DOI: 10.58254/viti.9.2026.05.66

УДК 004.94:004.056:519.87

канд. техн. наук, доцент Гріньков В. О. ORCID: 0000-0002-9574-3792 (ВІТІ ім. Героїв Крут)
Грінькова Г. В. ORCID: 0009-0003-4896-364X (НДІ ВР)
Слюсар П. П. ORCID: 0009-0007-3738-2523 (НДІ ВР)

МАТЕМАТИЧНА МОДЕЛЬ ОЦІНЮВАННЯ КІБЕРСТІЙКОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ ЗАЛЕЖНО ВІД ТОПОЛОГІЇ ПОБУДОВИ НА ОСНОВІ МЕТОДУ АНАЛІЗУ ІЄРАРХІЙ

У сучасних умовах ведення військових дій та зростання кіберзагроз забезпечення кіберстійкості інформаційних систем військового призначення набуває критичного значення. Одним із ключових факторів, що впливають на рівень кіберстійкості, є топологія побудови мережі, яка визначає її здатність протистояти відмовам, атакам і деградації функціонування.

Існуючі підходи до оцінювання кіберстійкості інформаційних систем, як правило, не враховують комплексного впливу структурних характеристик мережі або не забезпечують формалізованого багатокритеріального аналізу. Відсутність універсальної математичної моделі, яка дозволяє інтегрувати різнорідні топологічні показники та враховувати їхню відносну важливість, ускладнює обґрунтований вибір оптимальної структури мережі.

Метою статті є розроблення математичної моделі оцінювання кіберстійкості інформаційних систем залежно від топології їхньої побудови на основі методу аналізу ієрархій Analytic Hierarchy Process, що дозволяє визначати пріоритетність альтернативних топологічних рішень.

У роботі використано метод аналізу ієрархій для визначення вагових коефіцієнтів критеріїв кіберстійкості, зокрема робастності, алгебраїчної зв’язності, вершинної зв’язності, централізації та середньої довжини шляхів. Як альтернативи розглядаються типові мережеві топології (кільцева, подвійне кільце, дерево, часткова mesh-структура). Проведено формування матриць парних порівнянь критеріїв, альтернатив по кожному критерію, перевірку узгодженості суджень і розрахунок векторів пріоритетів.

Запропоновано математичну модель, яка дозволяє здійснювати інтегральну оцінку кіберстійкості інформаційних систем на основі агрегування зважених критеріїв. Отримано ранжування мережевих топологій за рівнем кіберстійкості та визначено найбільш ефективні структурні рішення для умов підвищених кіберзагроз. Показано, що використання методу аналізу ієрархій забезпечує обґрунтованість прийняття рішень за умов багатокритеріальності та невизначеності.

Розроблена модель дозволяє формалізувати процес оцінювання кіберстійкості інформаційних систем і враховувати вплив топологічних характеристик мережі. Отримані результати можуть бути використані при проєктуванні та модернізації інформаційно-телекомунікаційних систем військового призначення. Подальші дослідження доцільно спрямувати на розширення моделі за рахунок використання нечітких, нейтрософських підходів та методу аналітичного мережевого процесу Analytic Hierarchy Process для підвищення точності і адекватності моделі.

Ключові слова: *кіберстійкість, інформаційні системи, топологія мережі, метод аналізу ієрархій, AHP, FAHP, багатокритеріальний аналіз, структурна зв’язність, робастність, оцінювання ефективності.*

V. Hrinkov, H. Hrinkova, P. Sliusar. Mathematical model for assessing cyber resilience of information systems depending on the topology of the structure based on the hierarchy analysis method

In today's conditions of military operations and the growth of cyber threats, ensuring the cyber resilience of military information systems is becoming critical. One of the key factors affecting the level of cyber resilience is the topology of the network, which determines its ability to withstand failures, attacks, and degradation of functioning.

Existing approaches to assessing the cyber resilience of information systems, as a rule, do not take into account the complex impact of network structural characteristics or do not provide for formalized multi-criteria analysis. The lack of a universal mathematical model that allows integrating heterogeneous topological indicators and taking into account their relative importance complicates the informed choice of the optimal network structure.

The purpose of the article is to develop a mathematical model for assessing the cyber resilience of information systems depending on the topology of their construction based on the method of hierarchy analysis, which allows determining the priority of alternative topological solutions.

The paper uses the analysis of hierarchies method to determine the weighting coefficients of cyber resilience criteria, in particular robustness, algebraic connectivity, vertex connectivity, centralization, and average path length. Typical network topologies (ring, double ring, tree, partial mesh-structure) are considered as alternatives. Matrices of pairwise comparisons of criteria, alternatives for each criterion, verification of the consistency of judgments and calculation of priority vectors are formed.

