методи оцінювання та підвищення стійкості, визначити їх переваги та обмеження. Водночас різноманітність методик та відмінності у трактуванні ключових понять свідчать про відсутність єдиної уніфікованої системи. Це зумовлює необхідність критичного узагальнення існуючих підходів і визначення напрямів подальших наукових досліджень. Для вирішення завдань пов'язаних з забезпеченням та оцінюванням стійкості ОКІІ проведемо аналіз сучасних публікацій, опишемо існуючі підходи до визначення стійкості та проведемо їх порівняльний аналіз.

У роботі Плахотнюка Р. [4] представлено факторний підхід до забезпечення стійкості КІ України. Автор аналізує сучасні виклики, визначає ключові ризики та загрози, і пропонує системний аналіз чинників стійкості з метою розробки практичних заходів для зменшення вразливості та підвищення здатності до відновлення.

Герасименко О. у дослідженні [5] представив підхід забезпечення стійкості через класифікацію загроз ОКІ України в умовах воєнного стану. Автор акцентує увагу на правових, організаційних, технічних, кібернетичних та фізичних загрозах, підкреслюючи відсутність уніфікованого підходу до їхньої оцінки та системного врахування.

У статті [6] Третьяков О. представив кількісний підхід до оцінювання стійкості ОКІ. Запропоновано використання індексів та інтегральних показників, що враховують адаптивність, відновлюваність і толерантність до збоїв. Це дозволяє об'єктивно оцінювати рівень стійкості окремих об'єктів і систем у цілому.

Шкуропадська Д. [7] у своєму дослідженні представила інституційно-правовий підхід до забезпечення стійкості КІ. Автор аналізує законодавчу базу України, порівнює її з



практиками ЄС і НАТО, роблячи акцент на ролі державних органів та інституцій у створенні умов для підвищення стійкості.

Сокіран М. [8] у своїй статті розглянув адміністративно-правові засади забезпечення стійкості ОКІІ України. Автор обґрунтовує систему принципів адміністративно-правового регулювання у цій сфері, визначає роль державних інституцій у формуванні ефективної системи захисту та підкреслює важливість інтеграції правових і організаційних механізмів у процесі підвищення стійкості.

Суходоля О. [9] у своїй аналітичній доповіді здійснив комплексний огляд проблем забезпечення стійкості критичної енергетичної інфраструктури та життєдіяльності громад. Автор аналізує сучасні виклики та ризики в енергетичному секторі, акцентує на міжсекторальних залежностях і пропонує стратегічні напрями формування системи стійкості, що поєднують державні та місцеві механізми управління.

У статті [10] представлено загрозо-незалежний (threat-agnostic) підхід до оцінювання стійкості. Автори формулюють універсальні принципи — модульність, надлишковість, різноманітність, пластичність та розподіленість, які дозволяють інфраструктурі бути стійкою незалежно від природи загроз.

У дослідженні [11] представлено мережевий та оптимізаційний підхід до оцінювання стійкості інтерзалежних інфраструктур. За допомогою марковських процесів прийняття рішень (MDP) моделюється оптимальний розподіл ресурсів для ремонту та відновлення після збоїв, що дозволяє мінімізувати втрати.

У [12] готовність організацій до кібербезпеки розглядається як ключова передумова стійкості КІ. Автори доводять, що стійкість неможлива без належної підтримки керівництва, інвестицій у захист, розвиненої культури безпеки та підготовленого персоналу. Таким чином, кіберготовність інтерпретується як фундаментальний елемент забезпечення здатності систем протидіяти та відновлюватися після загроз.

У статті [13] представлено фазовий підхід CIERA (Critical Infrastructure Resilience Assessment), розширений за рахунок уваги до фази запобігання. Автори виділяють чотири етапи — запобігання, підготовка, реагування та відновлення — і пропонують конкретні критерії для оцінки стійкості на кожному з них.

У публікації [14] досліджено сталість міського транспорту в іранських мегаполісах. Автори досліджували рівень сталості транспортних систем. Хоча основна увага зосереджена на понятті «сталості», окремі індикатори мають безпосереднє значення для оцінювання стійкості транспортної інфраструктури, оскільки відображають її здатність підтримувати функціонування та адаптуватися до навантажень.

У табл. 1, враховуючи попереднє дослідження [15], систематизовано та представлено детальний аналіз підходів до забезпечення та оцінювання стійкості ОКІІ такими 10 критеріями (запропоновані автором).

1. Технічна надійність (TR) — здатність системи забезпечувати безперервне функціонування завдяки резервним ресурсам, альтернативним каналам постачання та стійкості до фізичних загроз.

2. Кіберстійкість (CR) — рівень захищеності інформаційних систем від кібератак, шкідливого ПЗ, витоків даних і здатність швидко відновлювати кіберфункціональність.

3. Оперативність відновлення (OR) — швидкість та ефективність реагування на надзвичайні ситуації, здатність відновлювати критично важливі функції.

4. Адаптивність і гнучкість (AF) — спроможність системи змінюватися у відповідь на нові загрози, впроваджувати інноваційні рішення та толерантність до дестабілізуючих чинників.



5. Система управління та координація (GC) — ефективність взаємодії між державними, приватними та міжнародними структурами, інтеграція механізмів управління ризиками.

6. Ресурсне забезпечення (RE) — рівень фінансування заходів із оцінювання стійкості, наявність кадрових і матеріальних ресурсів для їх реалізації.

7. Визначення категорії критичності (CC) — наявність методів чи алгоритмів поділу об'єктів на категорії критичності для пріоритизації захисту й ресурсів.

8. Модель PAAR (PAAR) — застосування фаз Prevent — Absorb — Adapt — Recover для аналізу здатності системи протидіяти загрозам.

9. Універсальність застосування (USA) — можливість використання підходу в різних секторах КІ.

10. Масштабність та рівень адаптації (SCL) — придатність методів як для державного, так і для регіонального чи місцевого рівнів.

