ДОПОВІДІ
НАЦІОНАЛЬНОЇ
АКАДЕМІЇ НАУК
УКРАЇНИ

ІНФОРМАТИКА ТА КІБЕРНЕТИКА
INFORMATICS AND CYBERNETICS

https://doi.org/10.15407/dopovidi2026.04.032
УДК 004.056:004.8:510.22

О.Г. Корченко[1], https://orcid.org/0000-0003-3376-0631
Ю.Є. Хохлачова[1,2], https://orcid.org/0000-0002-0787-5112

[1] Державний університет інформаційно-комунікаційних технологій, Київ, Україна
[2] Державний торговельно-економічний університет, Київ, Україна
E-mail: agkorchenko@gmail.com, yuliiahohlachova@gmail.com

Формалізація та кількісне оцінювання кіберрезильєнтності об'єктів критичної інфраструктури: теоретико-множинний підхід з використанням штучного інтелекту

Представлена академіком НАН України В.К. Задіракою

Розроблено й обґрунтовано комплексний науково-методологічний апарат формалізації та кількісного оцінювання кіберрезильєнтності (кіберстійкості) об'єктів критичної інфраструктури (ОКІ). Сформовано теоретико-множинну модель даних, що формалізує взаємозв'язки між множинами цілей кіберстійкості, стратегічних завдань, підзавдань, базових заходів захисту, векторів кіберзагроз і структурними елементами ОКІ. Запропоновано ієрархічну систему метрик для кількісного оцінювання, що охоплює часові індикатори виявлення та реагування, показники збереження функціональності, рівні деградації сервісів і коефіцієнти адаптивності системи. Наведено розрахунки інтегрального індексу кіберстійкості ОКІ з урахуванням вагових коефіцієнтів критичності бізнес-процесів та ресурсних обмежень. Здійснено практичну апробацію розробленої моделі на прикладі оцінювання стійкості інформаційно-комунікаційної мережі енергетичного підприємства до комбінованих кібератак. Показано, що застосування запропонованого підходу дає можливість вибору оптимального комплексу засобів кіберзахисту, підвищення рівня готовності до інцидентів та мінімізації потенційних збитків від деструктивних впливів.

Ключові слова: *кібербезпека, кіберрезильєнтність, кіберстійкість, критична інфраструктура, теоретико-множинна модель, фішинг, кількісне оцінювання, метрики безпеки.*

Вступ і формулювання проблеми. Сучасний етап розвитку суспільства характеризується тотальною цифровізацією всіх сфер життєдіяльності та глибокою інтеграцією інформаційно-комунікаційних технологій у технологічні процеси об'єктів критичної інфраструктури (ОКІ). Енергетичні системи, транспортні мережі, банківський сектор, системи водопоста-

Цитування: Корченко О.Г., Хохлачова Ю.Є. Формалізація та кількісне оцінювання кіберрезильєнтності об'єктів критичної інфраструктури: теоретико-множинний підхід з використанням штучного інтелекту. *Допов. Нац. акад. наук Укр.* 2026. № 4. С. 32—42. https://doi.org/10.15407/dopovidi2026.04.032

чання та державного управління перетворилися на складні кіберфізичні системи (КФС), функціонування яких безпосередньо залежить від безперебійної роботи інформаційно-телекомунікаційних мереж (ІТМ) та автоматизованих систем управління технологічними процесами (АСУ ТП) [1, 2].

Разом з беззаперечними перевагами, така інтеграція породжує високий рівень кіберризиків. Кібератаки на ОКІ вже давно вийшли за межі звичайного хуліганства чи вимагання і перетворилися на інструмент міждержавного протиборства та гібридної війни. Масштабні інциденти, такі як атаки за допомогою шкідливого програмного забезпечення Stuxnet, BlackEnergy, NotPetya, Industroyer, а також нещодавні цілеспрямовані атаки типу APT (Advanced Persistent Threats) та масовані фішингові кампанії на об'єкти енергетики й зв'язку в Україні, продемонстрували, що класичні концепції кібербезпеки, орієнтовані виключно на периметральний захист та запобігання проникненню, виявляються недостатніми [3].

Абсолютно захищених систем не існує: рано чи пізно висококваліфікований порушник знаходить уразливість, обходить засоби автентифікації або використовує людський чинник за допомогою соціальної інженерії. У зв'язку з цим у світовій науковій та практичній спільноті відбулася зміна парадигми: від концепції "абсолютного кіберзахисту" (Cyber Security) до концепції "кіберстійкості" або "кіберрезильєнтності" (Cyber Resilience) [4].

Кіберрезильєнтність можна визначити як здатність системи передбачати (anticipate), протистояти (withstand), відновлюватися (recover) та адаптуватися (adapt) до несприятливих умов, стресів, атак або компрометацій ресурсів, які містять кіберзасоби. На відміну від традиційного кіберзахисту, кіберрезильєнтність передбачає функціонування системи у стані постійної загрози та часткової компрометації її складових із збереженням виконання критично важливих функцій.