A mathematical model is proposed that allows for an integrated assessment of cyber resilience of information systems based on the aggregation of weighted criteria. A ranking of network topologies by the level of cyber resilience is obtained and the most effective structural solutions for conditions of increased cyber threats are determined. It is shown that the use of the method of hierarchy analysis ensures the validity of decision-making under conditions of multi-criteria and uncertainty.

The developed model allows to formalize the process of assessing the cyber resilience of information systems and take into account the influence of topological characteristics of the network. The results obtained can be used in the design and modernization of military information and telecommunication systems. Further research should be directed at expanding the model by using fuzzy, neutrosophic approaches and the analytical network process method to increase the accuracy and adequacy of the model.

Keywords: *cyber resilience, information systems, network topology, analytic hierarchy process, AHP, FAHP, multi-criteria analysis, structural connectivity, robustness, efficiency assessment.*

Актуальність та постановка завдання в загальному вигляді. У сучасних умовах цифровізації сектору безпеки та оборони, а також зростання інтенсивності кіберзагроз, забезпечення кіберстійкості інформаційних систем (ІС) військового призначення стає одним із ключових чинників ефективного управління військами та функціонування систем зв’язку. Особливу роль у цьому контексті відіграє структура мережі, зокрема її топологія, яка визначає здатність системи зберігати працездатність у разі відмов окремих елементів, кібератак або порушення каналів зв’язку.

Аналіз сучасних наукових підходів показує, що оцінювання кіберстійкості часто здійснюється або на основі окремих показників (надійності, зв’язності, живучості), або з використанням складних моделей, які не враховують системну взаємодію структурних характеристик мережі. При цьому недостатньо досліджено вплив топології побудови ІС на її кіберстійкість у рамках формалізованого багатокритеріального підходу.

У зв’язку з цим актуальним є розроблення математичних моделей, що дозволяють інтегрувати різнорідні критерії оцінювання, враховувати їхню відносну важливість та забезпечувати обґрунтований вибір оптимальної топології мережі в умовах невизначеності та обмеженості ресурсів.

Аналіз попередніх досліджень. Поняття кіберстійкості в сучасних дослідженнях трактується не лише як здатність системи протистояти кібератакам, а також як спроможність передбачати, витримувати, відновлюватися та адаптуватися до несприятливих умов, атак чи компрометації. Саме таке трактування закріплене у підходах Національного інституту технологій і стандартів США *National Institute of Standards and Technolog* (NIST) [1], де кіберстійкість розглядається як властивість системи, критична для досягнення функціональних цілей у конфліктному кіберсередовищі.

Теоретичною основою багатокритеріального вибору в задачах оцінювання складних систем є метод аналізу ієрархій Т. Сааті [2]. У праці сформовано базові положення: ієрархічне структурування задачі, побудова матриць парних порівнянь, визначення локальних пріоритетів та перевірка узгодженості експертних суджень. Це робить метод придатним для задач, у яких необхідно інтегрувати кілька різнорідних критеріїв в один інтегральний показник.

Окремий напрям досліджень стосується використання спектральних характеристик графа для оцінювання стійкості мережевих структур. У роботі [3] показано, що алгебраїчна зв’язність — друге найменше власне значення матриці Лапласа – має важливе значення для аналізу робастності мережі, оскільки характеризує складність роз’єднання графа на незалежні компоненти. Автори також показують, що зі зростанням алгебраїчної зв’язності зростає і стійкість мережі до вузлових і канальних відмов.

У роботі [4] досліджується зв’язок між алгебраїчною зв’язністю та класичними показниками робастності графа – вершинною і реберною зв’язністю. У ній обґрунтовується, що спектральні характеристики можуть бути корисними індикаторами здатності мережі зберігати цілісність при відмовах вузлів і ліній зв’язку. Це особливо важливо для задач оцінювання кіберстійкості топологій ІС.

У роботі [5] виконано порівняння поширених метрик робастності для прогнозування стійкості мереж до атак. Автори доводять, що жодна окрема метрика не є універсально найкращою для всіх типів графів, натомість ефективність метрики залежить від структури мережі та сценарію впливу. Цей висновок є важливим для нашого дослідження, оскільки підтверджує доцільність не однокритеріального, а багатокритеріального оцінювання кіберстійкості.

Аналогічний висновок наведено у праці [6], де здійснено порівняльний аналіз різних показників мережевої робастності. Дослідження підтверджує, що окремі метрики відображають різні аспекти стійкості мережі, а тому для комплексного оцінювання доцільно поєднувати кілька показників у межах єдиної моделі.

У статті [7] показано, що топологічні атрибути суттєво впливають на стійкість мереж, однак самих топологічних індикаторів недостатньо для обґрунтованого проєктування системи, оскільки між різними аспектами стійкості можуть існувати компроміси. Це прямо підтримує ідею побудови інтегральної моделі на основі кількох критеріїв.

