DOI: https://doi.org/10.32782/2524-0072/2025-82-38

УДК 338.2:004.056:303.7

КОГНІТИВНА МОДЕЛЬ ПІДВИЩЕННЯ РІВНЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ ЗА КРИТЕРІЯМИ КІБЕРСТІЙКОСТІ

COGNITIVE MODEL FOR IMPROVING NATIONAL ECONOMIC SECURITY ACCORDING TO CYBER RESILIENCE CRITERIA

Маслій Олександра Анатоліївна
кандидат економічних наук, доцент,
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
ORCID: https://orcid.org/0000-0003-2184-968X

Черв'як Анна Володимирівна
доктор філософії,
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
ORCID: https://orcid.org/0000-0002-2747-4041

Maslii Oleksandra, Cherviak Anna
National University «Yuriy Kondratyuk Poltava Polytechnic»

У статті обґрунтовано доцільність використання когнітивного підходу до підвищення рівня економічної безпеки України за критеріями кіберстійкості. Розроблено когнітивну модель підвищення рівня економічної безпеки за критеріями кіберстійкості на засадах проактивного управління з використанням відповідного інструментарію й кіберінформаційних технологій їх реалізації з урахуванням Стратегії забезпечення державної безпеки (Указ Президента України від 30.12.2021 № 56/2022) та Стратегії економічної безпеки України на період до 2025 року (відповідний указ від 11.08.2021 №347) в умовах війни та повоєнного відновлення. Модель розроблена на основі синергетичного підходу, комбінації інтерпретаційного структурного моделювання (fuzzy–ISM) та адаптованої багатокритеріальної моделі прийняття рішень (MCDM). Виконано структурно-топологічний аналіз нечіткої когнітивної карти, у межах якого розраховано показники щільності, ієрархічності та центральності її вузлів. Шляхом сценарного моделювання імітовано динаміку впливу ідентифікованих концептів на стан захищеності об'єкта критичної інфраструктури. Запропонована когнітивна модель дозволяє інтегрувати економічні та кібернетичні аспекти безпеки, забезпечує системне бачення загроз і створює підґрунтя для формування стратегічних пріоритетів проактивного управління.

Ключові слова: економічна безпека держави, кібербезпека, кіберстійкість, когнітивна модель, проактивне управління.

The article substantiates the expediency of using a cognitive approach to enhancing Ukraine's economic security based on cyber resilience criteria. A cognitive model for improving economic security based on cyber resilience criteria is developed on the principles of proactive management using appropriate tools and cyber information technologies for their implementation, taking into account the Strategy for Ensuring National Security (Decree of the President of Ukraine № 56/2022 dated December 30, 2021) and the Strategy for Economic Security of Ukraine for the period up to 2025 (corresponding decree № 347 dated August 11, 2021) in the context of war and post-war recovery. The model is based on a synergetic approach, combining Fuzzy-ISM and an adapted multi-criteria decision-making (MCDM) model. The relevance of the topic stems from the growing role of cyber threats as a systemic factor influencing Ukraine's economic stability and national security in the context of war, digitalization, and integration into the global economic space. Large-scale cyberattacks on state information resources, the financial sector, and critical infrastructure lead to significant economic losses and a decline in investment attractiveness, necessitating a rethink of approaches to economic security. At the same time, the complexity, multifactoriality, and dynamic nature of modern threats limit the effectiveness of traditional analytical tools and determine the expediency of using cognitive modeling as a means of formalizing cause-and-effect relationships, assessing indirect effects, and scenario analysis of management decisions. In this context, the development of a cognitive model that integrates economic and cybernetic security parameters is a scientifically sound and practically significant task aimed at

increasing the resilience of Ukraine's economy in the context of military and post-war transformations. The integration of these methods has resulted in a cognitive model for enhancing the economic security of the state, which reflects the dynamic interrelationships between threats, management tools, and expected outcomes. The proposed model is focused on proactive management and involves the use of cyber-information technologies for monitoring and decision support. It allows for the integration of economic and cybernetic aspects of security, provides a systematic view of threats, and creates a basis for the formation of strategic priorities for proactive management.

Keywords: national economic security, cybersecurity, cyber resilience, cognitive model, proactive management.

Постановка проблеми. В умовах повномасштабної війни та повоєнного відновлення Україна стикається з комплексом системних загроз економічній безпеці, серед яких особливе місце займають кіберзагрози, гібридні атаки на критичну інфраструктуру, інформаційно-психологічні операції та порушення стійкості цифрових економічних процесів. Цифровізація економіки, з одного боку, створює нові можливості для розвитку, а з іншого посилює вразливість економічної системи до кіберзагроз і системних збоїв.

Традиційні підходи до забезпечення економічної безпеки здебільшого мають реактивний характер і не враховують складну нелінійну природу взаємозв'язків між економічними, інформаційними та кібернетичними чинниками. У цьому контексті актуалізується потреба у формуванні когнітивних моделей, здатних відображати причинно-наслідкові зв'язки між загрозами, вразливостями та управлінськими впливами, а також забезпечувати проактивне управління економічною безпекою держави.

Зазначена проблематика безпосередньо пов'язана з виконанням завдань, визначених у Стратегії забезпечення державної безпеки та Стратегії економічної безпеки України на період до 2025 року, особливо в частині посилення кіберстійкості національної економіки, захисту національних економічних інтересів і формування безпекоорієнтованого інформаційного середовища.

