

УДК 351:321

DOI: <https://doi.org/10.31470/2786-6246-2026-17-185-196>

Рябцев Геннадій, доктор наук з державного управління, професор, професор Києво-Могилянської школи врядування імені Андрія Мелешевича Національного університету «Києво-Могилянська академія»; головний науковий співробітник Національного інституту стратегічних досліджень

Riabtsev Gennadii, Doctor of Sciences in Public Administration, Professor, Professor of the Andriy Meleshevych at Kyiv-Mohyla School of Governance, National University «Kyiv-Mohyla Academy»; Chief Research Fellow at National Institute for Strategic Studies

ORCID ID: <https://orcid.org/0000-0002-3478-825X>

ВИКЛИК, УРАЗЛИВІСТЬ, РИЗИК, ЗАГРОЗА: СУТНІСТЬ І ВЗАЄМОЗВ'ЯЗОК

CHALLENGE, VULNERABILITY, RISK, THREAT: ESSENCE AND INTERCONNECTION

Анотація. Статтю присвячено подоланню проблеми недостатньої упорядкованості понятійно-категоріального апарату безпекових досліджень, зокрема у сфері забезпечення енергетичної безпеки України в умовах сучасного динамічного, високоризикового та невизначеного геополітичного середовища.

Виявлено стійку термінологічну невизначеність і фрагментарність підходів до трактування категорій «виклик», «ризик», «загроза». Практики їхнього використання класифіковано за трьома моделями: семантична конвергенція (вживання безієрархічної тріади «виклик – ризик – загроза» як взаємозамінних синонімів), змішування ризику й загрози як однорівневих категорій, а також надмірно розширене та інтегративне трактування загрози як універсальної категорії небезпеки. Така понятійна розмитість знижує методологічну цінність наукових розробок, викривляє результати моніторингу, погіршує якість стратегічного планування, обмежує дієвість владного реагування.

З метою подолання кризи термінології та на основі узагальнення кращих світових практик обґрунтовано необхідність впровадження уніфікованих ризик-орієнтованих (risk-informed) та стійкісно-орієнтованих (resilience-based) підходів. Їхнє застосування дозволить переорієнтувати увагу суб'єктів управління з подолання безпосередніх наслідків криз на аналізування довгострокових тенденцій розвитку, виявлення структурних уразливостей об'єктів безпеки, оцінювання можливих наслідків процесів та явищ і превентивне підвищення стійкості систем.

Запропоновано таке розмежування понять: виклик – сукупність обставин і структурних змін чи тенденцій середовища, які формують особливі вимоги до умов функціонування об'єкта, потребують адаптації або мобілізації ресурсів, але самі по собі ще не несуть загрози чи шкоди; ризик – обумовлена невизначеністю майбутнього імовірна категорія, яка відображає можливість настання небажаних наслідків і відхилень від стратегічних цілей унаслідок вказаних змін; загроза – детермінований, конкретизований чинник, процес або подія короточасної чи тривалої дії, що здатна безпосередньо завдати шкоди системі, порушивши її функціонування. Обґрунтовано, що загроза впливає на об'єкт управління через його уразливість – слабкі місця в системі захисту, – що призводить до конкретних, вимірюваних негативних наслідків і втрат.

Розроблено рекомендації Кабінету Міністрів та Міністерству енергетики України щодо гармонізації термінології й упровадження єдиних підходів до оцінювання безпекового середовища в рамках логічної моделі «виклик → уразливість → ризик → загроза → наслідки → заходи реагування».

Ключові слова: енергетична безпека, виклик, ризик, загроза, уразливість, ризик-орієнтований підхід, вироблення політики, стратегічне планування, управління змінами.

Abstract. The article is devoted to addressing the lack of systematization within the conceptual and categorical apparatus of security studies, particularly in ensuring Ukraine's energy security amid today's dynamic, high-risk, and uncertain geopolitical environment.