Таблиця 1

Порівняльний аналіз підходів до оцінювання стійкості ОКП

№	Джерело	Критерії									
		TR	CR	OR	AF	GC	RE	CC	PAAR	USA	SCL
1.	Плахотнюк Р.	+	—	±	±	±	—	—	—	+	±
2.	Герасименко О.	+	+	—	—	±	—	—	—	+	±
3.	Третьяков О.	±	—	±	+	—	—	+	—	+	±
4.	Шкуропадська Д.	±	—	—	—	+	±	—	—	+	+
5.	Сокіран М.	—	—	—	—	+	—	—	—	±	+
6.	Суходоля О.	+	—	±	±	+	±	—	±	+	+
7.	Trump B. et al.	±	±	±	+	±	—	—	—	+	+
8.	Huang L. et al.	+	—	+	±	—	—	—	—	±	±
9.	Noor A. et al.	—	+	±	±	±	±	—	—	±	±
10.	Rehak D. et al.	+	—	+	±	±	—	—	+	+	±
11.	Alizadeh H. et al.	+	—	±	±	—	—	—	—	±	+

З табл. 1 видно, що жоден із проаналізованих підходів не охоплює всі критерії одночасно. Найчастіше розглядаються технічна надійність (TR), оперативність відновлення (OR) та адаптивність (AF), тоді як ресурсне забезпечення (RE) і визначення категорії критичності (CC) залишаються недостатньо розробленими. Вітчизняні дослідження більше зосереджені на правових, організаційних і координаційних аспектах, тоді як зарубіжні — на математичному моделюванні, кібербезпеці та загрозо-незалежних підходах. Недостатньо представлені критерії моделі (PAAR), універсальність застосування (USA) та масштабність (SCL), що вказує на наявність наукової прогалини. Це підкреслює необхідність розроблення інтегрованої методології, яка б поєднувала правові, організаційні та математичні інструменти для оцінювання стійкості ОКП, а також враховувала всі перелічені функціональні особливості та переваги.

Метою статті є розроблення розробка та експериментальне дослідження методу оцінювання стійкості ОКП держави.

ТЕОРЕТИЧНІ ОСНОВИ РОЗРОБКИ МЕТОДУ

Математичний опис методу оцінювання стійкості ОКП, з урахуванням [14], реалізується за допомогою наступних етапів:

Етап 1. Визначення множини ключових вимірів стійкості КІ

Для визначення загального переліку ключових вимірів стійкості КІ введемо множину $\mathbf{D}$ у наступному вигляді:

$$\mathbf{D} = \left\{ \bigcup_{i=1}^n D_i \right\} = \{D_1, D_2, \dots, D_n\}, \quad (1)$$

де $D_i \subseteq \mathbf{D} (i = \overline{1, n})$ — ключові виміри стійкості КІ, n — загальна кількість вимірів стійкості.

Етап 2. Визначення множини індикаторів, що характеризують ключові виміри стійкості КІ

Для визначення переліку індикаторів, що характеризують ключові виміри стійкості D_i , введемо множину $\mathbf{I}$ у наступному вигляді:

$$\mathbf{I}_i = \left\{ \bigcup_{j=1}^{m_i} I_{ij} \right\} = \{I_{i1}, I_{i2}, \dots, I_{im_i}\}, \quad (2)$$

де $I_{ij} \subseteq \mathbf{I}_i (i = \overline{1, n}; j = \overline{1, m_i})$ — індикатори, що відповідають виміру стійкості D_i , m_i — кількість індикаторів для відповідного виміру D_i .

Етап 3. Визначення множини змінних, що характеризують певний індикатор для відповідного виміру

Для визначення переліку змінних, що характеризують певний індикатор I_i для відповідного виміру D_i , введемо множину $\mathbf{X}_{ij}$ у наступному вигляді:

$$\mathbf{X}_{ij} = \left\{ \bigcup_{k=1}^{p_{ij}} X_{ijk} \right\} = \{X_{ij1}, X_{ij2}, \dots, X_{ijp_{ij}}\}, \quad (3)$$

де $X_{ijk} \subseteq \mathbf{X}_{ij} (i = \overline{1, n}; j = \overline{1, m_i}; k = \overline{1, p_{ij}})$ — змінні, що характеризують певний індикатор I_i , p_{ij} — кількість значень j -ї змінної i -го виміру.

Етап 4. Ранжування індикаторів у кожному вимірі

Крок 4.1. Оцінювання відносної важливості індикаторів та змінних за допомогою методу нечіткої Делфі-аналітичної ієрархії (FDAHP).

Для аналізу з використанням моделі FDAHP, використовуються нечіткі числа у формі трикутника — це нечіткі трикутні числа (НТЧ) (див. рис. 1) [14], які представляють агрегацію нечітких оцінок, придатних для роботи з суб'єктивною експертною інформацією. Оцінки відносної важливості надаються відповідно до критеріїв, наведених у табл. 2.

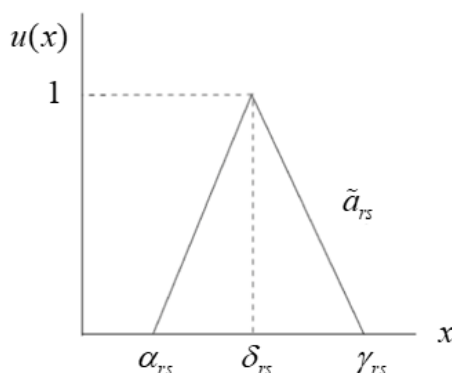


Рис. 1. Функція належності НТЧ

Таблиця 2

Шкала важливості для оцінювання у методі FDAHP

Шкала важливості	Оцінка	НТЧ	Опис
Дуже важливо	9	7, 9, 9	Дуже важливо, вказує на те, що індикатор є дуже значущим для оцінювання стійкості КІ
Важливо	7	5, 7, 9	Важливо, вказує на те, що індикатор є значущим для оцінювання стійкості КІ
Помірно важливо	5	3, 5, 7	Помірно важливо, вказує на те, що індикатор має середню значущість для оцінювання стійкості КІ
Маловажливо	3	1, 3, 5	Мало важливо, вказує на те, що індикатор є незначущим для оцінювання стійкості КІ
Дуже маловажливо	1	1, 1, 3	Дуже неважливо, вказує на те, що індикатор є зовсім незначущим для оцінювання стійкості КІ

Як видно з табл. 2, оцінки варіюються від 9 (дуже високий рівень важливості для оцінювання стійкості КІ) до 1 (дуже низький рівень важливості). Після збору даних усі ваги будуть перетворені на НТЧ для аналізу за допомогою методу FDAHP. Згідно з логікою трикутних нечітких чисел, максимальні та мінімальні значення оцінок експертів реєструються як граничні точки, а геометричне середнє визначається як ступінь належності трикутних нечітких чисел.