Аналіз останніх досліджень і публікацій. Проблеми економічної безпеки держави широко представлені у працях вітчизняних і зарубіжних науковців, де досліджуються питання ідентифікації загроз, оцінювання рівня безпеки, формування індикаторів та механізмів державного регулювання. Окремий напрям досліджень присвячено кібербезпеці та кіберстійкості як чинникам національної безпеки, захисту критичної інфраструктури та цифрової економіки.

Вивченню системи індикаторів, що використовуються для оцінки стану соціально-економічних систем різних рівнів ієрархії, присвячено праці багатьох учених, зокрема Богатчик Л.А. [1], Рудаченко О.О. та Клебанової Т.С. [2], Якимчук А.Ю., О. Кардаш О.Л., Постельжук О. П., Якимчук О.Ф. [3] та інших.

Манойленко О.В. [4] пропонує будувати когнітивну модель впливу факторів на економічну безпеку України із використанням сценарного підходу. Діденко А.В. та Протопопова Н.А. [5] розглядають когнітивне моделювання для оцінювання стану соціально-економічних систем.

Салієва О.В. та Яремчук Ю.Є. [6] у своїй роботі пропонують застосування когнітивної моделі на базі нечітких когнітивних карт для аналізу загроз і захищеності об'єктів критичної інфраструктури. Bellini E. та співавтори [7] здійснюють огляд перетину cyber resilience та Situation Awareness для побудови когнітивних критеріїв і контурів зворотного зв'язку.

Пугач О.А. [8] зазначає, що важливою властивістю системи економічної безпеки національної економіки є цілеспрямованість, що обумовлено адаптивністю її поведінки. І відповідно пропонує вивчення механізмів цілеспрямованої поведінки системи через структурну модель виникнення та розвитку загроз економічній безпеці національної економіки.

У сучасних наукових працях застосовуються методи багатокритеріального аналізу, системної динаміки, нечіткої логіки, підходи ризик-орієнтованого та адаптивного управління. Водночас більшість досліджень зосереджені на технічних аспектах кібербезпеки або розглядають економічну безпеку без належної інтеграції кібернетичного виміру.

Виділення невирішених раніше частин загальної проблеми. Потребують ґрунтовнішого дослідження питання інтеграції критеріїв кіберстійкості в систему економічної безпеки держави та використання когнітивних моделей для підтримки проактивних управлінських рішень у сфері економічної безпеки.

Формулювання цілей статті (постановка завдання). Розроблення когнітивної моделі підвищення рівня економічної безпеки України за критеріями кіберстійкості на засадах проактивного управління з використанням сучасного інструментарію в умовах війни та повоєнного відновлення. Досліджувана

проблема розглядатиметься системно, через призму економічної безпекології та побудови ефективних систем захисту інформації, а також більш масштабно з огляду на сучасні безпекові виклики в умовах війни.

Виклад основного матеріалу дослідження. Дослідження базується на синергетичному підході, який дозволяє розглядати економічну безпеку як складну відкриту систему, що функціонує в умовах невизначеності, турбулентності та багатофакторного впливу. У межах економічної безпекології кіберстійкість розглядається як інтегральна характеристика здатності економічної системи протистояти, адаптуватися та відновлюватися після кібернетичних і інформаційних впливів.

З метою розроблення когнітивної моделі підвищення рівня економічної безпеки держави за критеріями кіберстійкості, проактивного управління та з урахуванням воєнних дій на території України, за результатами аналізу нормативних документів та наукових праць можна сформувати множину основних детермінант економічній безпеці держави в умовах цифровізації [6; 8; 9; 10]:

– цільові концепти захисту національних економічних інтересів;
– кіберстійкість;
– технологічні спроможності;
– кадрові та організаційні спроможності;
– нормативно-правові та управлінські драйвери;
– цифрова трансформація та відновлення економіки.

Запропоновані категорії загроз є коректними для побудови когнітивної моделі економічної безпеки держави за критеріями кіберстійкості. Вони сформульовані як системні концепти, які в когнітивній моделі можуть виступати як дестимуляторами так і драйверами залежно від стану та напряму впливу. Визначені категорії не лише відповідають чинній нормативній базі України, а й органічно інтегруються в когнітивну модель як взаємопов'язані елементи, що дозволяють відобразити багатовимірний характер загроз економічній безпеці за критеріями кіберстійкості в умовах війни та повоєнного відновлення.

Найбільшу небезпеку становлять комбіновані загрози, а також такі, реалізація яких здатна спричинити катастрофічні та багатовимірні каскадні ефекти, обумовлені високим рівнем взаємозалежності елементів досліджуваної системи. [6]

У аналітичній довідці «Зелена книга з питань захисту критичної інфраструктури в Україні» [11] загрози критичній інфраструктурі розглядаються не лише за характером їх походження, а й за елементами, на які вони спрямовані. Даний поділ також є актуальним при визначенні загроз економічній безпеці держави за критеріями кіберстійкості. Найбільш уразливими складовими є фізичні компоненти (обладнання та ресурси), управлінсько-комунікаційні системи (автоматизовані системи управління й зв'язку), а також персонал об'єктів – насамперед диспетчерський і оперативний, який забезпечує безперервне функціонування систем у реальному часі.

За підсумками опрацювання наукових джерел та нормативно-правової бази [9; 10; 11; 12; 13] сформовано сукупність ключових концептів, що мають визначальне значення для дослідження потенційних загроз економічній безпеці держави крізь призму кіберстійкості на засадах проактивного управління:

К1. Рівень економічної безпеки держави – показник стійкості національної економіки до внутрішніх і зовнішніх загроз, зокрема кібернетичних, у воєнний і повоєнний періоди.