It identifies a persistent terminological ambiguity and fragmentation of approaches to interpreting the categories of "challenge," "risk," and "threat". The practices of their usage are classified into three models: semantic convergence (the use of a non-hierarchical triad of "challenge – risk – threat" as interchangeable synonyms), the conflation of risk and threat as single-level categories, and an overly broad, integrative interpretation of a threat as a universal category of danger. It is established that such conceptual fuzziness reduces the methodological value of scientific research, distorts monitoring results, undermines the quality of strategic planning, and limits the effectiveness of public authorities' response measures.

To resolve this terminological crisis and based on a synthesis of world best practices, the necessity of implementing a unified risk-informed and resilience-based approach is substantiated. Their systematic application enables management entities to shift their focus from merely addressing the immediate consequences of crises to a deeper analysis of long-term environmental trends, identifying the structural vulnerabilities of security objects, assessing the potential consequences of processes and phenomena, and proactively enhancing system resilience.

The following differentiation of concepts is proposed: challenge – a set of circumstances and structural changes or environmental trends that form special requirements for the object's operating conditions, requiring adaptation or resource mobilization, but do not inherently carry an immediate threat or harm; risk – a probabilistic category driven by future uncertainty, reflecting the likelihood of undesirable consequences and deviations from strategic goals resulting from the specified changes; threat – a deterministic, specified factor, process, or event of short-term or long-term action capable of directly causing harm to a system by disrupting its functioning. It is substantiated that a threat affects a management object through its vulnerability – a weak point in the defence system – which ultimately leads to specific, measurable negative consequences and losses.

Recommendations have been developed for the Cabinet of Ministers and the Ministry of Energy of Ukraine to harmonize terminology and implement unified approaches to assessing the security environment within the framework of the logical model: "challenge → vulnerability → risk → threat → consequences → response measures".

Keywords: energy security, challenge, risk, threat, vulnerability, risk-informed approach, policy-making, strategic planning, change management.

Постановка проблеми. Сучасне безпекове середовище характеризується високою динамічністю, зростанням рівня невизначеності та появою нових чинників впливу. За таких умов особливого значення набуває не лише своєчасне виявлення негативних тенденцій і факторів дестабілізації, а й формування адекватного понятійно-категоріального апарату, який дозволяє коректно ідентифікувати, класифікувати та оцінювати відповідні явища.

У наукових дослідженнях, нормативно-правових актах, стратегічних документах і аналітичних матеріалах органів державної влади значне поширення набули поняття «виклик», «ризик» і «загроза». Їх активно використовують під час аналізування безпекового середовища, оцінювання рівня безпеки, розроблення стратегій розвитку та проектування владних рішень. Однак відсутність єдиного підходу до трактування зазначених категорій нерідко призводить до їхнього змішування чи

ототожнення, що негативно позначається на якості наукових досліджень і практиці державного управління.

Для України методологічне впорядкування понять «виклик», «ризик», «загроза» має не лише теоретичне, а й прикладне значення. Від коректності трактування цих категорій залежить якість стратегічного планування, формування системи безпекового моніторингу, визначення пріоритетів політики, розроблення сценаріїв реагування на кризові ситуації та оцінювання результативності заходів із підвищення стійкості складних систем.

У зв'язку з цим виникає потреба в критичному аналізі наявних підходів до визначення зазначених категорій, виявленні їхніх спільних і відмінних ознак, а також формуванні узгодженого понятійного апарату, придатного для використання у сфері дослідження й забезпечення енергетичної безпеки. Саме це зумовлює актуальність теми та визначає її наукову й практичну значущість.

Аналіз останніх досліджень і публікацій [1–9; 11; 12; 16–22] свідчить, що вітчизняні та іноземні науковці по-різному визначають зміст понять «виклик», «ризик», «загроза», а також характер взаємозв'язків між ними. У частині публікацій ці категорії вважають взаємопов'язаними, але самостійними поняттями, що відображають різні стадії розвитку переважно негативних процесів, дій та явищ. В інших – їх розглядають як близькі за змістом або навіть взаємозамінні терміни. Така ситуація характерна не лише для українського наукового простору, а й для іноземних досліджень у сфері безпеки, політики, ризик-менеджменту та стратегічного планування [13–14; 23].