Трикутні нечіткі числа обчислюються з використанням [14] та за допомогою (4).

$$\tilde{a}_{rs} = (a_{rs}, \delta_{rs}, \gamma_{rs}), \quad (4)$$

$$\alpha_{rs} = \text{Min}(\beta_{rst}), (r, s, t = \overline{1, f}), \quad (5)$$

$$\delta_{rs} = \left(\prod_{t=1}^f \beta_{rst} \right)^{\frac{1}{3}}, \quad (6)$$

$$\gamma_{rs} = \text{Max}(\beta_{rst}), (r, s, t = \overline{1, f}). \quad (7)$$

Крок 4.2. Обчислення нечітких ваг кожного індикатора.

На основі нечітких чисел розробляється матриця парних порівнянь для параметрів, як показано у рівняннях (8) та (9).

$$\tilde{A} = [\tilde{a}_{rs}]_{f \times f}, \tilde{a}_{rs} \otimes \tilde{a}_{sr}, r, s = \overline{1, f}, \quad (8)$$

$$\tilde{A} = \begin{bmatrix} (1, 1, 1) \dots (\alpha_{12}, \delta_{12}, \gamma_{12}) \dots (\alpha_{13}, \delta_{13}, \gamma_{13}) \\ (\frac{1}{\gamma_{12}}, \frac{1}{\delta_{12}}, \frac{1}{\alpha_{12}}) \dots (1, 1, 1) \dots (\alpha_{23}, \delta_{23}, \gamma_{23}) \\ (\frac{1}{\gamma_{13}}, \frac{1}{\delta_{13}}, \frac{1}{\alpha_{13}}) \dots (\frac{1}{\gamma_{23}}, \frac{1}{\delta_{23}}, \frac{1}{\alpha_{23}}) \dots (1, 1, 1) \end{bmatrix} \quad (9)$$

Відносні нечіткі ваги параметрів обчислюються за допомогою виразів (10) та (11). У цих рівняннях символ $\otimes$ позначає множення нечітких чисел, а $\oplus$ позначає додавання нечітких чисел [14].

$$(\tilde{Z}_r = \tilde{a}_{rs} \otimes \dots \otimes \tilde{a}_{rs})^{\frac{1}{f}}, \quad (10)$$

$$\tilde{W}_r = \tilde{Z}_r \otimes \tilde{Z}_r \otimes \dots \otimes \tilde{Z}_r). \quad (11)$$

Крок 4.3. Обчислення ієрархії важливості індикаторів у кожному вимірі.

Цей етап включає перетворення нечітких чисел у чіткі числа на основі методу геометричного середнього.

$$W_r = \left(\prod_{s=1}^f w_{rs} \right)^{\frac{1}{3}}. \quad (12)$$

Крок 4.4. Графічне відображення ієрархії важливості індикаторів у кожному вимірі.

Для графоаналітичного представлення ієрархії важливості індикаторів у певному вимірі, будується діаграма (рис. 2), яка для кожного виміру стійкості D_i відображає обчислені за (12) ранги індикаторів W_i .

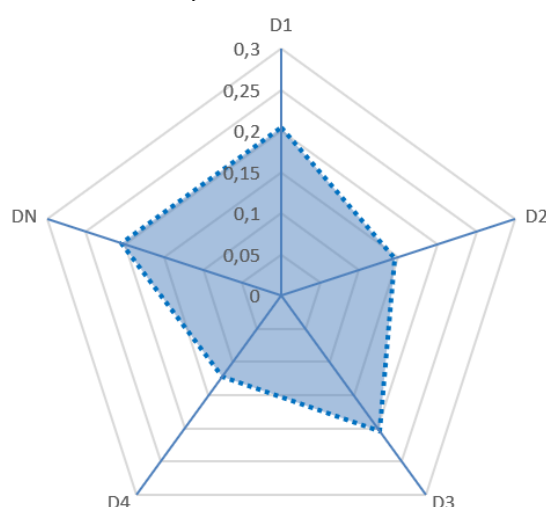


Рис. 2. Формальне представлення діаграми важливості індикаторів певного виміру D_i

Етап 5. Нормалізація значень змінних індикаторів

Оскільки змінні індикаторів можуть мати різні одиниці виміру, необхідно привести їх до єдиної шкали (до уніфікованого діапазону від 0 до 1), щоб забезпечити адекватність подальшого зважування та обчислення, у наступному вигляді:

$$X_{ij}^N = \frac{X_{ij}^A}{X_{ij}^R}, 0 \leq X_{ij} \leq 1, \quad (13)$$

де X_{ij}^N — нормалізоване значення змінної j в індикаторі i , X_{ij}^A — фактичне значення змінної, X_{ij}^R — максимальне можливе або еталонне значення, що задає верхню межу ефективності.

Етап 6. Розрахунок інтегрального показника стійкості

Крок 6.1. Обчислення часткової оцінки за кожним виміром стійкості.

Кожен вимір має набір нормалізованих індикаторів. Для інтеграції цих значень у єдиний показник використовують зважену суму:

$$S_i = \sum_{j=1}^{m_i} W_{ij} \cdot X_{ij}^N, \quad (14)$$



де S_i — інтегральна оцінка виміру, m_i — кількість індикаторів у вимірі, W_{ij} — вага індикатора у вимірі, X_{ij}^N — нормалізоване значення змінної індикатора.

Крок 6.2. Обчислення загального показника стійкості (PKOKI).

Отримані часткові оцінки об'єднуються у єдиний агрегований показник стійкості:

$$PKOKI = \sum_{i=1}^n V_i \cdot S_i, \quad (15)$$

де $PKOKI$ — зведений інтегральний показник стійкості ОКП [2], n — кількість ключових вимірів, V_i — вага виміру, S_i — інтегральна оцінка за виміром.

Етап 7. Визначення категорії критичності

В залежності від отриманого за (15) значення $PKOKI$ та відповідно до Постанови КМУ №1109 [2], об'єкту присвоюється визначена за допомогою табл. 3 категорія критичності.