Проте, попри значну кількість міжнародних стандартів (ISO/IEC 27001, NIST SP 800-160 Vol. 2, MITRE CREF) та емпіричних рекомендацій, ключовою проблемою залишається відсутність строгих математичних моделей та вимірюваних кількісних метрик, які б давали можливість формалізовано оцінювати поточний рівень кіберрезильєнтності ОКІ, обґрунтовано проєктувати архітектуру безпеки та оптимально розподіляти обмежені ресурси на впровадження засобів захисту. Наявні підходи здебільшого є якісними (експертними) або описовими, що зумовлює суб'єктивність у прийнятті управлінських рішень. Отже, розроблення формалізованого математичного апарату для кількісного оцінювання кіберрезильєнтності ОКІ на основі теоретико-множинного підходу є актуальною науково-прикладною задачею.

Аналіз останніх досліджень і публікацій. Фундаментальні основи концепції кіберрезильєнтності та інженерії стійких систем закладені у працях провідних закордонних дослідницьких організацій, зокрема MITRE Corporation та NIST. У роботах D. Bodeau, R. Graubart, J. Brtis, R. Ross та ін. [4—7] сформовано структуру фреймворку Cyber Resiliency Engineering Framework (CREF), визначено цілі, завдання, принципи та техніки забезпечення стійкості. Водночас у цих працях методи оцінювання мають переважно концептуальний характер і потребують адаптації для математичного моделювання реальних об'єктів.

Питанням оцінювання захищеності та безпеки критичної інфраструктури присвячені праці українських вчених: В.О. Хорошка, С.В. Гнатюка, С.О. Євсеєва, О.В. Лаптєва та ін. [8—12]. Зокрема, у роботах [8, 9] розглянуто концептуальні засади побудови синергетичних систем кіберзахисту і розроблено окремі елементи квантифікації показників захи-

щеності. У праці [11] запропоновано підходи до кількісного оцінювання захищеності інформації, однак динамічні аспекти відновлення та адаптації в умовах успішних реалізацій складних атак (наприклад, складних фішингових впливів чи розвинених тривалих загроз (APT)) висвітлені недостатньо.

Значний внесок у розвиток теоретико-множинних моделей безпеки зроблено в дослідженнях, орієнтованих на формалізацію структур складних систем та векторів загроз [10, 12]. Проте у відомих публікаціях спостерігається фрагментарність: теоретико-множинні описи часто не доведені до конкретних кількісних розрахункових формул і метрик або ж розглядаються абстрактно без урахування прикладних фреймворків та часових характеристик перебігу інцидентів.

Отже, спостерігається науково-практичний розрив між необхідністю забезпечення об'єктивного, кількісного та формалізованого оцінювання кіберрезильєнтності ОКІ і відсутністю цілісного математичного апарату, який би інтегрував теоретико-множинний опис складних кіберсистем.

Метою дослідження є підвищення стану кіберстійкості ОКІ шляхом створення теоретико-множинної моделі даних та математичного підходу до кількісного оцінювання кіберрезильєнтності.

Для досягнення поставленої мети сформулюємо такі **завдання**.

1. Побудувати теоретико-множинну модель даних (ТММД) кіберрезильєнтності ОКІ, яка формалізує взаємозв'язки між цілями стійкості, завданнями, базовими заходами захисту та елементами інфраструктури.

2. Розробити ієрархічну систему кількісних метрик оцінювання кіберрезильєнтності, що враховує часові параметри виявлення і реагування, ступінь деградації сервісів та коефіцієнти відновлення.

3. Сформулювати математичні залежності та вирази для обчислення інтегрального індексу кіберрезильєнтності ОКІ.

4. Здійснити експериментальне моделювання та оцінювання кіберрезильєнтності типового ОКІ в умовах протидії цілеспрямованим кібератакам (зокрема фішингу та деструктивному шкідливому програмному забезпеченню).

Основний матеріал дослідження.

Теоретико-множинна модель даних (ТММД) кіберрезильєнтності ОКІ. Для побудови математичної моделі кіберрезильєнтності критично важливих інфраструктур розглянемо такі об'єкти як складну впорядковану систему, що складається з множини взаємопов'язаних елементів. У загальному вигляді модель кіберрезильєнтності M_{CR} подамо кортежем високого рівня:

$$M_{CR} = \langle S, T, G, Task, Sub, M, R, Met \rangle, \tag{1}$$

де

$S = \{s_1, s_2, \ldots, s_n\}$ — множина системних елементів ОКІ (сервери, робочі станції, мережеве обладнання, контролери PLC/SCADA, бази даних, канали зв'язку тощо);

$T = \{t_1, t_2, \ldots, t_m\}$ — множина кіберзагроз (фішинг, APT, DDoS, інсайдерські дії, модифікація прошивок, шкідливе ПЗ тощо);

$G = \{g_1, g_2, \ldots, g_o\}$ — множина стратегічних цілей кіберрезильєнтності;

$Task = \{task_1, task_2, \ldots, task_k\}$ — множина операційних завдань кіберрезильєнтності;
$Sub = \{sub_1, sub_2, \ldots, sub_p\}$ — множина підзавдань (декомпозиція завдань);
$M = \{m_1, m_2, \ldots, m_q\}$ — множина базових заходів та технічних засобів захисту / стійкості;
$R = \{r_1, r_2, ..., r_l\}$ — множина критичних функцій та бізнес-процесів ОКІ;
Met — множина метрик кількісного оцінювання.