Щодо застосування *Analytic Hierarchy Process* (AHP) саме у сфері кібербезпеки, варто зазначити працю [8], де метод аналізу ієрархій використано для оцінювання стану мережевої безпеки для промислового інтернету речей. Автори демонструють, що AHP є придатним інструментом для визначення ваг окремих факторів безпеки та формування інтегральної оцінки. Водночас, такі роботи переважно орієнтовані на ситуаційне оцінювання безпеки, а не на аналіз впливу топології мережі на кіберстійкість.

Отже, аналіз літератури показує, що: по-перше, кіберстійкість доцільно трактувати як комплексну властивість системи, що охоплює протидію, відновлення та адаптацію; по-друге, графові та спектральні метрики дійсно є інформативними для аналізу стійкості топології; по-третє, жоден окремий показник не забезпечує повного опису кіберстійкості; по-четверте, AHP є придатним інструментом для агрегування різнорідних критеріїв.

Водночас у виявлених джерелах недостатньо опрацьованим залишається питання інтегрального оцінювання кіберстійкості ІС саме залежно від топології їхньої побудови на основі поєднання характеристик графів. Саме ця прогалина і зумовлює доцільність подальшого дослідження.

Метою статті є розробка математичної моделі оцінювання кіберстійкості ІС залежно від топології їхньої побудови на основі методу аналізу ієрархій, яка забезпечує інтеграцію структурних і топологічних характеристик мережі, визначення їхньої вагомості та обґрунтоване ранжування альтернатив з урахуванням принципів кіберстійкості, сформульованих у рекомендаціях NIST.

Виклад основного матеріалу. Під кіберстійкістю ІС розумітимемо здатність системи зберігати працездатність, структурну цілісність і функціональність в умовах деструктивних впливів, зокрема кібератак, відмов елементів та порушень зв'язності.

Кіберстійкість ІС значною мірою визначається її топологією побудови, оскільки саме структура зв'язків між вузлами впливає на здатність мережі до відновлення після пошкоджень, наявність альтернативних маршрутів передачі даних, ступінь централізації та вразливість до атак на критичні вузли, ефективність функціонування в умовах деградації.

Таким чином, задача оцінювання кіберстійкості може бути зведена до аналізу та порівняння різних варіантів топологічної структури ІС.

Нехай задано множину альтернативних топології ІС:

$$T = \{T_1,\ T_2,\ ...,\ T_n\},$$

де кожна топологія T_i описується графом $G_i = (V_i,\ E_i)$;

V_i − множина вузлів; E_i – множина каналів зв'язку.

Для оцінювання кіберстійкості вводиться множина критеріїв:

$$C = \{C_1,\ C_2,\ ...,\ C_m\},$$

які характеризують структурні та функціональні властивості мережі.

Кожній топології T_i за кожним критерієм C_j відповідає значення показника:

$$x_{ij} = f_j(T_i),$$

де x_{ij} – значення показника i топології та j критерію.

На основі значень показників x_{ij} для кожного критерію C_j сформовано вектор локальних пріоритетів альтернатив, отриманий через матрицю парних порівнянь альтернатив за критерієм C_j:

$$P^{(j)} = \{p_{1j},\ p_{2j},\ ...,\ p_{nj}\},$$

де p_{ij} – відносна перевага (вага) альтернативи T_i за критерієм C_j і виконується умова нормування: $\sum_{i=1}^{n} p_{ij} = 1,\ \ p_{ij} \geq 0.$

За методом аналізу ієрархій визначено ваги критеріїв:

$$W = \{w_1,\ w_2,\ ...,\ w_m\},\ \ \sum_{j=1}^{m} w_j = 1.$$

Задача полягає у визначенні інтегральної оцінки кіберстійкості для кожної топології T_i, визначеної як зважена сума локальних пріоритетів, згідно з виразом (1):

$$S_i = \sum_{j=1}^{m} w_j \cdot p_{ij}. \qquad (1)$$

Оптимальна топологія визначається як:

$$T^* = \arg \max_{T_i \in T} S_i.$$

Таким чином, практична реалізація запропонованої моделі потребує уточнення двох ключових складових: множини альтернатив, що визначають простір можливих топологічних рішень; системи критеріїв, які адекватно відображають кіберстійкість з урахуванням структурних властивостей мережі.

З огляду на те, що вибір критеріїв безпосередньо залежить від типу досліджуваних альтернатив, доцільним є попереднє обґрунтування набору топологій, що підлягають аналізу.

Для аналізу оцінки кіберстійкості ІС обрано наступну множину топології (рис. 1):

$$T = \{T_1, T_2, T_3, T_4, T_5\},$$

де T_1 – деревоподібна топологія (*Tree*);

T_2 – кільцева топологія (*Ring*);
T_3 – подвійне кільце (*Dual Ring*);
T_4 – кільце з центральним вузлом (*Ring + Hub*);
T_5 – частково-зв’язна мережа (*Partial Mesh*).