Особливої актуальності проблема набуває у сфері енергетичної безпеки. Сучасні енергетичні системи функціонують за одночасного впливу великої кількості технологічних, економічних, екологічних, соціальних, військових і геополітичних чинників. До традиційних загроз енергопостачанню додаються виклики енергетичного переходу, декарбонізації, цифровізації енергетики, розвитку розподіленої генерації, інтеграції відновлюваних джерел енергії. За таких умов результативність та ефективність суспільної політики значною мірою визначаються здатністю своєчасно розмежовувати зміни середовища, потенційні небезпеки та реальні чинники дестабілізації.

Основним пріоритетом у цій сфері є створення системи гарантування енергетичної безпеки, зокрема в частині формування реєстру, ідентифікування та аналізування наявних загроз для встановлення цілей і завдань суб'єктам гарантування безпеки й визначення заходів пріоритетного реагування [24–26].

Важливим є й те, що провідні міжнародні організації, зокрема Міжнародне енергетичне агентство, Європейська комісія, Міжнародне агентство з атомної енергії, дедалі ширше використовують ризик-орієнтовані підходи до аналізування безпеки енергетичних систем [13–14; 23]. У межах таких підходів увага зосереджується не лише на безпосередніх загрозах, а й на тенденціях розвитку середовища, уразливостях систем та окремих об'єктів, можливих наслідках реалізації небезпечних подій, а також на заходах із підвищення стійкості. Попри відмінності в термінології, відповідні підходи ґрунтуються на необхідності чіткого розмежування джерел небезпеки, ризиків, загроз і наслідків їхньої реалізації.

Метою статті є виявлення особливостей використання понять «виклик», «ризик», «загроза» у фаховій літературі та обґрунтування ієрархічної моделі взаємозв'язку зазначених категорій для потреб дослідження й забезпечення енергетичної безпеки України.

Для досягнення поставленої мети визначено такі завдання:

- класифікувати сучасні наукові підходи до визначення понять «виклик», «ризик», «загроза», наведені у вітчизняних та зарубіжних фахових публікаціях;
- виявити спільні та відмінні ознаки зазначених категорій, встановити особливості їхньої інтерпретації в сучасних безпекових дослідженнях;
- оцінити вплив термінологічної невизначеності на методологію дослідження та оцінювання стану енергетичної безпеки;

- обґрунтувати авторський підхід до розмежування понять «виклик», «ризик», «загроза» та сформулювати ієрархічну модель їхнього взаємозв'язку для використання в дослідженнях енергетичної безпеки України.

Наукова новизна дослідження полягає в уточненні змісту та співвідношення понять «виклик», «ризик» і «загроза» на основі поєднання аналізу наукових дефініцій та контент-аналізу сучасних термінологічних практик, а також в обґрунтуванні ієрархічної моделі «виклик → ризик → загроза» як методологічної основи дослідження енергетичної безпеки.

Виклад основного матеріалу. Категорії «виклик», «ризик», «загроза» в україномовних працях. Сучасні безпекові дослідження демонструють наявність термінологічної невизначеності у трактуванні категорій «виклик», «ризик», «загроза» вітчизняними науковцями. Попри активізацію дискусії з 2022 р., фрагментарність підходів до визначення зазначених категорій зберігається. Це ускладнює формування єдиної методологічної основи для досліджень.

Для уточнення характеру застосування відповідних термінів проведено контент-аналіз публікацій, що дозволив виявити термінологічні моделі без інтерпретації авторських визначень. Методологічно він базувався на ідентифікації контексту використання термінів, що дозволяє встановити ступінь їхньої диференціації або, навпаки, зближення.

Аналіз праць [1–9] свідчить, що значна частина авторів використовує терміни «виклик», «ризик», «загроза» як взаємозамінні або такі, що належать до одного семантичного поля без чіткого ієрархічного розмежування (табл. 1).