Таблиця 3

Визначення категорії критичності об'єкта відповідно до значення PKOKI

Категорія	Діапазон значень PKOKI	Опис
I категорія	$0.80 < PKOKI \leq 1.00$	Надзвичайно критичний
II категорія	$0.63 < PKOKI \leq 0.80$	Дуже критичний
III категорія	$0.37 < PKOKI \leq 0.63$	Значущий
IV категорія	$0.20 < PKOKI \leq 0.37$	Помірна важливість
Не критичний	$PKOKI \leq 0.20$	Низький рівень впливу

Етап 8. Моделювання циклу стійкості (за моделлю P-A-A-R)

Оцінювання відбувається шляхом аналізу готовності об'єкта до повного циклу стійкості, з використанням моделі «Predict–Absorb–Adapt–Recover» [9], [13], яка враховує здатність об'єкта KI:

- Прогнозувати потенційні загрози (Predict);
- Поглинати/витримувати удар (Absorb);
- Адаптуватися до нових умов (Adapt);
- Відновлювати функціональність (Recover).

Для цього обчислюється коефіцієнт системної готовності (KSG):

$$KSG = \frac{P + A + A + R}{4}, \quad (16)$$

де KSG — середня здатність системи до проходження всіх фаз життєвого циклу стійкості [13], $KSG \in [0,1]$, P, A, A, R — нормалізовані (або експертні) оцінки відповідних фаз.

Етап 9. Розрахунок кінцевого (скоригованого) показника стійкості

Кінцевий показник стійкості об'єкта (PKOKI) коригується за формулою:

$$PKOKI_{new} = PKOKI \cdot KSG, \quad (17)$$

де $PKOKI$ — зведений інтегральний показник стійкості ОКП визначений за (15), KSG — середня здатність системи до проходження всіх фаз життєвого циклу стійкості,

Це дозволяє врахувати не тільки поточний рівень захищеності, а й потенціал системи до динамічного реагування та відновлення.



ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ МЕТОДУ ОЦІНЮВАННЯ СТІЙКОСТІ ОКП

Експериментальне дослідження методу реалізується за допомогою вище зазначених етапів і передбачає систематизацію чинних нормативно-правових засад з метою обґрунтованого виділення вимірів, індикаторів і змінних та подальшого обрахунку інтегрального показника стійкості ОКП держави.

Етап 1. Відповідно запропонованого методу, розглянемо приклад формування загального переліку ключових вимірів стійкості КІ згідно [2], при $n = 6$ з урахуванням (1), визначимо множину вимірів стійкості КІ таким чином:

$$D_{RCI} = \{\bigcup_{i=1}^6 D_i\} = \{D_1, D_2, \dots, D_6\} = \{D_{ECON}, D_{SOC}, D_{ECOL}, D_{SEC}, D_{DEF}, D_{GOV}\},$$

де D_{ECON} — економічний вимір, D_{SOC} — соціальний вимір, D_{ECOL} — екологічний вимір, D_{SEC} — вимір громадської безпеки, D_{DEF} — вимір оборони, D_{GOV} — вимір державного управління згідно [1]–[3].

Етап 2. Для множини вимірів стійкості $D_{ECON}, D_{SOC}, D_{SEC}$, при $n = 1, m_1 = 5$, $n = 2, m_2 = 5$ та $n = 4, m_4 = 5$ з використанням (2) представимо множину індикаторів $I_1 = I_{ECON}$, $I_2 = I_{SOC}$, $I_4 = I_{SEC}$ у вигляді табл. 4 згідно [1]–[3].

Таблиця 4

Представлення множин індикаторів стійкості

Вимір	Значення n, m_i	Індикатор	Назва індикатору
$D_{ECON} = ECO$	$n = 1, m_1 = 5$	$I_{ECON1} = ECO1$	Частка бюджету на утримання КІ
		$I_{ECON2} = ECO2$	Економічна ефективність
		$I_{ECON3} = ECO3$	Диверсифікація джерел фінансування
		$I_{ECON4} = ECO4$	Рівень резервного потенціалу
		$I_{ECON5} = ECO5$	Інвестиції в інновації
$D_{SOC} = SOC$	$n = 2, m_2 = 5$	$I_{SOC1} = SOC1$	Забезпеченість базовими послугами
		$I_{SOC2} = SOC2$	Оперативність реагування
		$I_{SOC3} = SOC3$	Наявність систем оповіщення
		$I_{SOC4} = SOC4$	Рівень залучення персоналу
		$I_{SOC5} = SOC5$	Соціальна вразливість
$D_{SEC} = SEC$	$n = 4, m_4 = 5$	$I_{SEC1} = SEC1$	Наявність систем фізичної охорони
		$I_{SEC2} = SEC2$	Відеоспостереження та контроль доступу
		$I_{SEC3} = SEC3$	Час реагування охорони
		$I_{SEC4} = SEC4$	Наявність планів евакуації
		$I_{SEC5} = SEC5$	Навчання з безпеки персоналу

Етап 3. Для множини індикаторів визначених на Етапі 2 індикаторів, з використанням (3) представимо множини змінних у вигляді табл. 5 згідно [1]–[3].