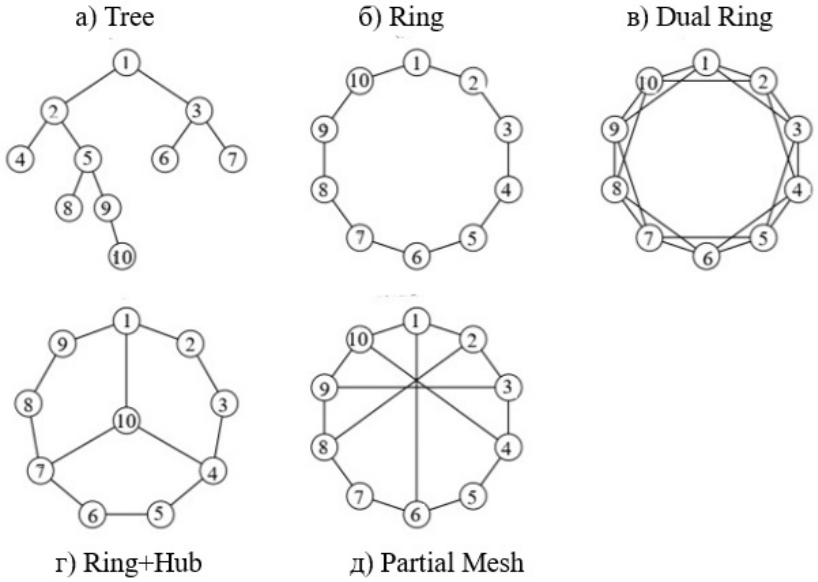

Рис. 1. Альтернативні топології мережі

Вибір топології *Tree, Ring, Dual Ring, Ring + Hub, Partial Mesh*, на наш погляд, є обґрунтованим, оскільки вони утворюють репрезентативну множину альтернатив, що відрізняються за рівнем централізації, резервування, зв’язності та наявністю альтернативних маршрутів передавання інформації. Це дозволяє всебічно дослідити вплив структурної організації мережі на кіберстійкість ІС. Використання однакової кількості вузлів $n = 10$ забезпечує коректність порівняння альтернатив і дає можливість зосередити аналіз саме на топологічних особливостях мережевої побудови.

Обрана множина топологій визначає простір альтернатив для оцінювання кіберстійкості та характеризується різними структурними властивостями, зокрема рівнем зв’язності, надмірності та централізації. Для їх коректного порівняння необхідно ввести систему критеріїв, що дозволяє кількісно оцінити вплив цих властивостей на стійкість мережі до деструктивних впливів. У зв’язку з цим наступним етапом є формування та обґрунтування критеріїв оцінювання кіберстійкості.

Для оцінювання кіберстійкості обраних топологічних структур введемо множину наступних критеріїв: робастність, алгебраїчна зв’язність, вершинна зв’язність, централізація графа, середня довжину шляхів.

У теорії графів робастність — це здатність графа зберігати зв’язність при видаленні вузлів або ребер. Робастність мережевої топології визначається її здатністю зберігати зв’язність та функціональну цілісність при частковому видаленні вузлів або каналів зв’язку та є структурною складовою кіберстійкості ІС [9].

Робастність мережевої структури є безрозмірним показником, що відображає частку збереженої зв’язності системи при поступовому видаленні її елементів та набуває значень у межах [0; 1]. Цей показник будемо визначати з урахуванням двох типів дестабілізуючих впливів: порушень вузлів (компрометація/відмова мережевих елементів) та порушень каналів зв’язку (блокування/перехоплення/порушення маршрутизації), що моделюються відповідно як видалення вершин і ребер графа. Для розрахунку робастності для всіх топологічних структур застосуємо формулу (2) [10]:

$$R = \frac{1}{k}\sum_{q=1}^{k} S(q), \tag{2}$$

де k – кількість вузлів; $S(q)$ − частка вузлів у найбільшій компоненті після видалення q вузлів, причому на кожному кроці вибирається така множина вилучених вузлів, яка мінімізує найбільшу компоненту, що відповідає імітації цільової атаки.

Робастність деревоподібної топології при цільової атаці становить $R_{Tree} = 0{,}16$, що свідчить про високу вразливість ієрархічної структури до атак на вузли з найбільшим ступенем.

Для кільцевої топології робастність становить $R_{Ring} = 0{,}23$, що перевищує відповідний показник деревоподібної структури. Це пояснюється відсутністю центральних вузлів і більш рівномірним розподілом зв'язків.

Робастність кільця з центральним вузлом дорівнюється $R_{Ring + Hub} = 0{,}25$. Додавання hub-вузла не завжди знижує кіберстійкість, у деяких випадках воно підвищує робастність завдяки резервним шляхам.

Робастність подвійного кільця становить $R_{Dual\ Ring} = 0{,}41$, бо подвійне кільце має більше альтернативних шляхів, не містить жодного критичного вузла, довше зберігає зв'язність при видаленні вузлів.