Таблиця 1

Узагальнені результати контент-аналізу публікацій [1–9]

Автори і джерело	Терміни в тексті	Аналітичний ефект
М. Диха [1]	«виклики та загрози виробничій безпеці»	виклики й загрози – єдина категорія без розмежування
М. Роговець, В. Євдокимов [2]	«виклики, ризики та загрози державній безпеці»	виклики, ризики й загрози – синонімічний ряд
В. Базиченко [3]	«загрози та виклики державному управлінню»	часткове ототожнення: виклик – загроза
О. Маслій, А. Максименко [4]	«ризики та загрози економічній безпеці»	ризик і загроза – однорівневі явища
І. Босак [5]	«загрози інформаційній безпеці»	загроза охоплює ризики, виклики й наслідки
О. Пархоменко-Куцевіл [6]	«сучасні виклики національній безпеці»	виклик – узагальнена форма загрози
В. Бобиль та ін. [7]	«ризики та джерела загроз»	ризик – джерело або передумова загрози
С. Онищенко, А. Глушко [8]	«виклики та загрози кібербезпеці»	виклики й загрози – перехресні категорії
А. Найчук, В. Маркітанов [9]	«загрози державним інтересам» (у контексті викликів)	виклики включають до категорії загроз

Джерело: узагальнено автором.

Зокрема, у працях з національної безпеки трапляється одночасне вживання конструкції «виклики та загрози», де обидві категорії не розмежовуються за рівнем імовірності, джерелом походження чи характером впливу [9]. Схожий підхід спостерігається і в дослідженнях державного управління, де зустрічаються конструкції типу «виклики, ризики та загрози державній безпеці» [2], що свідчить про їхнє семантичне групування в межах єдиного проблемного поля. У праці [5] «виклики сучасності» фактично ототожнюють із загрозами без додаткової диференціації. Така ж практика спостерігається у дослідженнях кібернетичної безпеки, де зазначені категорії іноді використовують як однорідні чинники впливу [8].

Особливістю аналізованих праць є використання тріади «виклики – ризики – загрози» як узагальненого переліку без встановлення логічних зв'язків між її елементами [3; 10]. Як наслідок, ці категорії виконують радше описову, ніж аналітичну функцію, що знижує методологічну цінність досліджень.

Окремою проблемою є змішування категорій «ризик» і «загроза». Їх розглядають як однорівневі явища, що негативно впливають на стан безпеки держави або окремих її підсистем [2;

4; 7]. Показовим у цьому плані є трактування загроз інформаційній безпеці, де під «загрозою» одночасно розуміють сукупність умов, факторів і потенційних дій, що можуть призвести до порушення безпеки [5]. Така інтерпретація охоплює як ризикові ситуації, так і вже сформовані небезпечні впливи, розмиваючи межу між імовірнісною природою ризику й більш детермінованим характером загрози.

У частині публікацій виявлено тенденцію до семантичного зближення понять «виклик» і «загроза». Термін «виклик» часто використовують як позначення широкого спектра зовнішніх впливів, які одночасно інтерпретують як загрози для системи [3; 6; 9]. Таким чином, виклик втрачає функцію початкової стадії трансформаційного процесу. Відбувається його концептуальне розширення до рівня загрози, а розмежування між потенційним і актуалізованим впливом не фіксується.

У низці досліджень поняття «виклик» набуває надмірно широкого значення і використовується для позначення будь-яких змін зовнішнього середовища, включно з тими, що мають ознаки ризиків або загроз. Це призводить до концептуального розширення поняття та втрати його аналітичної специфіки як терміна для опису початкового рівня трансформаційних процесів.

Частина дослідників використовує категорію «загроза» як інтегративне поняття, що охоплює ризики, виклики та потенційні негативні наслідки [5]. Такий підхід призводить до фактичного перетворення терміна «загроза» на універсальну категорію для опису небезпеки.

Таким чином, можна виокремити три моделі термінологічних практик: семантичну конвергенцію, за якої одночасно використовують безієрархічну тріаду «виклик – ризик – загроза» [2; 8]; змішування ризику й загрози як однорівневих категорій [4; 7]; розширене трактування загрози з включенням до неї ризику й виклику [5].