К2. Стійкість фінансово-економічної системи – здатність фінансових ринків, бюджету, банківської та платіжної систем функціонувати без критичних збоїв під впливом криз і кібератак.

К3. Інвестиційна та макрофінансова стабільність – рівень довіри інвесторів, кредиторів і міжнародних партнерів, що залежить від передбачуваності та безпеки економічного середовища.

К4. Кіберстійкість критичної інформаційної інфраструктури – здатність об'єктів енергетики, фінансів, транспорту, зв'язку та держуправління протидіяти кібератакам і швидко відновлюватися.

К5. Безперервність державних та фінансових сервісів – здатність ключових цифрових і фінансових послуг працювати без зупинок навіть у разі кібератак або фізичних ушкоджень.

К6. Операційна кіберстійкість – ефективність процесів виявлення інцидентів, реагування та відновлення.

К7. Стійкість цифрових державних реєстрів і даних – захищеність, цілісність та доступність державних інформаційних ресурсів, зокрема реєстрів у сфері фінансів, власності, соціальної політики.

К8. Технологічна зрілість систем кіберзахисту – рівень впровадження сучасних технологій: Zero Trust, SIEM/SOAR, EDR/XDR, шифрування, резервування.

К9. Фізична безпека інфраструктури – інтегрований захист цифрових і фізичних компонентів.

К10. Стійкість телекомунікаційних і мережевих систем – здатність мереж зв'язку забезпечувати доступність і цілісність інформаційних потоків у кризових умовах.

К11. Рівень автоматизації та аналітики кіберзахисту – використання AI, поведінкової аналітики та автоматизованих сценаріїв реагування.

К12. Кадровий потенціал у сфері кібербезпеки – наявність кваліфікованих фахівців у державному та фінансовому секторах.

К13. Рівень кіберкультури та обізнаності персоналу – наявність навичок безпечної поведінки, протидії фішингу, соціальній інженерії.

К14. Інституційна спроможність державних органів – здатність реалізовувати політику кібербезпеки та координувати дії у кризових ситуаціях.

К15. Міжвідомча координація – ефективність взаємодії між державними органами, фінансовим сектором і приватним бізнесом.

К16. Нормативно-правове забезпечення кібербезпеки – якість законодавства, стандартів, вимог та відповідальності за порушення.

К17. Державна політика проактивного управління кіберризиками – перехід від реактивної до превентивної моделі управління кіберзагрозами.

К18. Фінансування заходів з кіберстійкості – обсяги та стабільність фінансування з державного бюджету та міжнародної підтримки.

К19. Система управління кіберризиками – формалізовані процедури ідентифікації, оцінювання та мінімізації кіберризиків у державі.

К20. Обмін даними з кіберрозвідки – систематичний обмін інформацією про загрози між державними, фінансовими та міжнародними структурами.

К21. Міжнародна співпраця у сфері кібербезпеки – взаємодія з партнерами, CERT-мережами, міжнародними організаціями та союзниками.

К22. Цифрова трансформація держави – рівень цифровізації управління та фінансових процесів як чинник ефективності й одночасно ризику.

К23. Secure-by-design у цифрових проєктах – інтеграція вимог кібербезпеки на всіх етапах цифрової трансформації.

К24. Інтенсивність кіберзагроз і гібридних атак – рівень тиску з боку державних і недержавних суб'єктів у кіберпросторі.

К25. Воєнні та поствоєнні ризики для кіберпростору – специфічні ризики, пов'язані з бойовими діями, руйнуванням інфраструктури та відновленням.

Для побудови когнітивної моделі підвищення рівня економічної безпеки держави за критеріями кіберстійкості визначаємо силу впливу $W_{ij}T\left[-1;1\right]$, яка характеризує вплив зміни концепта Ki на концепт Kj. Зв'язки між концептами у когнітивній моделі можуть бути додатними, тобто підсилюючими вплив концепту Ki на концепт Kj ($W_{ij} > 0$), так і від'ємними – послаблюючими вплив концепту Ki на концепт Kj ($W_{ij} < 0$).

Для розв'язання завдання необхідно задати нечітку лінгвістичну шкалу. У дослідженні [6] використано актуальну шкалу для побудови когнітивної моделі підвищення рівня економічної безпеки держави за критеріями кіберстійкості: Сила зв'язку = {Не впливає; Дуже слабка; Слабка; Середня; Сильна; Дуже сильна}. Кожному з цих термінів поставимо у відповідність числовий діапазон з врахуванням позитивного та негативного впливу:

$$W_{ij} = \begin{cases} (0{,}85;\ 1] \text{ - позитивна дуже сильна;} \\ (0{,}6;\ 0{,}85] \text{ - позитивна сильна;} \\ (0{,}35;\ 0{,}6] \text{ - позитивна середня;} \\ (0{,}15;\ 0{,}35] \text{ - позитивна слабка;} \\ (0;\ 0{,}15] \text{ - позитивна дуже слабка;} \\ 0 \text{ – не впливає;} \\ (0;\ -0{,}15] \text{ - негативна дуже слабка;} \\ (-0{,}15;\ -0{,}35] \text{ - негативна слабка;} \\ (-0{,}35;\ -0{,}6] \text{ - негативна середня;} \\ (-0{,}6;\ -0{,}85] \text{ - негативна сильна;} \\ (-0{,}85;\ -1] \text{ - негативна дуже сильна.} \end{cases}$$

Відповідно до числового діапазону здійснюється кількісна оцінка інтенсивності взаємозв'язків між кожною парою концептів, що відображається у відповідних числових значеннях. Формування фахівцями у сфері економічної безпеки держави структурованого уявлення про систему захисту, визначення переліку ключових концептів і характеру та сили їх взаємного впливу створює методологічні передумови для побудови когнітивної моделі підвищення рівня економічної безпеки держави за критеріями кіберстійкості (рис. 1). Моделювання когнітивної моделі виконано за допомогою програмного забезпечення Mental Modeler [14].