Для частково зв'язаної топології при цільовій атаці на вузли отримано значення робастності $R_{Partial\ Mesh} = 0{,}28$, що перевищує відповідні показники для кільцевої та деревоподібної структур. Це пояснюється наявністю додаткових каналів, які забезпечують збереження альтернативних маршрутів після видалення критичних вузлів.

Алгебраїчна зв'язність графа λ_2 визначається як друге найменше власне значення лапласіана графа та використовується як показник структурної зв'язаності мережі [11; 12].

Для кільцевої топології алгебраїчна зв'язність визначалась за аналітичними формулами (3), (4) спектра циклічного графа [11; 12]:

$$\lambda_{2_{Ring}} = 2\left(1 - \cos\frac{2\pi}{k}\right), \tag{3}$$

$$\lambda_{2_{Dual\ \ Ring}} = 2\left(1 - \cos\frac{4\pi}{k} - \cos\frac{8\pi}{k}\right), \tag{4}$$

де k – кількість вузлів графа. Для топології *Tree*, *Ring* + *Hub*, *Partial Mesh* значення λ_2 визначалися зі спектрів матриць лапласіанів графів. Отримані значення алгебраїчної зв'язності для аналізованих топології представлені в таблиці 1.

Таблиця 1

Значення алгебраїчної зв'язності

Топологія	Алгебраїчна зв'язність λ_2
Tree	0,154
Ring	0,382
Dual Ring	1,764
Ring + Hub	0,697
Partial Mesh	1,121

Для оцінювання мінімального рівня руйнування мережевої структури використано показник вершинної зв’язності графа *k(G)*, який визначає мінімальну кількість вузлів, видалення яких призводить до втрати зв’язності мережі. За критерієм вершинної зв’язності найбільш стійкою є двокільцева топологія $k_{Dual\ Ring} = 4$, тоді як деревоподібна структура має мінімальну стійкість $k_{Tree} = 1$. Кільцева, гібридна та частково зв’язана топології мають однакове значення вершинної зв’язності $k_{Ring} = k_{Ring+Hub} = k_{Partial\ Mesh} = 2$.

Централізація показує, наскільки мережа залежить від одного або кількох вузлів. Якщо більшість маршрутів проходить через один вузол, мережа високо централізована, що знижує її кіберстійкість. Це безрозмірна величина. Для оцінювання централізації топології використано ступеневу централізацію, що визначається через відхилення ступенів вершин від максимального значення. Такий підхід дозволяє виявити наявність структурно домінуючих вузлів у мережі і визначається за формулою (5) [13]:

$$C_D = \frac{\sum_{i=1}^{k} (d_{\max} - d(v_i))}{(k-1)(k-2)}, \tag{5}$$

де $d(v_i)$ – ступінь i вузла; $d_{\max}$ – максимальна ступінь у графі; k – кількість вузлів графа.

У таблиці 2 приведені отримані значення централізації альтернативних топології.

Таблиця 2

Значення централізації C_D

Топологія	Централізація C_D	Інтерпретація значень
Tree	0,167	Помірна централізація
Ring	0,000	Децентралізація
Dual Ring	0,000	Децентралізація
Ring + Hub	0,083	Низька централізація
Partial Mesh	0,083	Низька централізація

Отримані результати показують, що кільцеві топології мають нульову централізацію, тоді як ієрархічна деревоподібна структура характеризується більшою залежністю від окремих вузлів.

Середня довжина шляху у мережевій структурі – це середня кількість кроків, необхідних для з’єднання будь-яких двох випадкових вузлів мережі. Вона вимірює ефективність передачі інформації або взаємодії в мережі: чим менше це значення, тим швидше та ефективніше вузли. Середня довжина найкоротших шляхів характеризує компактність мережевої топології та визначає ефективність маршрутизації в умовах порушення зв’язності. Менші значення цього показника свідчать про наявність коротких альтернативних маршрутів, що підвищує здатність мережі зберігати функціональність після атак або відмов. Зростання середньої довжини шляхів призводить до підвищення залежності мережі від проміжних вузлів, збільшення затримок та ускладнення відновлення маршрутизації, що негативно впливає на кіберстійкість ІС. Для неорієнтованого графа середня довжина шляхів визначається за формулою (6) [14]:

$$L = \frac{2}{k(k-1)} \sum_{i<j} d(i,\ j), \tag{6}$$

де $d(i, j)$ – довжина найкоротшого шляху між вузламиі i та j; k − кількість вузлів.

У таблиці 3 приводяться значення середньої довжини шляхів топології, що аналізуються.

Таблиця 3

Підсумкова таблиця критерію *L*

Топологія	Середня довжина шляхів *L*
Tree	2,89
Ring	2,78
Dual Ring	1,67
Ring + Hub	2,09
Partial Mesh	1,84

У таблиці 4 приведено всі показники для типів мереж, що аналізуються.