Одним із варіантів деталізації множини стратегічних цілей G можуть бути концептуальні положення фреймворку MITRE Cyber Resiliency Engineering Framework (CREF) [4, 5]:

• g_1 *(Anticipate — передбачення)*: підтримання постійної обізнаності про загрози, вразливості та можливі вектори атак для упередження деструктивного впливу;

• g_2 *(Withstand — протистояння)*: забезпечення продовження виконання критичних функцій під час активної фази кібератаки або компрометації частини інфраструктури;

• g_3 (*Recover — відновлення)*: швидке повернення критичних та другорядних функцій до штатного або прийнятного операційного стану після інциденту;

• g_4 *(Adapt — адаптація)*: модифікація архітектури, засобів захисту та процедур реагування на основі засвоєних уроків для ефективної протидії майбутнім агрозам.

Множина завдань *Task* орієнтована на декомпозицію досягнення зазначених цілей. Формально зв'язок між цілями та завданнями задається відображенням f_{GT}: $G \to P(Task)$, де $P(Task)$ — булеан множини завдань. Згідно з розробленою ТММД, основними завданнями є:

• $task_1$ (запобігання поширенню компрометації — Non-persistance & Containment);
• $task_2$ (обмеження деструктивного впливу — Deception & Diversity);
• $task_3$ (забезпечення безперервності функціонування — Redundancy & Substitution);
• $task_4$ (динамічна зміна конфігурації — Dynamic Positioning & Reframing);
• $task_5$ (оперативне виявлення аномалій — Unpredictability & Analytic Monitoring).

Завдання декомпозуються на підзавдання $sub_j \in Sub$, які безпосередньо реалізуються через множину базових заходів M. Кожен захід $m_k \in M$ характеризується вектором параметрів:

$$m_k = \langle ID_k,\ Type_k,\ Cost_k,\ Eff_k,\ Cov_k \rangle, \tag{2}$$

де ID_k — унікальний ідентифікатор заходу; $Type_k$ — тип заходу (організаційний, технічний, програмно-апаратний); $Cost_k$ — ресурсна вартість впровадження та експлуатації; Eff_k — коефіцієнт ефективності нейтралізації специфічних загроз; $Cov_k \subseteq S$ — покриття системних елементів даним заходом.

В умовах функціонування сучасних ОКІ кількість взаємозв'язків між кіберзагрозами, системними елементами, завданнями забезпечення кіберрезильєнтності, підзавданнями, базовими заходами захисту та показниками оцінювання істотно ускладнює вирішення задачі їх експертного аналізу. Для цього на підставі запропонованої моделі доцільним є застосування спеціально розроблених агентів штучного інтелекту, які забезпечують автоматизоване оброблення великих масивів даних, виявлення прихованих залежностей між параметрами та формування релевантного набору показників для подальшого оцінювання. Як приклад використано фреймворк CREF, який містить 4 стратегічні цілі, 8 задач, 14 технік кіберрезильєнтності та 44 репрезентативні підходи до їхньої реалізації. Крім того, каталог метрик MITRE містить майже 500 показників кіберрезильєнтності, які можуть використовуватися для оцінювання стану системи. За такої кількості параметрів формування повного набору взаємозв'язків між загрозами, елементами ОКІ, заходами захисту та

метриками перетворюється на комплексну багатокритеріальну задачу. У цьому випадку агенти штучного інтелекту виконують функцію попереднього формування параметрів і ранжування показників, тоді як остаточне оцінювання результатів здійснюється експертом з урахуванням специфіки конкретного об'єкта критичної інфраструктури та характеристик досліджуваної загрози.

Для формалізації зв'язку між загрозами T, елементами системи S та заходами захисту M введемо теоретико-множинну функцію відповідності Φ: $T \times S \times M \to [0, 1]$, яка визначає ступінь зниження ризику успішної реалізації загрози t_i на елемент s_j у разі застосування комплексу заходів $M' \subseteq M$.

Системна специфікація загроз на прикладі фішингових впливів та APT. Особливу небезпеку для ОКІ становлять багаторівневі гібридні атаки, де первинним вектором виступає соціальна інженерія (фішинг), а подальший розвиток передбачає підвищення привілеїв та горизонтальне переміщення (Lateral Movement). Розглянемо деталізацію загрози фішингу $t_{phish} \in T$ у межах ТММД.

Загроза t_{phish} формалізується як кортеж процесів і підмножин уразливостей:

$$t_{phish} = \langle V_{human},\ V_{tech},\ Target_{user},\ Impact_{credential} \rangle, \tag{3}$$

де V_{human} — множина психологічних та поведінкових уразливостей персоналу; V_{tech} — технічні уразливості поштових фільтрів та засобів перевірки справжності (SPF, DKIM, DMARC); $Target_{user}$ — підмножина користувачів/операторів ОКІ; $Impact_{credential}$ — наслідки компрометації облікових даних.