У результаті аналізу причинно-наслідкових зв'язків між концептами встановлено, що роз-

роблена когнітивна модель характеризується наявністю 90 взаємозв'язків між концептами. У структурі моделі виокремлено шість концептів зі статусом «Driver», які здійснюють односторонній вплив на інші елементи системи та не зазнають зворотного впливу, а також дев'ятнадцять концептів зі статусом «Ordinary», для яких характерні двосторонні, взаємозалежні зв'язки з іншими концептами моделі.

Розглянемо матрицю $W_{ij} = \left[w(\mathrm{K}\forall\mathrm{Kj}) \right]_{n^x n}$, взаємовпливів концептів даної когнітивної моделі (табл. 1, табл. 2).

Визначимо структурно-топологічні властивості розробленої когнітивної моделі, проаналізувавши показники структурної складності – щільність, індекс ієрархії та центральність концептів.

Щільність (насиченість) когнітивної моделі, тобто рівень взаємопов'язаності концептів між собою знаходиться за формулою:

$$\mathrm{d} = \frac{\mathrm{m}}{\mathrm{n}(\mathrm{n}-1)}, \qquad (1)$$

де *n* – загальна кількість концептів, m – загальна кількість зв'язків. Для представленої когнітивної матриці *d* = 0,15. Отримане значення показника щільності свідчить про помірну структурну насиченість когнітивної моделі, обмежену кількість зворотних зв'язків і достатній рівень структурної впорядкованості, що забезпечує можливість виокремлення ключових драйверів впливу. Така структура моделі створює підґрунтя для формування пріоритетних управлінських впливів і застосування інструментарію сценарного та проактивного управління.

Центральність концепта відображає ступінь його залученості до системи причинно-наслідкових зв'язків когнітивної моделі та характеризує інтенсивність взаємодії відповідного концепта з безпосередньо пов'язаними з ним сусідніми концептами.