Причини такої термінологічної невизначеності мають комплексний характер. По-перше, у багатьох дослідженнях домінує описово-емпіричний підхід, який не передбачає формалізації категоріального апарату. По-друге, спостерігається вплив законотворчої практики, дієвці якої часто використовують узагальнені позаструктурні формулювання. По-третє, відсутність узгодженої міждисциплінарної термінології призводить до того, що ту саму категорію інтерпретують по-різному в межах державного управління, політології, економіки, права та забезпечення безпеки.

Подолання цієї проблеми потребує впровадження уніфікованого ризик-орієнтованого (risk-informed) підходу [10], в межах якого: виклик розглядають як зміну середовища функціонування системи; ризик – як імовірність настання негативних наслідків цієї зміни; загрозу – як конкретизований чинник або подію, здатні завдати шкоди об'єктові управління (безпеки).

Зміни в підходах до визначення категорій «виклик», «ризик», «загроза». Сучасні дослідження у сфері безпеки складних систем характеризуються посиленням уваги до концептуального розмежування понять «виклик» (challenge), «ризик» (risk) і «загроза» (threat). У працях 2022–2026 рр. спостерігається поступовий перехід від суб'єктивних авторських до інтегрованих ризик-орієнтованих (risk-informed) та стійкісно-орієнтованих (resilience-based) підходів, що поєднують аналіз невизначеностей, уразливостей і наслідків розвитку подій у рамках єдиного процесу оцінювання стану системи.

«Виклик» переважно інтерпретують як чинник або сукупність умов середовища, що зумовлюють необхідність адаптації системи, але не містять безпосереднього негативного впливу. У психологічних та організаційних дослідженнях його розглядають як елемент середовища, що сприяє мобілізації ресурсів і підвищенню ефективності діяльності [11]. У теорії безпеки виклики трактують як процеси й тенденції, що сигналізують про потенційні зміни без негайної шкоди [12]. У вітчизняних дослідженнях виклик також вивчають як сигнал про необхідність змін у механізмах управління або розвитку системи.

У Міжнародному енергетичному агентстві (MEA, International Energy Agency – IEA) розглядають виклики енергетичного переходу як структурні трансформації (декарбонізація, електрифікація, цифровізація), що змінюють контекст функціонування енергосистем, але не є загрозами як такими [13; 14]. Схожа логіка спостерігається й у документах Європейського Союзу [15].

Поняття ризику в сучасних дослідженнях є найбільш методологічно розвиненим і уніфікованим. Більшість авторів пов'язує ризик із невизначеністю майбутніх подій і можливістю виникнення наслідків, що впливатимуть на досягнення поставлених цілей. У класичному трактуванні [16], ризик визначають як поєднання подій, їхніх наслідків і невизначеності. У подальших дослідженнях його розглядають як потенційне відхилення фактичних результатів діяльності від очікуваних унаслідок дії складно прогнозованих чинників [17; 24]. Водночас низка авторів наголошує на двокомпонентній природі ризику, яка поєднує ймовірність настання події та масштаб її наслідків [26]. Таким чином, на відміну від виклику, ризик уже передбачає можливість негативного розвитку подій, однак ще не свідчить про неминучість заподіяння шкоди.

Методологічно важливими є підходи, що трактують ризик як епістемічну категорію, залежну від рівня знань про систему [18]. Ризик пов'язують також із потенціалом катастрофічних подій і масштабом їхніх наслідків [19]. У сфері кібернетичної безпеки ризик аналізують як результат взаємодії невизначеності та загроз у складних системах [20]. У звітах МЕА [13; 14] ризик визначено як ймовірність порушення енергопостачання під впливом геополітичних, технологічних і кліматичних факторів, а енергетичну безпеку – як здатність системи витримувати шоки й відновлювати функціонування.

Категорія загрози має більш детермінований характер. У соціально-психологічних дослідженнях її визначають як потенційну шкоду для цінностей або ресурсів [21], у менеджменті та організаційних науках – як подію або умову, здатну завдати шкоди організації [22], у теорії безпеки – як конкретизовану можливість завдання шкоди життєво важливим інтересам [12].