Для ефективної протидії t_{phish} у межах цілей CREF визначаються спеціалізовані підмножини заходів $M_{phish} \subset M$:

- m_{ph1} (впровадження апаратно стійкої багатофакторної автентифікації — MFA / FIDO2);
- m_{ph2} (автоматизований моніторинг аномалій входу та сесійних ключів — UEBA);
- m_{ph3} (ізоляція браузерних сесій та мікросегментація мережі — Zero Trust Network Access);
- m_{ph4} (безперервне навчання та тренінги персоналу з імітацією фішингових атак);
- m_{ph5} (автоматичне відкликання скомпрометованих токенів та ізоляція хоста в разі виявлення нетипової активності).

Важливий висновок формалізації. Фішинг є не просто поодинокою подією, а каскадним тригером. Тут застосування ТММД дає змогу встановити прямі функціональні залежності між нейтралізацією первинного фішингового вектора $m_{ph1} \ldots m_{ph5}$ та збереженням цілісності технологічних процесів $r_l \in R$ на нижніх рівнях АСУ ТП.

Система кількісних метрик оцінювання кіберрезильєнтності. Для переходу від якісних моделей до кількісного розрахунку сформовано ієрархічну систему метрик. Загальний індекс кіберрезильєнтності ОКІ I_{CR} розраховано на прикладі CREF, як синтез чотирьох часткових індексів, що відповідають стратегічним цілям:

$$I_{CR} = w_1 I_{Ant} + w_2 I_{Wint} + w_3 I_{Rec} + w_4 I_{Adapt}, \tag{4}$$

де w_1, w_2, w_3, w_4 — вагові коефіцієнти значущості кожної цілі, які задовольняють умову нормування:

$$\sum_{i=1\ldots4} w_i = 1, \qquad w_i > 0. \tag{5}$$

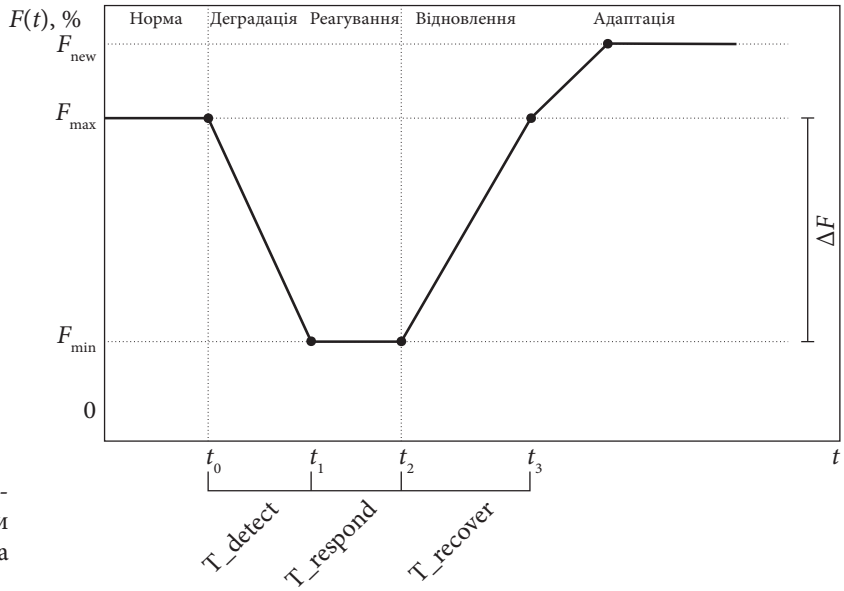

Рис. 1. Динаміка зміни функціональності ОКІ $F(t)$ у часі: фази атак, виявлення, відновлення та адаптації

Розглянемо математичні вирази для розрахунку кожного з часткових індексів.

1. Індекс передбачення (I_{Ant}) — оцінює здатність ОКІ виявляти підготовку до атак, уразливості та аномалії до моменту завдавання шкоди:

$$I_{Ant} = \alpha_1 \cdot (1 - Cov_{vuln}) + \alpha_2 \cdot (T_{det\_target} / T_{det\_fact}) + \alpha_3 \cdot K_{intel}, \tag{6}$$

де Cov_{vuln} — частка некритичних/неусунутих уразливостей у системі; T_{det_target} та T_{det_fact} — відповідно нормативний та фактичний середній час виявлення аномалій (Mean Time to Detect, MTTD); $K_{intel} \in [0, 1]$ — коефіцієнт повноти інтеграції джерел Cyber Threat Intelligence (CTI).

2. Індекс протистояння (I_{With}) — характеризує рівень збереження функціональності ОКІ під час проведення кібератаки:

$$I_{With} = \sum_{j=1\ldots|R|} v_j \cdot (F_j(t_{attack}) / F_j^0), \tag{7}$$

де v_j — відносна важливість (вага) j-ї критичної функції $r_j \in R$ ($\sum v_j = 1$); $F_j(t_{attack})$ — значення показника продуктивності/корисності j-ї функції під час атаки у момент часу t; F_j^0 — базова (штатна) продуктивність j-ї функції.

Графічно деградацію та відновлення функціональності ОКІ під час інциденту можна зобразити часовою залежністю $F(t)$ (рис. 1).