Таблиця 4

Зведена таблиця показників

Критерій / Топологія	Робастність *R*	Структурна зв’язність λ_2	Вершинна зв’язність *k*	Централізація *C*	Середня довжина шляхів *L*
Tree	0,16	0,154	1	0,167	2,89
Ring	0,23	0,382	2	0	2,78
Dual Ring	0,41	1,764	4	0	1,67
Ring +Hub	0,25	0,697	2	0,083	2,09
Partial Mesh	0,28	1,121	2	0,083	1,84

Аналіз показників обраних критеріїв показує, що окремі топологічні критерії частково корелюють між собою, однак не є взаємозамінними. Зокрема, алгебраїчна зв’язність відображає спектральну стійкість графа, робастність − поведінку мережі при цільових атаках, централізація − наявність структурно домінуючих вузлів, середня довжина шляхів − компактність маршрутизації. Таким чином, обрані критерії (робастність, алгебраїчна зв’язність, вершинна зв’язність, централізація та середня довжина шляхів) забезпечують достатньо повне та об’єктивне оцінювання кіберстійкості.

Сформована система критеріїв дозволяє кількісно оцінити кіберстійкість розглянутих топологій, однак для отримання інтегральної оцінки та врахування відносної важливості кожного критерію необхідно застосувати метод багатокритеріального аналізу. З цією метою побудуємо ієрархічну модель задачі на основі методу аналізу ієрархій, яка забезпечує визначення ваг критеріїв і пріоритетів альтернатив.

Задачу оцінювання кіберстійкості можна подати у вигляді трирівневої ієрархії:

мета – вибір топології, яка структурно забезпечує найбільшу кіберстійкість за вибраними критеріями;

критерії – показники кіберстійкості (робастність, зв’язність, централізація тощо);

альтернативи – розглянуті топології мережі (*Tree*, *Ring*, *Dual Ring*, *Ring + Hub*, *Partial Mesh*).

Побудована ієрархія забезпечує основу для подальших парних порівнянь, визначення ваг критеріїв і локальних пріоритетів альтернатив.

Визначення відносної важливості критеріїв оцінювання кіберстійкості здійснюється із застосуванням методу парних порівнянь у межах методу аналізу ієрархій [2]. Такий підхід дозволяє формалізувати судження щодо пріоритетності критеріїв та врахувати їх неоднорідну природу.

При формуванні матриці парних порівнянь були враховані такі положення: критерії, що характеризують здатність мережі зберігати зв’язність (робастність, алгебраїчна зв’язність), як

правило, мають вищий пріоритет; критерії, що відображають вразливість структури (централізація), оцінюються з урахуванням ризику компрометації критичних вузлів; критерії ефективності (середня довжина шляхів) мають допоміжний характер і, як правило, поступаються за важливістю критеріям стійкості.

З урахуванням цих пріоритетів, матриця парних порівнянь критеріїв має наступний вигляд (табл. 5).

Таблиця 5

Матриця парних порівнянь обраних критеріїв

Критерій	R	λ_2	k	C_D	L
R	1	1,5	2	3	4
λ_2	2/3	1	1,5	2	3
k	1/2	2/3	1	1,5	2
C_D	1/3	1/2	2/3	1	1,5
L	1/4	1/3	1/2	2/3	1

Провівши відповідні дії методу аналізу ієрархій (нормалізація, виділення середніх значень, перевірка коефіцієнту узгодженості *CR*), отримаємо вектор ваг критеріїв:

$$W = \{R = 0{,}361,\ \lambda_2 = 0{,}253,\ k = 0{,}177,\ C_D = 0{,}123,\ L = 0{,}086\}.$$

Розрахований коефіцієнт узгодженості $CR = 0{,}00068$.

Отриманий розподіл ваг підтверджує, що при оцінюванні кіберстійкості ІС ключовими є показники, що характеризують здатність мережі зберігати зв’язність та функціональність в умовах деструктивних впливів.

Для кожної топології визначаються значення показників за обраними критеріями, на основі яких формуються локальні пріоритети альтернатив. Оцінювання здійснюється шляхом побудови матриць парних порівнянь для кожного критерію (табл. 6−10).

Таблиця 6

Матриця парних порівнянь топології за критерієм робастність

R	*Tree*	*Ring*	*Dual Ring*	*Ring + Hub*	*Partial Mesh*
Tree	1	2/3	1/5	1/2	1/3
Ring	3/2	1	1/4	2/3	1/2
Dual Ring	5	4	1	3	3
Ring + Hub	2	3/2	1/3	1	1
Partial Mesh	3	2	1/3	1	1
Коефіцієнт узгодженості *CR*			0,01		

Таблиця 7

Матриця парних порівнянь топології за критерієм алгебраїчна зв’язність

λ_2	*Tree*	*Ring*	*Dual Ring*	*Ring + Hub*	*Partial Mesh*
Tree	1	1/2	1/9	1/5	1/7
Ring	2	1	1/7	1/3	1/5
Dual Ring	9	7	1	6	3
Ring + Hub	5	3	1/6	1	1/3
Partial Mesh	7	5	1/3	3	1
Коефіцієнт узгодженості *CR*			0,06		