Таблиця 5

Представлення множин змінних індикаторів стійкості

Індикатор	Значення n, m, p_{ij}	Індикатор	Назва індикатору
$I_{ECON1} = ECO1$	$n = 1, m_1 = 1, p_{1.1} = 2$	$X_{ECON1.1} = ECO1.1$	Відсоток фінансування об'єкта у загальному бюджеті галузі
		$X_{ECON1.2} = ECO1.2$	Обсяг річного фінансування у гривнях
$I_{ECON2} = ECO2$	$n = 1, m_1 = 2, p_{1.2} = 2$	$X_{ECON2.1} = ECO2.1$	Співвідношення витрат до обсягу виробленої/переданої продукції
		$X_{ECON2.2} = ECO2.2$	Питомі витрати на одиницю продукції
$I_{ECON3} = ECO3$	$n = 1, m_1 = 3, p_{1.3} = 2$	$X_{ECON3.1} = ECO3.1$	Кількість джерел фінансування
		$X_{ECON3.2} = ECO3.2$	Частка приватного/державного капіталу
$I_{ECON4} = ECO4$	$n = 1, m_1 = 4, p_{1.4} = 2$	$X_{ECON4.1} = ECO4.1$	Обсяг резервного обладнання, палива або матеріалів
		$X_{ECON4.2} = ECO4.2$	Тривалість автономної роботи системи (у годинах)
$I_{ECON5} = ECO5$	$n = 1, m_1 = 5, p_{1.5} = 2$	$X_{ECON5.1} = ECO5.1$	Частка бюджету на інновації або R&D
		$X_{ECON5.2} = ECO5.2$	Наявність затверджених інноваційних проєктів (так/ні)
$I_{SOC1} = SOC1$	$n = 2, m_2 = 1, p_{2.1} = 2$	$X_{SOC1.1} = SOC1.1$	Частка населення, яке має доступ до базових послуг під час НС
		$X_{SOC1.2} = SOC1.2$	Середня кількість годин без доступу до послуг у кризу
$I_{SOC2} = SOC2$	$n = 2, m_2 = 2, p_{2.2} = 2$	$X_{SOC2.1} = SOC2.1$	Середній час прибуття аварійних служб
		$X_{SOC2.2} = SOC2.2$	Частота інцидентів із затримкою реагування
$I_{SOC3} = SOC3$	$n = 2, m_2 = 3, p_{2.3} = 2$	$X_{SOC3.1} = SOC3.1$	Покриття населення системами оповіщення, у %
		$X_{SOC3.2} = SOC3.2$	Наявність резервних каналів сповіщення (так/ні)
$I_{SOC4} = SOC4$	$n = 2, m_2 = 4, p_{2.4} = 2$	$X_{SOC4.1} = SOC4.1$	Кількість навчань/тренувань персоналу за рік
		$X_{SOC4.2} = SOC4.2$	Відсоток персоналу, що пройшов навчання
$I_{SOC5} = SOC5$	$n = 2, m_2 = 5, p_{2.5} = 2$	$X_{SOC5.1} = SOC5.1$	Кількість соціально вразливих осіб без доступу до КІ
		$X_{SOC5.2} = SOC5.2$	Частка таких осіб серед загального населення
$I_{SEC1} = SEC1$	$n = 4, m_4 = 1, p_{4.1} = 2$	$X_{SEC1.1} = SEC1.1$	Чисельність охоронного персоналу
		$X_{SEC1.2} = SEC1.2$	Відсоток території, охопленої відеонаглядом
$I_{SEC2} = SEC2$	$n = 4, m_4 = 2, p_{4.2} = 2$	$X_{SEC2.1} = SEC2.1$	Наявність системи контролю доступу (так/ні)
		$X_{SEC2.2} = SEC2.2$	Середній час реагування охорони (хвилини)



$I_{SEC3} = SEC3$	$n = 4, m_4 = 3, p_{4,3} = 2$	$X_{SEC3.1} = SEC3.1$	Кількість інцидентів з перевищенням допустимого часу реагування
		$X_{SEC3.2} = SEC3.2$	Наявність плану евакуації (так/ні)
$I_{SEC4} = SEC4$	$n = 4, m_4 = 4, p_{4,4} = 2$	$X_{SEC4.1} = SEC4.1$	Кількість тренувань з евакуації за рік
		$X_{SEC4.2} = SEC4.2$	Кількість навчань з безпеки на рік
$I_{SEC5} = SEC5$	$n = 4, m_4 = 5, p_{4,5} = 2$	$X_{SEC5.1} = SEC5.1$	Частка персоналу, охопленого навчаннями
		$X_{SEC5.2} = SEC5.2$	Чисельність охоронного персоналу

Етап 4. Ранжування індикаторів у кожному вимірі.

Крок 4.1. Оцінювання відносної важливості індикаторів та змінних за допомогою методу нечіткої Делфі-аналітичної ієрархії (FDAHP).

Відповідно до логіки трикутних нечітких чисел (рис. 1), максимальні та мінімальні значення оцінок експертів реєструються як граничні точки (табл. 2), а геометричне середнє визначається як ступінь належності трикутних нечітких чисел.

Представимо у вигляді табл. 6 систематизовані дані оцінки важливості індикаторів стійкості, а у вигляді табл. 7 дані оцінки важливості змінних індикаторів стійкості визначені за (4) – (7).

Таблиця 6

Оцінка важливості індикаторів стійкості

Індикатор	Оцінка (W_i)	НТЧ
ECO1	7	5, 7, 9
ECO2	5	3, 5, 7
ECO3	7	5, 7, 9
ECO4	9	7, 9, 9
ECO5	7	5, 7, 9
SOC1	9	7, 9, 9
SOC2	7	5, 7, 9
SOC3	5	3, 5, 7
SOC4	5	3, 5, 7
SOC5	7	5, 7, 9
DEC1	7	5, 7, 9
DEC2	5	3, 5, 7
DEC3	7	5, 7, 9
DEC4	9	7, 9, 9
DEC5	7	5, 7, 9

Таблиця 7

Оцінка важливості змінних індикаторів стійкості

Змінна	Оцінка (W_i)	НТЧ
ECO1.1	3	1, 3, 5
ECO1.2	5	3, 5, 7
ECO2.1	5	3, 5, 7
ECO2.2	5	3, 5, 7
ECO3.1	5	3, 5, 7



ECO3.2	7	5, 7, 9
ECO4.1	7	5, 7, 9
ECO4.2	5	3, 5, 7
ECO5.1	5	3, 5, 7
ECO5.2	7	5, 7, 9
SOC1.1	5	3, 5, 7
SOC1.2	5	3, 5, 7
SOC2.1	3	1, 3, 5
SOC2.2	3	1, 3, 5
SOC3.1	7	5, 7, 9
SOC3.2	5	3, 5, 7
SOC4.1	3	1, 3, 5
SOC4.2	7	5, 7, 9
SOC5.1	7	5, 7, 9
SOC5.2	5	3, 5, 7
SEC1.1	3	1, 3, 5
SEC1.2	7	5, 7, 9
SEC2.1	3	1, 3, 5
SEC2.2	7	5, 7, 9
SEC3.1	7	5, 7, 9
SEC3.2	7	5, 7, 9
SEC4.1	5	3, 5, 7
SEC4.2	5	3, 5, 7
SEC5.1	3	1, 3, 5
SEC5.2	7	5, 7, 9

Крок 4.2. Обчислення нечітких ваг кожного індикатора.