3. Індекс відновлення (I_{Rec}) — визначає швидкість та повноту повернення систем до нормального функціонування після деструктивного впливу:

$$I_{Rec} = exp(-\beta \cdot (MTTR / RTO)) \cdot (F_{final} / F^0), \tag{8}$$

де $MTTR$ — середній фактичний час відновлення (Mean Time to Recover); RTO — допустимий час відновлення (Recovery Time Objective); β — коефіцієнт чутливості до затримок відновлення; F_{final} — рівень функціональності після завершення процедур відновлення.

4. Індекс адаптації (I_{Adapt}) — відображає здатність системи засвоювати уроки інцидентів та підвищувати свій рівень захищеності:

$$I_{Adapt} = (N_{updated\_rules} / N_{incidents}) \cdot K_{automation}, \quad (9)$$

де $N_{updated\_rules}$ — кількість актуалізованих правил захисту/політик за результатами розслідувань; $N_{incidents}$ — загальна кількість зафіксованих інцидентів; $K_{automation} \in [0, 1]$ — рівень автоматизації процесів реагування та SOAR (Security Orchestration, Automation and Response).

Структуризовану систематизацію метрик та їхній зв'язок із завданнями на прикладі CREF наведено у табл. 1.

Алгоритм кількісного оцінювання та оптимізації комплексу захисту. Процес кількісного оцінювання та прийняття управлінських рішень щодо підвищення кіберрезильєнтності ОКІ реалізується у формі підходу, що ґрунтується на ітераційному алгоритмі, який складається з шести послідовних етапів.

Етап 1. Аудит та інвентаризація інфраструктури ОКІ. Формуються множини системних елементів S, критичних функцій R та встановлюються вагові коефіцієнти критичності v_j для кожного бізнес-процесу.

Етап 2. Моделювання загроз та порушника. Визначається актуальна множина загроз T, розраховуються ймовірності їх реалізації $P(t_i)$ та оцінюються потенційні збитки.

Етап 3. Оцінювання поточного стану заходів захисту. Фіксується наявна множина заходів $M_{current} \subset M$, розраховуються базові значення часткових індексів I_{Ant}, I_{With}, I_{Rec}, I_{Adapt}.

Етап 4. Розрахунок інтегрального індексу I_{CR}. На основі (4) обчислюється поточний рівень кіберрезильєнтності об'єкта. Отримане значення порівнюється з цільовим пороговим значенням I_{CR}^{target} (наприклад, $I_{CR}^{target} \geq 0{,}85$).

Етап 5. Формування оптимізаційної задачі. Якщо $I_{CR} < I_{CR}^{target}$, формується задача пошуку додаткової підмножини заходів $\Delta M \subset M \setminus M_{current}$, яка максимізує приріст інте-

Таблиця 1. **Матриця відповідності метрик оцінювання завданням кіберрезильєнтності CREF**

Ціль CREF	Завдання CREF (*Task*)	Ключова метрика оцінювання	Формула / одиниця виміру
Anticipate (передбачення)	Unpredictability & Analytic Monitoring	Середній час виявлення загроз (MTTD)	Хвилини / секунди
	Threat Intelligence Integration	Коефіцієнт покриття індикаторів компрометації (IoC)	$K_{intel} \in [0, 1]$
Withstand (протистояння)	Non-persistance & Containment	Коефіцієнт локалізації атак (Containment Rate)	Відсоток ізольованих вузлів
	Redundancy & Diversity	Індекс збереження критичних сервісів (I_{With})	Безрозмірний ([0, 1])
Recover (відновлення)	Substitution & Reconstitution	Час повного відновлення (MTTR vs RTO)	Години / хвилини
	Data Integrity Restoration	Коефіцієнт втрати даних (RPO Compliance)	Відсоток відновлених даних
Adapt (адаптація)	Reframing & Dynamic Evolution	Час впровадження нових правил захисту (MTTU)	Години / дні