Таблиця 8

Матриця парних порівнянь топології за критерієм вершинна зв’язність

k	*Tree*	*Ring*	*Dual Ring*	*Ring + Hub*	*Partial Mesh*
Tree	1	1/2	1/5	1/2	1/2
Ring	2	1	1/3	1	1
Dual Ring	5	3	1	3	3
Ring + Hub	2	1	1/3	1	1
Partial Mesh	2	1	1/3	1	1
Коефіцієнт узгодженості *CR*			0,001		

Таблиця 9

Матриця парних порівнянь топології за критерієм централізація

C_D	*Tree*	*Ring*	*Dual Ring*	*Ring + Hub*	*Partial Mesh*
Tree	1	1/4	1/4	1/2	1/2
Ring	4	1	1	2	2
Dual Ring	4	1	1	2	2
Ring + Hub	2	1/2	1/2	1	1
Partial Mesh	2	1/2	1/2	1	1
Коефіцієнт узгодженості *CR*			0,000		

Таблиця 10

Матриця парних порівнянь топології за критерієм середня довжина шляхів

L	*Tree*	*Ring*	*Dual Ring*	*Ring + Hub*	*Partial Mesh*
Tree	1	1/2	1/5	1/3	1/4
Ring	2	1	1/4	1/2	1/3
Dual Ring	5	4	1	3	2
Ring + Hub	3	2	1/3	1	1/2
Partial Mesh	4	3	1/2	2	1
Коефіцієнт узгодженості *CR*			0,020		

Зведена матриця локальних пріоритетів альтернатив приведена в таблиці 11.

Таблиця 11

Зведена матриця локальних пріоритетів альтернатив

Критерій / Топологія	Робастність *R*	Структурна зв’язність λ_2	Вершинна зв’язність *k*	Централізація *C*	Середня довжина шляхів *L*
Tree	0,077	0,037	0,081	0,077	0,062
Ring	0,108	0,060	0,156	0,308	0,099
Dual Ring	0,462	0,516	0,451	0,308	0,416
Ring + Hub	0,163	0,130	0,156	0,154	0,161
Partial Mesh	0,190	0,257	0,156	0,154	0,262

Після визначення вагових коефіцієнтів критеріїв та локальних пріоритетів альтернатив за кожним критерієм здійснюється інтеграція отриманих результатів з метою формування узагальненої оцінки кіберстійкості. Інтегральна оцінка кожної альтернативи визначається як зважена сума локальних пріоритетів у матричній формі (1):

$$S = P \cdot W,$$

де $S = \{S_1, S_2, \ldots, S_n\}$ – вектор глобальних пріоритетів альтернатив і $\sum_{i=1}^{n} S_i = 1$ має нормований характер.

У результаті агрегації локальних пріоритетів отримано вектор глобальних оцінок кіберстійкості топологій:

$$S = \{S_{Tree} = 0{,}066,\ S_{Ring} = 0{,}128,\ S_{Dual\ Ring} = 0{,}451,\ S_{Ring\ +\ Hum} = 0{,}152,\ S_{Parth\ Mesh} = 0{,}203\}.$$

За отриманими значеннями глобальних пріоритетів топології впорядковуються наступним чином:

$$Dual \quad Ring \succ Parth \quad Mesh \succ Ring + Hub \succ Ring \succ Tree.$$

Результати оцінювання кіберстійкості топологій наведено на рисунку 2.

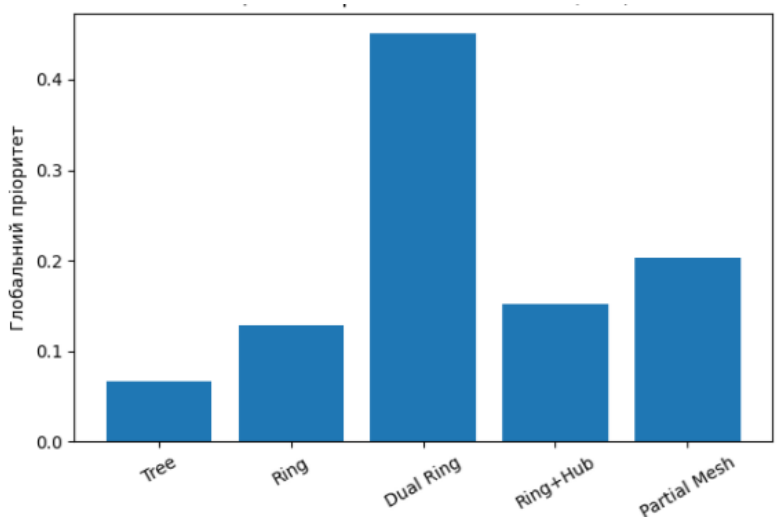

Рис. 2. Оцінка кіберстійкості топологій AHP

Як видно з графіка, топологія *Dual Ring* має суттєво вищий інтегральний показник (0,451) порівняно з іншими альтернативами, що підтверджує її перевагу за сукупністю критеріїв. Другу позицію займає *Partial Mesh* (0,203), тоді як топології *Ring* + *Hub* (0,152) та *Ring* (0,128) демонструють середні значення. Найнижчий рівень кіберстійкості характерний для *Tree* (0,066).