На основі нечітких чисел розробимо матриці парних порівнянь для параметрів, як показано у рівняннях (8) – (11), та представимо у вигляді табл. 8.

Таблиця 8

Матриця попарних порівнянь

Вимір	α	β	γ
ECO як базовий			
ECO	1.0	1.0	1.0
SOC	0.311	0.428	0.538
SEC	0.331	0.405	0.464
SOC як базовий			
ECO	0.686	0.746	0.842
SOC	1.0	1.0	1.0
SEC	0.539	0.656	0.722
SEC як базовий			
ECO	0.341	0.447	0.501
SOC	0.533	0.674	0.752
SEC	1.0	1.0	1.0

Крок 4.3. Обчислення ієрархії важливості індикаторів у кожному вимірі.

Процес перетворення нечітких чисел у чіткі числа на основі методу геометричного середнього та (12) представлено у табл. 9.

Таблиця 9

Нечіткі ваги кожного індикатора та ранг важливості у кожному вимірі

Індикатор	Wi (L)	Wi (M)	Wi (U)	Wi (δ)	Ранг
ECO1	0.1456	0.2039	0.2621	0.2039	2
ECO2	0.0874	0.1456	0.2039	0.1456	5
ECO3	0.1456	0.2039	0.2621	0.2039	3
ECO4	0.2039	0.2621	0.2621	0.2427	1
ECO5	0.1456	0.2039	0.2621	0.2039	4
SOC1	0.161	0.2372	0.2897	0.2293	3
SOC2	0.1945	0.2732	0.3264	0.2647	1
SOC3	0.0917	0.1565	0.2069	0.1517	5
SOC4	0.1925	0.2547	0.3101	0.2524	2
SOC5	0.1416	0.2175	0.2768	0.212	4
SEC1	0.1303	0.1806	0.2382	0.1830	2
SEC2	0.0828	0.1567	0.2095	0.1497	5
SEC3	0.1296	0.195	0.2475	0.1907	1
SEC4	0.1026	0.1806	0.2345	0.1726	4
SEC5	0.1226	0.1824	0.2366	0.1805	3

Крок 4.4. Графічне відображення ієрархії важливості індикаторів у кожному вимірі.

Побудуємо діаграми (рис. 3), які для кожного виміру стійкості D_i відображають обчислені за (12) та табл. 9 ранги індикаторів W_i .

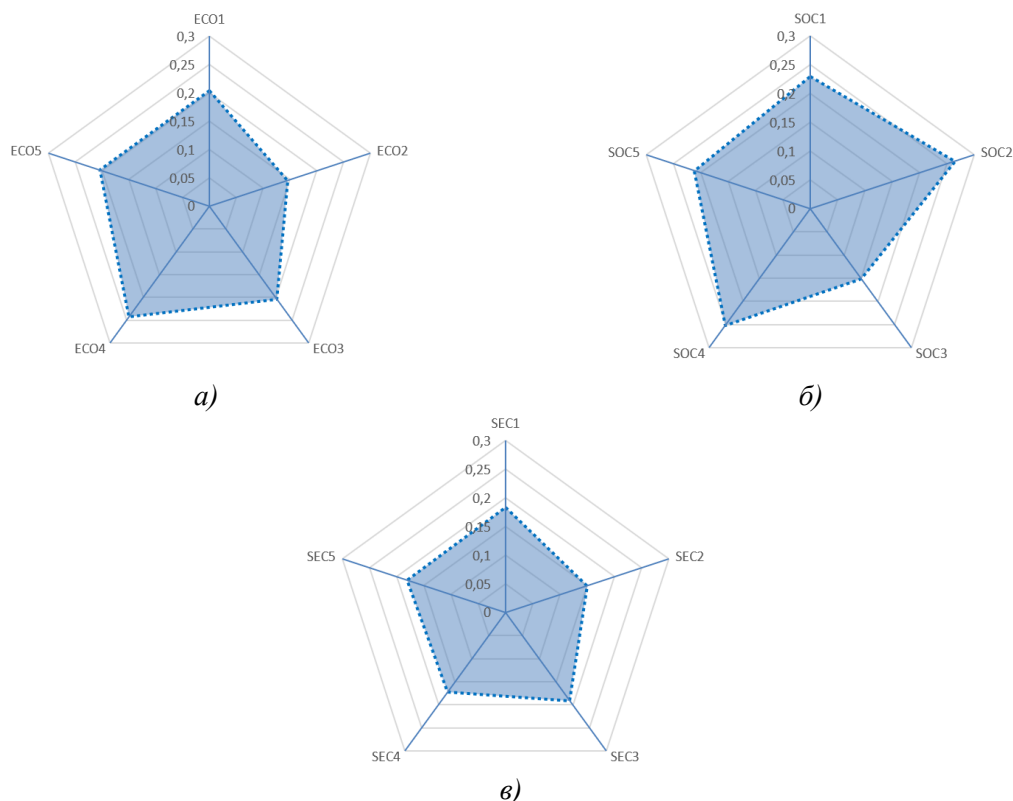


Рис. 3. Представлення діаграм важливості індикаторів:

а) вимір стійкості D_{ECON} , б) вимір стійкості D_{SOC} , в) вимір стійкості D_{SEC}

**Етап 5 – Етап 9. Розрахунок інтегрального та кінцевого (скоригованого) показників стійкості**

Процес обчислення інтегрального та кінцевого показників стійкості за допомогою (13) – (17) та табл. 2 представлено у табл. 10.

*Таблиця 10***Нечіткі ваги кожного індикатора та ранг важливості у кожному вимірі**

Вимір	S_i	V_i	$PKOKI$	KSG	$PKOKI_{new}$
ECO	0.602	0.15	0.0903	0.9	0.558
SOC	0.704	0.20	0.1408	0.8	0.528
SEC	0.824	0.25	0.2060	0.91	0.7735

З табл. 10 видно, що обчислення інтегрального та кінцевого показників стійкості у трьох вимірах показало, що найбільш значущим чинником стійкості є безпековий вимір (SEC), який отримав найвищий інтегральний та скоригований показник (0.7735). Це свідчить про визначальну роль заходів безпеки у оцінюванні і забезпеченні стійкості КІ. Дещо нижчі значення спостерігаються у економічному (ECO) та соціальному (SOC) вимірах (0.558 та 0.528 відповідно), що вказує на їх важливість, але менш критичний вплив порівняно з безпековими факторами. Таким чином, інтегральний та кінцевий (скоригований) показники демонструють, що для забезпечення високого рівня стійкості ОКІІ ключовим є пріоритетний розвиток безпекового компонента при одночасному збалансуванні економічних і соціальних чинників.