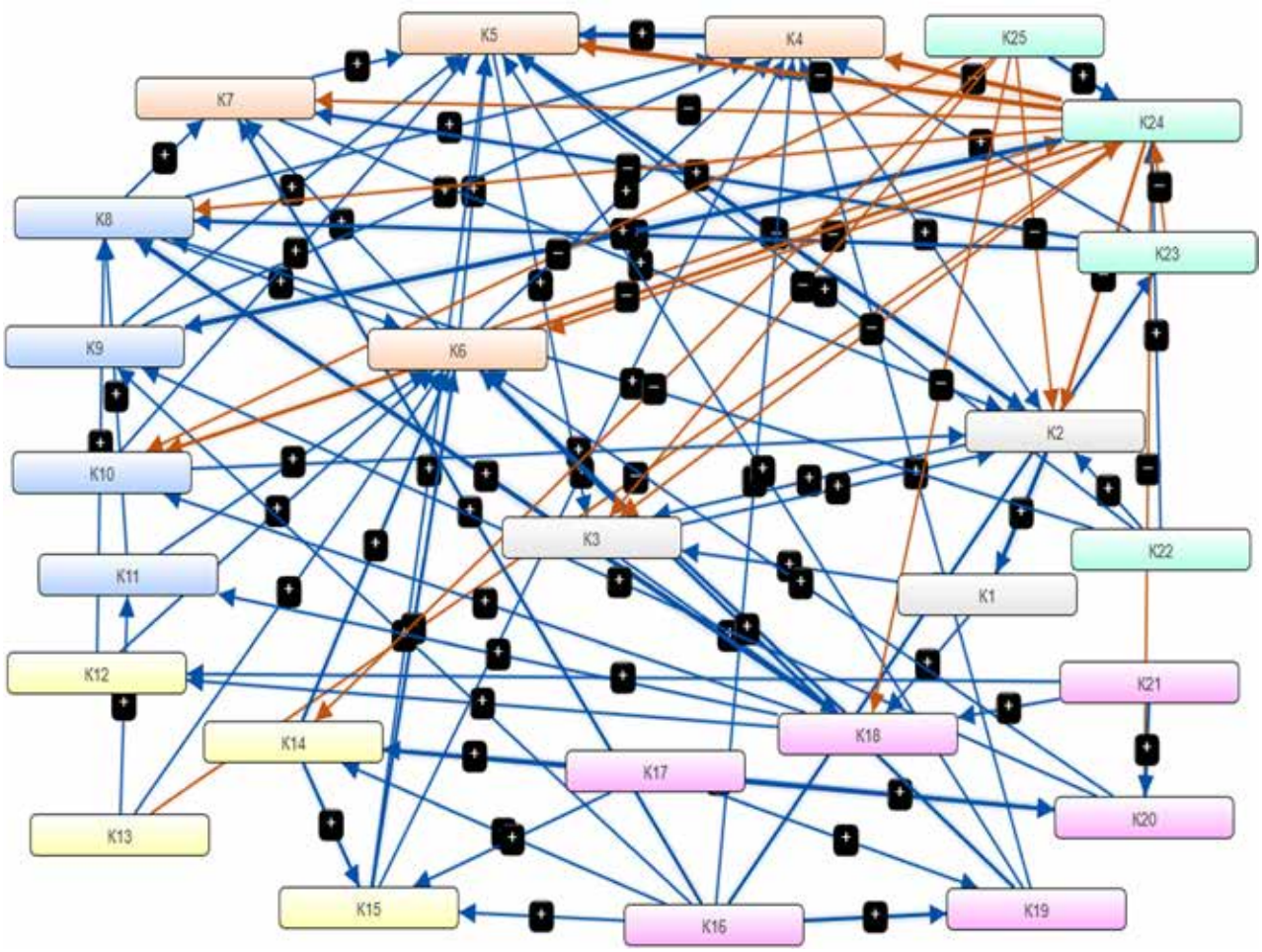

Рис. 1. Когнітивна модель підвищення рівня економічної безпеки держави за критеріями кіберстійкості

Джерело: сформовано авторами на основі [14]

Таблиця 1

Матриця взаємовпливів концептів предметної області на концепти К1 – К12 у когнітивній моделі

	К1	К2	К3	К4	К5	К6	К7	К8	К9	К10	К11	К12
К1			0,25									
К2	0,9		0,25									
К3		0,25										
К4		0,25			0,95							
К5		0,9	0,45									
К6				0,45	0,45		0,45					
К7		0,25			0,45							
К8				0,45		0,25	0,45					
К9				0,45	0,25					0,5		0,25
К10		0,25			0,45							
К11						0,45		0,25				
К12						0,45		0,25				
К13						0,25					0,25	
К14						0,5						
К15				0,25	0,45	0,5						
К16				0,2			0,5		0,25			
К17												
К18						0,5		0,95		0,45	0,45	0,45
К19				0,25	0,25	0,5						
К20						0,45			0,25			
К21												0,25
К22		0,25			0,25			0,25				
К23				0,25			0,5	0,55				
К24		-0,5	-0,45	-0,9	-0,9	-0,25	-0,45	-0,25	1	-0,5		
К25		-0,25	-0,25							-0,45		

Джерело: сформовано авторами на основі [9; 10; 11; 12; 13]

Кількісно центральність визначається за формулою:

$$\mathrm{td_i} = \mathrm{od_i} + \mathrm{id_i}, \quad (2)$$

де $\mathrm{od_i}$ це вихідна центральність, що характеризує вихідну сукупну силу зв'язку (W_{ij}) аналізованого концепта Ki:

$$\mathrm{od_i} = \sum_{j=1}^{n} W_{ij}, \quad (3)$$

де $\mathrm{od_j}$ це вхідна центральність, що характеризує вхідну сукупну силу зв'язку (W_{ij}) аналізованого концепта Ki:

$$i\mathrm{d_i} = \sum_{j=1}^{n} W_{ij}, \quad (4)$$

Розрахунок показників центральності для представленої когнітивної моделі підвищення рівня економічної безпеки держави за критеріями кіберстійкості показав, що найвищу структурну значимість мають концепти інтенсивності кіберзагроз і гібридних атак ($\mathrm{td}_{24} = 7,45$), безперервності державних та фінансових сервісів ($\mathrm{td}_5 = 5,75$) та операційної кіберстійкості ($\mathrm{td}_6 = 5,7$). Основні показники предметної області когнітивної моделі економічної безпеки держави за критеріями кіберстійкості представлено у таблиці 3.

Індекс ієрархії (h) когнітивної моделі характеризує модель як повністю ієрархічну при *h* = 1, або як повністю демократичну при *h* = 0. Він розраховується за формулою:

$$h = \frac{12 * \tilde{A}_{od}^2}{n^2 - 1}, \text{ де} \quad (5)$$

Таблиця 2

Матриця взаємовпливів концептів предметної області на концепти К13 – К12 у когнітивній моделі

	К13	К14	К15	К16	К17	К18	К19	К20	К21	К22	К23	К24	К25
К1						0,25	0,25						
К2													
К3						0,25	0,4	0,4					
К4													
К5													
К6												-0,25	
К7													
К8													
К9												-0,5	
К10													
К11													
К12													
К13												-0,25	
К14			0,5					0,5					
К15													
К16		0,45	0,45				0,5				0,5		
К17		0,25	0,25				0,45	0,45					
К18													
К19													
К20												-0,25	
К21						0,25		0,5					
К22												0,25	
К23												-0,25	
К24													
К25		-0,25				-0,25						0,5	

Джерело: сформовано авторами на основі [9;10; 11; 12; 13]

$$¼_{\text{od}} = \frac{\sum_{i=1}^{n} od_i}{\text{n}}, \quad (6)$$

$$\sigma_{od}^2 = \frac{\sum_{i=1}^{n} (od_i - \mu_{od}).^2}{\text{n}} \quad (7)$$

Для розробленої моделі *h* = 0,05, що свідчить про мережевий характер взаємодії концептів та високий рівень структурної взаємозалежності концептів. За таких умов система функціонує не як жорстко підпорядкована ієрархія, а як взаємопов'язана мережа, у якій зміни одного елемента можуть поширюватися через множинні контури зворотного зв'язку.