Отримані результати підтверджують, що топології з високим рівнем структурної надмірності та зв’язності забезпечують кращу кіберстійкість ІС. Найбільш доцільною для використання в умовах деструктивних впливів є топологія *Dual Ring*, яка забезпечує максимальну живучість мережі при збереженні прийнятної ефективності функціонування.

Висновки. У статті розроблено математичну модель оцінювання кіберстійкості ІС залежно від топології їхньої побудови на основі методу аналізу ієрархій. Сформовано множину альтернатив та обґрунтовано систему критеріїв, що відображають структурні властивості мережі.

Отримані вагові коефіцієнти підтвердили домінування показників структурної стійкості. За результатами розрахунків встановлено, що найбільш кіберстійкою є топологія *Dual Ring* (0,451), тоді як найменш стійкою – *Tree* (0,066).

Показано, що топологія мережі має визначальний вплив на рівень кіберстійкості, а застосування AHP забезпечує обґрунтоване ранжування альтернатив. Запропонований підхід дозволяє формалізувати процес вибору оптимальної мережевої структури в умовах багатокритеріальності та невизначеності.

Перспективним напрямком наукових досліджень є розширення моделі за рахунок використання нечітких FAHP, нейтрософських підходів та методу аналітичного мережевого процесу ANP, які дозволяють враховувати невизначеність і суперечливість експертних оцінок, а також взаємозалежності між критеріями оцінювання, що підвищує адекватність і точність моделі при аналізі кіберстійкості інформаційних систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ross R., McEvilley M., Oren J. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST Special Publication 800-160, Vol. 2 Rev. 1. Gaithersburg : National Institute of Standards and Technology, 2021. DOI: 10.6028/NIST.SP.800-160v2r1.

2. Saaty T. L. The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation. New York: McGraw-Hill International Book Company, 1980. 287 p. ISBN 9780070543713.

3. Jamakovic A., Van Mieghem P. On the Robustness of Complex Networks by Using the Algebraic Connectivity // NETWORKING 2008. Lecture Notes in Computer Science. Berlin; Heidelberg: Springer, 2008. Vol. 4982. P. 183–194. DOI: 10.1007/978-3-540-79549-0_16.

4. Jamakovic A., Uhlig S. On the Relationship Between the Algebraic Connectivity and Graph's Robustness to Node and Link Failures // Proceedings of the 3rd EuroNGI Conference on Next Generation Internet Networks. 2007. P. 96–102.

5. Alenazi M. J. F., Sterbenz J. P. G. Comprehensive Comparison and Accuracy of Graph Metrics in Predicting Network Resilience // 11th International Conference on the Design of Reliable Communication Networks (DRCN). Kansas City, 2015. DOI: 10.1109/DRCN.2015.7149007.

6. Liu J., Zhou M., Wang S., Liu P. A Comparative Study of Network Robustness Measures // Frontiers of Computer Science. 2017. Vol. 11, No. 4. P. 568–584. DOI: 10.1007/s11704-016-6108-z.

7. Meng F., Fu G., Farmani R., Sweetapple C., Butler D. Topological Attributes of Network Resilience: A Study in Water Distribution Systems // Water Research. 2018. Vol. 143. P. 376–386. DOI: 10.1016/j.watres.2018.06.048.

8. Yi J., Qin Z., Yang K., Zhao H., Han Q. AHP-Based Network Security Situation Assessment for Industrial Internet of Things // Electronics. 2023. Vol. 12, No. 16. Art. 3458. DOI: 10.3390/electronics12163458.

9. Diestel R. Graph Theory. 5th ed. Berlin: Springer, 2017. 428 p.

10. Schneider C. M., Moreira A. A., Andrade J. S., Havlin S., Herrmann H. J. Mitigation of malicious attacks on networks // *PNAS*. 2011.

11. Fiedler M. Algebraic connectivity of graphs // Czechoslovak Mathematical Journal. 1973. Vol. 23, № 2. P. 298–305.

12. Chung F. R. K. Spectral graph theory. Providence: American Mathematical Society, 1997. 212 p.

13. Freeman L. C. Centrality in social networks: conceptual clarification // *Social Networks*. 1979. Vol. 1. P. 215–239.

14. Diestel R. Graph Theory. 5th ed. Berlin: Springer, 2017. 428 p.

Надійшла до редколегії 30.03.2026.
Схвалена до друку 22.05.2026.
Дата публікації 29.05.2026.