ВИСНОВКИ

У роботі було проведено комплексний аналіз сучасних підходів до оцінювання стійкості ОКІІ. Він охоплював як вітчизняні, так і зарубіжні наукові публікації, що дозволило виявити їх сильні та слабкі сторони. Результати показали, що жоден із існуючих підходів не забезпечує повного охоплення всіх ключових критеріїв стійкості. Найчастіше дослідження зосереджуються на технічній надійності, здатності до відновлення та адаптивності, тоді як питання ресурсного забезпечення, визначення категорії критичності та масштабованості підходів залишаються недостатньо дослідженими. Це свідчить про наявність важливого наукового завдання щодо розробки інтегрованого методу, здатного враховувати як технічні, так і організаційно-правові та соціально-економічні аспекти.

Було розроблено метод оцінювання стійкості ОКІІ, який базується на багатовимірній системі індикаторів і методах нечіткого аналізу, що забезпечує гнучке ранжування факторів ризику та уніфікований підхід до нормалізації змінних. Важливо, що у запропонованому методі вперше інтегровано модель життєвого циклу стійкості (P–A–A–R), яка дозволяє розраховувати категорію критичності двічі: перший раз — на основі інтегрального показника РКОКІ, а другий — з урахуванням здатності системи прогнозувати, поглинати впливи, адаптуватися та відновлюватися. Це дає змогу отримати більш точну та динамічну оцінку стійкості, що враховує як поточний рівень захищеності, так і потенціал інфраструктури до реагування в умовах змін середовища. Таким чином, метод забезпечує науково обґрунтовану основу для прийняття рішень щодо управління ризиками, посилення національної безпеки та формування адаптивних політик у сфері захисту КІ.

Крім того, у роботі було проведено експериментальне дослідження, спрямоване на апробацію запропонованого методу на трьох основних вимірах стійкості: економічному,



соціальному та безпековому. Результати показали, що найбільший вплив на загальний рівень стійкості має безпековий вимір, який продемонстрував найвищі інтегральні значення та скориговані показники. Водночас економічний і соціальний виміри, хоча й поступаються за впливовістю, відіграють важливу роль у формуванні збалансованої системи стійкості.

Продовженням даного дослідження стане верифікація запропонованого методу на розширеній вибірці, що охоплюватиме всі можливі виміри стійкості для різних міст та регіонів нашої держави. Це дозволить оцінити універсальність та масштабованість методики, перевірити її ефективність у різних секторах КІ та виробити практичні рекомендації для державних органів і операторів КІ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про критичну інфраструктуру» (2021). №1882-IX. <https://zakon.rada.gov.ua/laws/show/1882-20>.
2. Кабінет Міністрів України. (2021). Постанова №1109 «Деякі питання забезпечення безпеки та стійкості критичної інфраструктури» від 09.10.2021. <https://zakon.rada.gov.ua/laws/show/1109-2021-%D0%BF>.
3. Кабінет Міністрів України. (2022). Постанова №518 «Про затвердження критеріїв віднесення об'єктів до категорій критичності» від 13.05.2022. <https://zakon.rada.gov.ua/laws/show/518-2022-%D0%BF>.
4. Плахотнюк, Р. В. (2024). Забезпечення стійкості критичної інфраструктури в Україні в умовах сучасних викликів. Економічний простір, 195(47–54). <https://economic-prostir.com.ua/wp-content/uploads/2024/12/195-47-54-plahotnyuk.pdf>.
5. Герасименко, О. М. (2024). Загрози об'єктам критичної інфраструктури України в умовах воєнного стану. Науковий вісник Ужгородського національного університету. Серія: Право, 84(3). <https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/09/41-2.pdf>.
6. Третьяков, О. В., Халмурадов, Б. Д., Кічата, Н. М., & Ремська, А. В. (2025). Підхід до кількісної оцінки стійкості об'єктів критичної інфраструктури. Системи управління, навігації та зв'язку, 1(79), 178–183. <https://doi.org/10.26906/SUNZ.2025.1.178-183>.
7. Шкуропадська, Д. (2025). Інституційне забезпечення стійкості критичної інфраструктури. Scientia Fructuosa (KHTEU). <https://journals.knute.edu.ua/scientia-fructuosa/article/view/2225>.
8. Сокиран, М. В. (2020). Система принципів адміністративно-правового забезпечення стійкості критичної інформаційної інфраструктури України. Наукові записки. Серія: Право, (8, спецвип.), 73–77. https://cusu.edu.ua/images/nauk_zapiski/pravo/8_spec_2020/73-77.pdf.
9. Суходоля, О. М. (2024). Стійкість критичної енергетичної інфраструктури та життєдіяльності громад: Аналітична доповідь. Київ: НІСД. https://niss.gov.ua/sites/default/files/2024-05/ad_sukhodolia_resilience_29052024.pdf.
10. Trump, B. D., Mitoulis, S., Argyroudis, S., Kiker, G., Palma-Oliveira, J., Horton, R., Pescaroli, G., Pinigina, E., Trump, J., & Linkov, I. (2025). Threat-agnostic resilience: Framing and application for critical infrastructure. International Journal of Disaster Risk Reduction. <https://arxiv.org/abs/2501.01318>.
11. Huang, L., Chen, J., & Zhu, Q. (2018). Distributed and optimal resilient planning of large-scale interdependent critical infrastructures. Proceedings of the Winter Simulation Conference. <https://arxiv.org/abs/1809.02231>.
12. Ahmad Fairuz Mohamed Noor, Sedigheh Moghavvemi & Farzana Parveen Tajudeen. (2025) Identifying key factors of cybersecurity readiness in organizations: Insights from Malaysian critical infrastructure. Computers & Security 159, pages 104674.
13. Rehak, D., Flynnova, L., Hromada, M., & Fuggini, C. (2023). The importance of resistance in the context of critical infrastructure resilience: An extension of the CIERA method. Systems, 11(10), 506. <https://doi.org/10.3390/systems11100506>.
14. Alizadeh, H., Sharifi, A., Kamelifar, M.J. et al. A Study on the Sustainability of Urban Transportation in Iranian Metropolitan Areas. Transp. in Dev. Econ. 9, 8 (2023). <https://doi.org/10.1007/s40890-023-00178-7>.
15. Сидоренко, В., & Максимець, А. (2025). Модель забезпечення стійкості критичних інформаційних систем в умовах впливу внутрішніх та зовнішніх дестабілізуючих чинників. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(27), 560–571. <https://doi.org/10.28925/2663-4023.2025.27.779>.