Отримане значення індексу ієрархії підтверджує актуальність когнітивної моделі для аналізу сценаріїв розвитку та оцінювання системної стійкості, оскільки відсутність жорсткої ієрархії підвищує чутливість моделі до альтернативних управлінських впливів. Водночас це обґрунтовує доцільність застосування проактивного та адаптивного управління, спрямованого не на ізольований вплив на окремі концепти, а на узгоджену зміну взаємопов'язаних підсистем.

У ході проведення аналізу було встановлено що найвищу структурну значимість має концепт К24 – інтенсивність кіберзагроз і гібридних атак. Доцільно провести сценарне моделювання для встановлення зміни рівня економічної безпеки держави за критеріями кіберстійкості при максимальному впливі на неї найвагомішого концепту.

Таблиця 3

Основні показники предметної області когнітивної моделі

№	Компонент	Вхідна сила зв'язку	Вихідна сила зв'язку	Загальний вплив концепту
1.	К24	2,25	5,2	7,45
2.	К5	4,4	1,35	5,75
3.	К6	4,1	1,6	5,7
4.	К4	3,2	1,2	4,4
5.	К2	2,9	1,15	4,05
6.	К18	1	2,8	3,8
7.	К8	2,5	1,15	3,65
8.	К9	1,5	1,95	3,45
9.	К7	2,35	0,7	3,05
10.	К3	1,65	1,3	2,95
11.	К16	0	2,85	2,85
12.	К20	1,85	0,95	2,8
13.	К19	1,6	1	2,6
14.	К10	1,9	0,7	2,6
15.	К14	0,95	1,5	2,45
16.	К15	1,2	1,2	2,4
17.	К23	0,5	1,55	2,05
18.	К25	0	1,95	1,95
19.	К12	0,95	0,7	1,65
20.	К1	0,9	0,75	1,65
21.	К17	0	1,4	1,4
22.	К11	0,7	0,7	1,4
23.	К22	0	1	1
24.	К21	0	1	1
25.	К13	0	0,75	0,75

Джерело: сформовано авторами на основі [14]

Сценарій 1. Моделюємо ситуацію при максимально негативному значенні концепту інтенсивності кіберзагроз і гібридних атак.

Відповідно до сформованої діаграми за допомогою програмного забезпечення Mental Modeler (рис. 2) спостерігається значне зниження ряду концептів, що свідчить про комплексний дестабілізуючий вплив К24 на систему економічної безпеки держави за критеріями кіберстійкості, що підтверджується поведінкою ключових концептів моделі.

Зниження концепту К1 відображає інтегральний негативний ефект дії кіберзагроз на всі підсистеми. Погіршення К2 та К3 свідчить про високу чутливість фінансового середовища до цифрових і гібридних ризиків. Найбільш суттєве падіння К4 (-0,14) підтверджує його ключову роль як системоутворюючого елемента та основного каналу поширення каскадних негативних ефектів. Зменшення К5 та К6 відображає порушення стабільності функціонування цифрових процесів. Зниження К7 та К8 свідчить про вразливість цифрової основи державного управління. Негативна динаміка К10 підкреслює залежність кіберстійкості від надійності мережевої інфраструктури. Скорочення К18 обмежує можливості превентивного реагування, тоді як зниження К19 та К20 вказує на ослаблення інституційних і координаційних механізмів безпеки.

Водночас зростання К9 та кадрового потенціалу у сфері кібербезпеки К12 відображає реактивну адаптацію системи до посилення загроз, яка має компенсаторний характер,