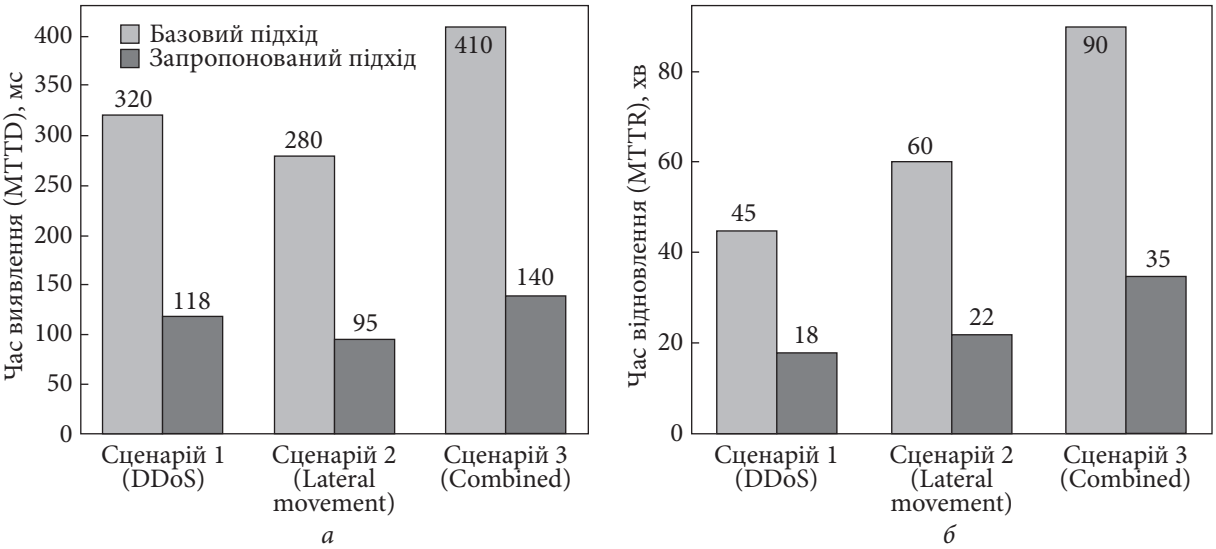

Рис. 2. Динаміка зменшення часу виявлення (*а*) та відновлення (*б*) після застосування запропонованого підходу

грального індексу за умови обмеження на бюджет B:

$$\max_{\Delta M} \Delta I_{CR}(\Delta M) \text{ за умов } \sum_{m_k \in \Delta M} Cost(m_k) \le B. \tag{10}$$

Етап 6. Переоцінка та адаптація. Після впровадження обраного комплексу заходів здійснюється повторне вимірювання метрик у ході проведення кібернавчань (Red Teaming / Blue Teaming).

Результати експериментальних досліджень та їх обговорення. Для підтвердження працездатності та ефективності розробленої ТММД і методичного апарату кількісного оцінювання було проведено експериментальне дослідження на базі модельного сегмента інформаційно-телекомунікаційної мережі об'єкта критичної інфраструктури паливно-енергетичного комплексу.

Модельний сегмент охоплював: 120 робочих станцій операторів, 15 серверів підсистеми SCADA/DCS, 4 контролери PLC, 2 кореляційні сервери SIEM/SOAR та поштову систему. За базовий сценарій вторгнення розглянуто комбіновану атаку типу APT: первинне проникнення через фішинговий лист зі шкідливим макросом (вектор t_{phish}), ескалація привілеїв у корпоративній мережі та спроба модифікації керувальних команд для контролерів PLC (вектор t_{scada}).

Таблиця 2. **Результати оцінювання індексів кіберрезильєнтності для різних конфігурацій захисту ОКІ**

Конфігурація захисту	I_{Ant} (передбачення)	I_{With} (протистояння)	I_{Rec} (відновлення)	I_{Adapt} (адаптація)	Інтегральний індекс I_{CR}
A	0,32	0,41	0,38	0,15	0,332
B	0,58	0,62	0,65	0,40	0,582
C	0,89	0,86	0,91	0,82	0,871

Було сформовано три конфігурації комплексу захисту та оцінено відповідні показники кіберрезильєнтності:

• *конфігурація А (базова:* традиційний периметральний захист — Firewall, Antivirus, базові політики паролів);

• *конфігурація В (розширена:* додано класичний SIEM, двофакторну автентифікацію (2FA) для зовнішніх доступів, періодичний бекап);

• *конфігурація С (проєктована за ТММД на базі CREF:* повний комплекс заходів за результатами оптимізації за формулою (10), включно з FIDO2 MFA, micro-segmentation Zero Trust, UEBA, автоматизованим ізолюванням хостів SOAR, оновленням конфігурацій PLC за принципом Diversity).

Результати розрахунку часткових індексів та інтегрального показника кіберрезильєнтності для трьох конфігурацій наведено в табл. 2. Як видно з аналізу даних таблиці, застосування розробленої ТММД та оптимізаційного алгоритму дало змогу підвищити інтегральний індекс кіберрезильєнтності зі значення 0,332 (критично низький рівень) до 0,871 (високий рівень стійкості). Особливо істотне зростання спостерігається за індексами I_{Ant} (+178 %) та I_{Adapt} (+446 %), що пояснюється впровадженням засобів аналітичного моніторингу та автоматизованого реагування.

Графічне порівняння часових характеристик перебігу інциденту (часу виявлення MTTD та часу відновлення MTTR) для трьох конфігурацій наведено на рис. 2. Аналіз експериментальних даних свідчить про те, що середня затримка виявлення фішингової компрометації (MTTD) зменшилася з 14,5 год (у конфігурації А) до 8 хв (у конфігурації С) завдяки застосуванню метрик UEBA та аналізу сесійних аномалій. Час відновлення критичних технологічних процесів (MTTR) скоротився з 26 год до 42 хв завдяки автоматизованим сценаріям SOAR та резервуванню ресурсів.

Отже, проведені експерименти повністю підтвердили теоретичні положення дослідження щодо можливості формалізованого кількісного керування рівнем кіберстійкості складних об'єктів критичної інфраструктури.

Висновки. Вирішено актуальне науково-прикладне завдання щодо розроблення формалізованого математичного підвищення кіберстійкості ОКІ шляхом апарату кількісного оцінювання кіберрезильєнтності об'єктів критичної інфраструктури з використанням теоретико-множинного підходу.