**Viktoriia Sydorenko**

PhD, Associate Professor,

Associate Professor of the Department of Computer Information Technologies

State University "Kyiv Aviation Institute", Kyiv, Ukraine

ORCID ID: 0000-0002-5910-0837

v.sydorenko@ukr.net

METHOD FOR ASSESSING THE RESILIENCE OF CRITICAL INFORMATION INFRASTRUCTURE OBJECTS OF THE STATE

Abstract. In the modern context of increasing number and complexity of threats, the issue of assessing the resilience of critical information infrastructure (CII) objects becomes of paramount importance for the national security of the state. The vulnerability of infrastructural systems, combined with intersectoral dependencies, necessitates the application of integrated and scientifically grounded approaches to the assessment of CII and the enhancement of their resilience. The article presents an integrated method for assessing the resilience of CII, which combines a multidimensional system of indicators, fuzzy analysis methods, unified variable normalization, and categorization of objects in accordance with current regulatory documents. For the first time, the resilience life cycle model (P–A–R) has been integrated into the assessment process, enabling a dual calculation of the criticality category: the primary one – based on the integral indicator PKOKI, and the secondary one – taking into account the system's ability to predict, absorb impacts, adapt, and recover. An experimental study conducted on the example of three resilience dimensions (economic, social, and security) confirmed the priority of the security aspect while simultaneously demonstrating the significance of economic and social factors in shaping a balanced system. The results of the study have practical value for state and private entities responsible for protecting critical infrastructure, as they provide a foundation for strategic risk management and the development of adaptive policies. Further research will be aimed at verifying the method across all dimensions of resilience for different cities of the state in order to confirm its universality and scalability.

Keywords: critical infrastructure, critical information infrastructure objects, cybersecurity, resilience, resilience assessment, fuzzy analysis, risk management, criticality, criticality categories.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Law of Ukraine «On Critical Infrastructure» (2021). No. 1882-IX. <https://zakon.rada.gov.ua/laws/show/1882-20>
2. Cabinet of Ministers of Ukraine. (2021). Resolution No. 1109 «Certain issues of ensuring the security and resilience of critical infrastructure» (October 9, 2021). <https://zakon.rada.gov.ua/laws/show/1109-2021-%D0%BF>
3. Cabinet of Ministers of Ukraine. (2022). Resolution No. 518 «On approval of the criteria for classifying objects by categories of criticality» (May 13, 2022). <https://zakon.rada.gov.ua/laws/show/518-2022-%D0%BF>
4. Plakhotnyuk, R. V. (2024). Ensuring the resilience of critical infrastructure in Ukraine under modern challenges. *Economic Space*, 195, 47–54. <https://economic-prostir.com.ua/wp-content/uploads/2024/12/195-47-54-plakhotnyuk.pdf>
5. Herasymenko, O. M. (2024). Threats to critical infrastructure objects of Ukraine under martial law. *Scientific Bulletin of Uzhhorod National University. Series: Law*, 84(3). <https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/09/41-2.pdf>
6. Tretiakov, O. V., Khalmuradov, B. D., Kichata, N. M., & Remska, A. V. (2025). An approach to quantitative assessment of the resilience of critical infrastructure objects. *Control, Navigation and Communication Systems*, 1(79), 178–183. <https://doi.org/10.26906/SUNZ.2025.1.178-183>
7. Shkuropadska, D. (2025). Institutional support for the resilience of critical infrastructure. *Scientia Fructuosa (KNUTE)*. <https://journals.knute.edu.ua/scientia-fructuosa/article/view/2225>



8. Sokiran, M. V. (2020). The system of principles of administrative and legal support for the resilience of Ukraine's critical information infrastructure. *Scientific Notes. Series: Law*, 8(Special Issue), 73–77. https://cusu.edu.ua/images/nauk_zapiski/pravo/8_spec_2020/73-77.pdf
9. Sukhodolia, O. M. (2024). Resilience of critical energy infrastructure and community life: Analytical report. Kyiv: National Institute for Strategic Studies. https://niss.gov.ua/sites/default/files/2024-05/ad_sukhodolia_resilience_29052024.pdf
10. Trump, B. D., Mitoulis, S., Argyroudis, S., Kiker, G., Palma-Oliveira, J., Horton, R., Pescaroli, G., Pinigina, E., Trump, J., & Linkov, I. (2025). Threat-agnostic resilience: Framing and application for critical infrastructure. *International Journal of Disaster Risk Reduction*. <https://arxiv.org/abs/2501.01318>
11. Huang, L., Chen, J., & Zhu, Q. (2018). Distributed and optimal resilient planning of large-scale interdependent critical infrastructures. *Proceedings of the Winter Simulation Conference*. <https://arxiv.org/abs/1809.02231>
12. Noor, A. F. M., Moghavvemi, S., & Tajudeen, F. P. (2025). Identifying key factors of cybersecurity readiness in organizations: Insights from Malaysian critical infrastructure. *Computers & Security*, 159, 104674.
13. Rehak, D., Flynnova, L., Hromada, M., & Fuggini, C. (2023). The importance of resistance in the context of critical infrastructure resilience: An extension of the CIERA method. *Systems*, 11(10), 506. <https://doi.org/10.3390/systems11100506>
14. Alizadeh, H., Sharifi, A., Kamelifar, M. J., et al. (2023). A study on the sustainability of urban transportation in Iranian metropolitan areas. *Transportation in Developing Economies*, 9, 8. <https://doi.org/10.1007/s40890-023-00178-7>
15. Sydorenko, V., & Maksymets, A. (2025). A model for ensuring the resilience of critical information systems under the influence of internal and external destabilizing factors. *Cybersecurity: Education, Science, Technology*, 3(27), 560–571. <https://doi.org/10.28925/2663-4023.2025.27.779>