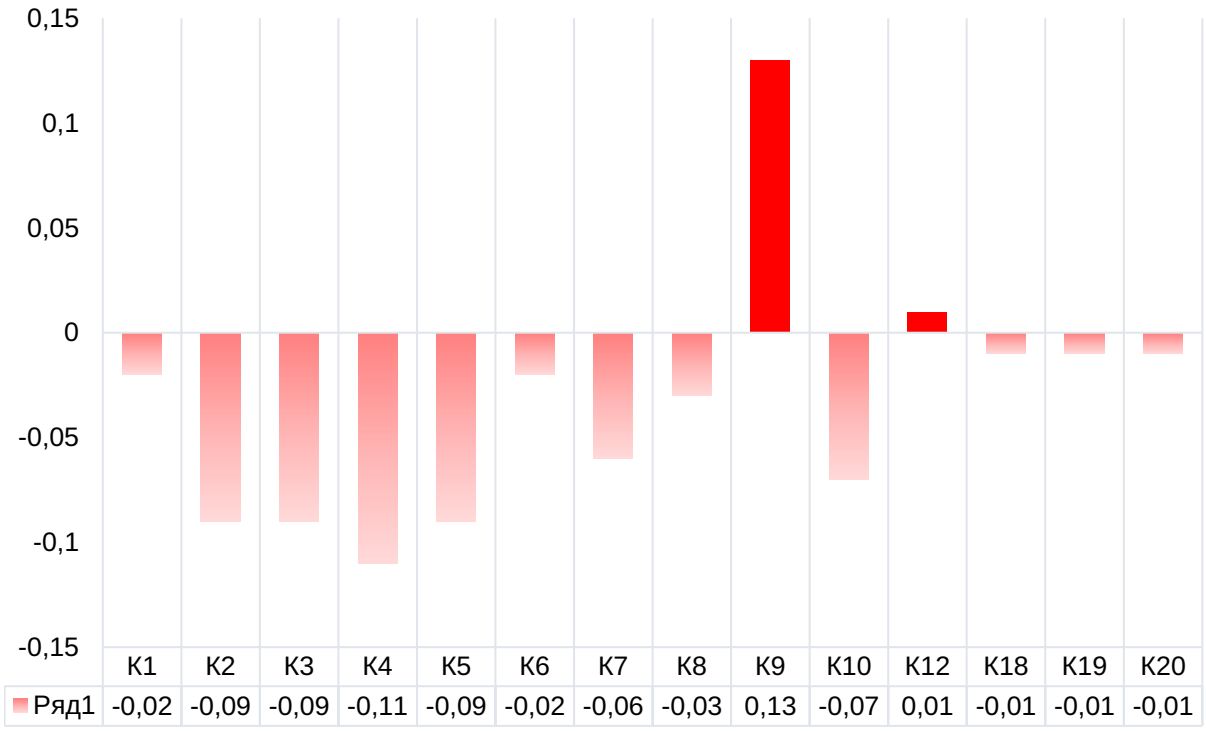

Рис. 2. Зміни в концептуальній моделі при реалізації сценарію з максимально негативним значенням концепту К24

Джерело: сформовано авторами на основі [14]

але не здатна повністю нейтралізувати системні деструктивні ефекти.

У цілому отримані результати підтверджують, що ескалація кіберзагроз і гібридних атак формує каскадне зниження ключових параметрів економічної безпеки, що обґрунтовує необхідність проактивного, системно орієнтованого управління кіберстійкістю держави з акцентом на критичну інфраструктуру, фінансування, управління ризиками та міжвідомчу координацію.

Розроблена когнітивна модель є основою для обґрунтування стратегічних пріоритетів підвищення економічної безпеки держави на засадах проактивного управління з використанням відповідного інструментарію й кіберінформаційних технологій їх реалізації в умовах війни та повоєнного відновлення.

Висновки. Результати дослідження сприятимуть формуванню безпекоорієнтованого інформаційного середовища, створенню сучасної ІТ-інфраструктури, забезпеченню захисту національних економічних інтересів, стійкості, адаптивності національної економіки в умовах воєнних та повоєнних викликів, зміцненню економічної безпеки держави в цілому.

Практична цінність отриманих результатів полягає у можливості їх використання при розробленні державних програм зміцнення економічної безпеки, формуванні безпекоорієнтованого інформаційного середовища та створенні сучасної ІТ-інфраструктури в умовах воєнних і повоєнних викликів.

Перспективи подальших досліджень пов’язані з емпіричною апробацією запропонованої моделі, її адаптацією до окремих секторів економіки та розширенням інструментарію оцінювання кіберстійкості на макро- та мікрорівнях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Богатчик Л. А. Аналіз можливостей застосування кластерного підходу як індикатора рівня економічної безпеки соціально-економічних систем. *Вісник Хмельницького національного університету.* 2021. № 290(1). С. 219–225.

2. Рудаченко О. О., Клебанова Т. С. Розвиток регіональних соціально-економічних систем в умовах кризи: аналіз, оцінка, прогнозування : монографія. Харків : ХНУМГ ім. О. М. Бекетова, 2023. 400 с.

3. Якимчук А. Ю., Кардаш О. Л., Постельжук О. П., Якимчук О. Ф. Оцінка показників соціальної безпеки України у контексті національної безпеки держави задля досягнення цілей сталого розвитку. *Інвестиції: практика та досвід.* 2020. № 13. С. 75–80. URL: http://www.investplan.com.ua/pdf/13-14_2020/13.pdf (дата звернення: 15.12.2025).

4. Манойленко О.В., Ягі М. Когнітивне моделювання забезпечення безпеки національної економіки України. *Причорноморські економічні студії.* 2018. № 28(1). С. 188–193.

5. Діденко А.В., Протопопова Н.А. Оцінка індикаторів стану соціально-економічних систем країни. *Економіка та суспільство.* 2023. № 51. URL: https://economyandsociety.in.ua/index.php/journal/article/view/2451/2370 (дата звернення: 15.12.2025).

6. Салієва О.В., Яремчук Ю.Є. Когнітивна модель для дослідження рівня захищеності об'єкта критичної інфраструктури. *Безпека інформації.* 2020. № 26(2). С. 164–73.

7. Bellini E., D'Aniello G., Francesco Flammini F., Gaeta R. Situation Awareness for Cyber Resilience: A review. *International Journal of Critical Infrastructure Protection.* 2025. № 49. С. 2–18. URL: https://www.sciencedirect.com/science/article/pii/S1874548225000162 (дата звернення: 14.12.2025).

8. Пугач О. А. Моделювання загроз системі економічної безпеки національної економіки з позицій їх своєчасного виявлення та передбачення. *Економіка і регіон*. 2015. № 3(52). С. 103–109.

9. Стратегія забезпечення державної безпеки. Указ Президента України від 30.12.2021 № 56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#Text (дата звернення: 20.12.2025).

10. Стратегія економічної безпеки України на період до 2025 року. Указ Президента України від 11.08.2021 №347. URL: https://zakon.rada.gov.ua/laws/show/347/2021#Text (дата звернення: 20.12.2025).

11.Бірюков Д.С., Кондратов С.І., Насвіт О.І., Суходоля О.М. Зелена книга з питань захисту критичної інфраструктури в Україні: аналітична доповідь. Київ : НІСД, 2015. 35 с.

12. Маслій О.А., Галушка Р.М. Ієрархічний аналіз ризиків і загроз економічній безпеці України в умовах воєнного стану. *Економічний простір.* 2025. № 198. С. 69–75.