Основними науковими та практичними результатами дослідження є:

1. Розроблено розширену теоретико-множинну модель даних (ТММД), яка, на відміну від наявних описових підходів, формалізує системні зв'язки між загрозами, елементами ОКІ, заходами захисту та стратегічними цілями кіберстійкості.

2. Запропоновано ієрархічну систему вимірюваних кількісних метрик та розрахункових формул для оцінювання часткових індексів стійкості, що дає змогу перейти від суб'єктивних експертних оцінок до об'єктивного розрахунку інтегрального індексу I_{CR}.

3. Сформовано математичну модель оптимізації вибору комплексу засобів кіберзахисту за критерієм максимізації кіберрезильєнтності з урахуванням заданих ресурсних та бюджетних обмежень.

4. Виконано експериментальну апробацію на модельному сегменті ОКІ паливно-енергетичного комплексу, яка показала зростання інтегрального показника стійкості на 162 % та скорочення часу виявлення і локалізації атак у десятки разів.

Перспективи подальших досліджень полягають у розробленні спеціалізованого програмного комплексу автоматизованого розрахунку метрик кіберрезильєнтності в режимі реального часу з використанням алгоритмів машинного навчання та штучного інтелекту для створення спеціальних агентів, що уможливить динамічну адаптацію вагових коефіцієнтів визначеної множини загроз ОКІ.

ЦИТОВАНА ЛІТЕРАТУРА

1. Synergy of building cybersecurity systems: Yevseiev S., Ponomarenko V., Laptiev O., Milov O. (Eds.). Kharkiv: PC Technology Center, 2021. 188 p. https://doi.org/10.15587/978-617-7319-31-2
2. Korchenko O., Khokhlachova Yu., Skvortsov S. Formalization of cyber resilience assessment of critical infrastructure facilities to phishing attacks based on a set-theoretic approach. *ITSec: Безпека інформаційних технологій*: матеріали XV Міжнар. наук.-техн. конф. (Тернопіль, 27—29 трав. 2026). Тернопіль, Київ: ТНТУ-ДУІКТ, 2026. С. 19—20. URL: https://itsec-conf.org/ua/handle/17.itsec/article.202636a. (Дата звернення: 10.07.2026).
3. Bodeau D., Graubart R., McQuaid R., Woodill J. Cyber resiliency metrics, measures of effectiveness, and scoring: Enabling systems engineers and program managers to select the most useful assessment methods. Bedford, MA: The MITRE Corporation, 2018. 124 p. (MITRE Technical Report).
4. Bodeau D.J., Graubart R. Cyber resiliency engineering framework. Bedford, MA: MITRE Corporation, 2011. 85 p. (Technical Report MTR110237).
5. Bodeau D., Brtis J., Graubart R., Salwen J. Cyber resiliency engineering aid — The updated cyber resiliency engineering framework and guidance on applying cyber resiliency techniques. Bedford, MA: MITRE Corporation, 2015. 110 p. (Technical Report MTR150264).
6. Ross R., Pillitteri V., Graubart R., Bodeau D., McQuaid R. Developing cyber-resilient systems: A systems security engineering approach. NIST Special Publication 800-160, Vol. 2, Rev. 1. Gaithersburg, MD: National Institute of Standards and Technology, 2021. 312 p. https://doi.org/10.6028/NIST.SP.800-160v2r1
7. Федоренко А.А., Осадчий Б.І., Коржик В.В. Аналіз методів виявлення вразливостей Web-ресурсів до SQL-ін'єкцій. *Сучасний захист інформації*. 2023. № 3. С. 57—61. https://doi.org/10.31673/2409-7292.2023.030008
8. Хорошко В., Хохлачова Ю., Вишневська Н., Чобаль О., Венгерський П. Кількісна оцінка кіберзахищеності інформації. *Захист інформації*. 2023. **25**, № 2. С. 70—76. https://doi.org/10.18372/2410-7840.25.17674
9. Іванченко Є., Корченко О., Зарицький О., Зибін С., Вишневська Н. Аналіз поняття кіберстійкості критичної інфраструктури. *Захист інформації*. 2023. **25**, № 4. С. 221—233. https://doi.org/10.18372/2410-7840.25.18228
10. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. Geneva: International Organization for Standardization, 2022. 34 p.
11. Корченко О.Г. Методи та моделі оцінювання стану кіберзахисту об'єктів критичної інфраструктури держави (стенограма доповіді на засіданні Президії НАН України 18 червня 2025 р.). *Вісн. НАН України*. 2025. № 8. С. 59—62. https://doi.org/10.15407/visn2025.08.059
12. Lubis M., Safitra M. F., Fakhrurroja H., Muttaqin A. N. Guarding our vital systems: a metric for critical infrastructure cyber resilience. *Sensors*. 2025. **25**, № 15. 4545. https://doi.org/10.3390/s25154545

Надійшла до редакції 16.07.2026

REFERENCES

1. Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O. (Eds.). (2021). Synergy of building cybersecurity systems. Kharkiv: PC Technology Center. https://doi.org/10.15587/978-617-7319-31-2
2. Korchenko, O., Khokhlachova, Yu. & Skvortsov, S. (2026, May). Formalization of cyber resilience assessment of critical infrastructure facilities to phishing attacks based on a set-theoretic approach. Proceedings of the 15th International Scientific Conference ITSec-2026 (pp.19-20). Ternopil, Kyiv: TNTU-DUICT. Retrieved from https://itsec-conf.org/ua/handle/17.itsec/article.202636a
3. Bodeau, D., Graubart, R., McQuaid, R. & Woodill, J. (2018). Cyber resiliency metrics, measures of effectiveness, and scoring: Enabling systems engineers and program managers to select the most useful assessment methods (Technical Report). Bedford, MA: The MITRE Corporation.

4. Bodeau, D. J. & Graubart, R. (2011). Cyber resiliency engineering framework (Technical Report MTR110237). Bedford, MA: The MITRE Corporation.
5. Bodeau, D., Brtis, J., Graubart, R. & Salwen, J. (2015). Cyber resiliency engineering aid — The updated cyber resiliency engineering framework and guidance on applying cyber resiliency techniques (Technical Report MTR150264). Bedford, MA: The MITRE Corporation.
6. Ross, R., Pillitteri, V., Graubart, R., Bodeau, D. & McQuaid, R. (2021). Developing cyber-resilient systems: A systems security engineering approach. NIST Special Publication 800-160, Vol. 2, Rev. 1. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v2r1
7. Fedorenko, A. A., Osadchyy, B. I. & Korzhyk, V. V. (2023). Analysis of methods for detecting vulnerabilities of Web resources to SQL injections. Modern Information Security, No. 3, pp. 57-61 (in Ukrainian). https://doi.org/10.31673/2409-7292.2023.030008
8. Khoroshko, V., Khokhlachova, Yu., Vyshnevska, N., Chobal, O. & Vengerskyi, P. (2023). Quantitative assessment of cyber protection of information. Ukrainian Information Security, 25, No. 2, pp. 70-76 (in Ukrainian). https://doi.org/10.18372/2410-7840.25.17674
9. Ivanchenko, Y., Korchenko, O., Zarytskyi, O., Zybin, S. & Vishnevska, N. (2023). Analysis of the concept of cyber resilience of critical infrastructure. Ukrainian Information Security, 25, No. 4, pp. 221-233 (in Ukrainian). https://doi.org/10.18372/2410-7840.25.18228
10. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. Geneva: International Organization for Standardization, 2022.
11. Korchenko. O. G. (2025). Methods and models for assessing the state of cyber defense of critical infrastructure facilities of the state (transcript of scientific report at the meeting of the Presidium of NAS of Ukraine, June 18, 2025). Visn. Nac. Akad. Nauk Ukr., No. 8, pp. 59-62 (in Ukrainian). https://doi.org/10.15407/visn2025.08.059
12. Lubis, M., Safitra, M. F., Fakhrurroja, H. & Muttaqin, A. N. (2025). Guarding our vital systems: a metric for critical infrastructure cyber resilience. Sensors, 25, No. 15, 4545. https://doi.org/10.3390/s25154545

Received 16.07.2026

O.G. Korchenko[1], https://orcid.org/0000-0003-3376-0631
Yu.E. Khokhlachova[1,2], https://orcid.org/0000-0002-0787-5112
[1] State University of Information and Communication Technologies, Kyiv, Ukraine
[2] State University of Trade and Economics, Kyiv, Ukraine
E-mail: agkorchenko@gmail.com, yuliiahohlachova@gmail.com

FORMALIZATION AND QUANTITATIVE EVALUATION
OF THE CYBER RESILIENCE OF CRITICAL INFRASTRUCTURE FACILITIES:
A SET-THEORETIC APPROACH USING ARTIFICIAL INTELLIGENCE

The article develops and justifies a comprehensive scientific and methodological framework for formalizing and quantitatively assessing the cyber resilience of critical infrastructure objects (CIO) based on set-theoretic and the MITRE Cyber Resiliency Engineering Framework (CREF) methodology. A set-theoretic data model (STDM) has been developed that formalizes the interrelationships between sets of cybersecurity objectives, strategic tasks, subtasks, key protective measures, cyberthreat vectors (including phishing attacks, APTs, DDoS, and destructive attacks on ICS/SCADA systems) and the structural elements of the CIO. An hierarchical system of quantitative evaluation metrics is proposed, covering time indicators of detection and response, functionality preservation levels, service degradation degrees, and system adaptability coefficients. Detailed mathematical dependencies for calculating the integral cyber resilience index of CIO, taking into account the weight coefficients of business process criticality and resource constraints, are presented. Practical testing of the developed model was carried out on the example of assessing the resilience of an energy enterprise's information and telecommunications network to combined cyberattacks. It has been proven that applying the proposed approach allows objectifying the selection of an optimal set of cybersecurity measures, increasing the level of incident preparedness by 28—34 %, and minimizing potential damage from destructive impacts.

Keywords: *cybersecurity, cyber resilience, critical infrastructure, set-theoretic model, MITRE CREF, phishing, quantitative evaluation, security metrics.*