13. Onyshchenko S., Maslii O., Hlushko A. Digital and Economic Security of the State Under Global Threats. *Lecture Notes in Networks and Systems.* 2025. Vol. 1338. С. 580-602.

14. Програмне забезпечення Mental Modeler. URL: https://www.mentalmodeler.com (дата звернення: 23.12.2025).

REFERENCES:

1. Bohatych L.A. (2021) Analiz mozhlyvostey zastosuvannya klasternoho pidkhodu yak indykatora rivnya ekonomichnoyi bezpeky sotsial'no-ekonomichnykh system [Analysis of the possibilities of applying the cluster approach as an indicator of the level of economic security of socio-economic systems]. *Bulletin of Khmelnytsky National University,* vol. 290(1), pp. 219–225.

2. Rudychenko O. O., Klebanova T. S. (2023) *Rozvytok rehional'nykh sotsial'no-ekonomichnykh system v umovakh kryzy: analiz, otsinka, prohnozuvannya* [Development of regional socio-economic systems in crisis conditions: analysis, assessment, forecasting: monograph]. Kharkiv: O. M. Beketov National University of Water and Environmental Engineering, 400 p. (in Ukrainian)

3. Yakymchuk A. Y., Kardash O. L., Postelzuk O. P., Yakymchuk O. F. (2020) Otsinka pokaznykiv sotsial'noyi bezpeky Ukrayiny u konteksti natsional'noyi bezpeky derzhavy zadlya dosyahnennya tsiley staloho rozvytku [Assessment of Ukraine's social security indicators in the context of national security for the achievement of sustainable development goals]. *Investments: practice and experience,* vol. 13, pp. 75–80. Available at: http://www.investplan.com.ua/pdf/13-14_2020/13.pdf (accessed December 15, 2025)

4. Manoilenko O.V., Yagi M. (2018) Kohnityvne modelyuvannya zabezpechennya bezpeky natsional'noyi ekonomiky Ukrayiny [Cognitive modeling of ensuring the security of Ukraine's national economy]. *Black Sea Economic Studies*, vol. 28(1), pp. 188–193.

5. Didenko A.V., Protopopova N.A. (2023) Otsinka indykatoriv stanu sotsial'no-ekonomichnykh system krayiny [Assessment of indicators of the state of the country's socio-economic systems]. *Economy and Society*, vol. 51. Available at: https://economyandsociety.in.ua/index.php/journal/article/view/2451/2370 (accessed December 15, 2025)

6. Salieva O.V., Yaremchuk Y.E. (2020) Kohnityvna model' dlya doslidzhennya rivnya zakhyshchenosti ob'yekta krytychnoyi infrastruktury [Cognitive model for researching the level of protection of critical infrastructure objects]. *Information Security*, vol. 26(2), pp. 164–73.

7. Bellini E., D'Aniello G., Francesco Flammini F., Gaeta R. (2025) Situation Awareness for Cyber Resilience: A review. *International Journal of Critical Infrastructure Protection*, vol. 49, pp. 2–18. Available at: https://www.sciencedirect.com/science/article/pii/S1874548225000162 (accessed December 14, 2025)

8. Pugach O. A. (2015) Modelyuvannya zahroz systemi ekonomichnoyi bezpeky natsional'noyi ekonomiky z pozytsiy yikh svoyechasnoho vyyavlennya ta peredbachennya [Modeling threats to the economic security system of the national economy from the perspective of their timely detection and prediction]. *Economy and Region*, vol. 3(52), pp. 103–109.

9. Stratehiya zabezpechennya derzhavnoyi bezpeky. Ukaz Prezydenta Ukrayiny vid 30.12.2021 № 56/2022 [Strategy for ensuring national security. Decree of the President of Ukraine № 56/2022 dated December 30, 2021]. Available at: https://zakon.rada.gov.ua/laws/show/56/2022#Text (accessed December 20, 2025)

10. Stratehiya ekonomichnoyi bezpeky Ukrayiny na period do 2025 roku. Ukaz Prezydenta Ukrayiny vid 11.08.2021 № 347 [Strategy for Economic Security of Ukraine for the Period until 2025. Decree of the President of Ukraine № 347 dated August 11, 2021]. Available at: https://zakon.rada.gov.ua/laws/show/347/2021#Text (accessed December 20, 2025)

11. Biryukov D.S., Kondratov S.I., Nasvit O.I., Sukhodolia O.M. (2015) *Zelena knyha z pytan' zakhystu krytychnoyi infrastruktury v Ukrayini: analitychna dopovid'* [Green Paper on Critical Infrastructure Protection in Ukraine: Analytical Report]. Kyiv: NISD, 35 p. (in Ukrainian)

12. Masliy O.A., Galushka R.M. (2025) Iyerarkhichnyy analiz ryzykiv i zahroz ekonomichniy bezpetsi Ukrayiny v umovakh voyennoho stanu [Hierarchical analysis of risks and threats to Ukraine's economic security under martial law]*. Economic Space*, vol. 198, pp. 69-75.

13. Onyshchenko S., Maslii O., Hlushko A. (2025) Digital and Economic Security of the State Under Global Threats. *Lecture Notes in Networks and Systems,* vol. 1338. pp. 580-602.

14. Mental Modeler software. Available at: https://www.mentalmodeler.com (accessed December 23, 2025).

Дата надходження статті: 06.12.2025
Дата прийняття статті: 17.12.2025
Дата публікації статті: 29.12.2025