У документах Міжнародного агентства з атомної енергії (МАГАТЕ, International Atomic Energy Agency – IAEA) загрозу формалізують через оцінювання (threat assessment), використовуючи модель «небезпечний чинник (hazard) → уразливість (vulnerability) → ризик (risk) → загроза (threat) → наслідок (consequence)», яка поєднує аналізування її складових в єдину систему прийняття рішень (risk-informed decision-making) [23]. При цьому ризик визначають як поєднання ймовірності події та її наслідків, а загрозу – як потенційний чинник, здатний реалізувати небажаний сценарій.

В енергетичній політиці ЄС ризик-орієнтований підхід реалізовано через оцінювання готовності до криз, зокрема в електроенергетиці [15]. Використовується концепція «виклики (challenges) → уразливості (vulnerabilities) → ризики (risks) → загрози (threats) → [заходи реагування] → безпека постачання (security of supply)». Наприклад, зростання частки відновлюваних джерел енергії в енергетичному балансі розглядають як виклик для енергосистеми; недостатню гнучкість мережі – як її уразливість; можливість дефіциту потужності – як ризик; реальне порушення постачання електроенергії – як загрозу енергетичній безпеці.

У документах МЕА поняття «енергетична безпека» (energy security) визначають як здатність енергетичної системи протистояти ризикам і шокам. Найчастіше використовують послідовність «довгострокові тенденції та виклики (energy transition, electrification, critical minerals dependence) → уразливості (vulnerabilities) → ризики постачання (supply risks) → загрози безпеці (security threats) → інструменти забезпечення стійкості (resilience)» [13; 14]. Наприклад, у дослідженнях щодо енергетичного переходу МЕА розглядає декарбонізацію не як загрозу, а як виклик, який породжує ризики порушення енергопостачання лише в разі неналежного управління.

Порівняльний аналіз наведених вище визначень дозволяє дійти висновку, що категорії «виклик», «ризик», «загроза» описують різні стадії розвитку небажаних або потенційно небажаних процесів у системі. Водночас вони мають спільну методологічну основу, пов'язану з невизначеністю майбутнього стану об'єкта та потребою владного реагування на зміни середовища (табл. 2).

Таблиця 2

Спільні й відмінні риси категорій «виклик», «ризик» і «загроза»

Ознака	Опис для категорії		
	«виклик»	«ризик»	«загроза»
Спільне			
Зв'язок із майбутнім станом системи	стосується подій, процесів, тенденцій, наслідки яких можуть проявитися в майбутньому		
Наявність невизначеності	виникають в умовах неповної визначеності щодо напрямів розвитку подій та їхніх наслідків		
Потреба в реагуванні	вимагають дій із боку суб'єкта управління		
Вплив на досягнення цілей	здатні змінити умови функціонування системи, вплинути на реалізацію її інтересів або стратегічних цілей		
Системність	є елементами гарантування безпеки та стійкості складних систем		
Відмінне			
Характер впливу	переважно нейтральний	невизначений	переважно негативний
Наявність шкоди	неочевидна	можлива	імовірна, очікувана
Визначеність наслідків	найнижча	недостатня	найвища
Можливість використання на користь розвитку	висока	часткова	майже відсутня
Реагування	адаптація	управління ризиком	нейтралізація

Джерело: розроблено автором.

Таким чином, сучасні дослідження демонструють перехід від наявних в українському науковому полі авторських суб'єктивних підходів [1–9] до інтегрованих моделей, в рамках яких виклики, ризики й загрози розглядають у вигляді ланцюга «виклик → уразливість → ризик → загроза → наслідки → заходи реагування».

Виклики, загрози, ризики у сфері енергетичної безпеки. У контексті енергетичної безпеки аналізовані поняття доцільно розглядати як ієрархічно пов'язані категорії:

- виклик відображає зміни енергетичного середовища, що потребують адаптації сектору. Ним може бути нова тенденція або зміна умов функціонування енергетичної системи, наприклад масове впровадження розподіленої генерації;
- ризик характеризує ймовірність недосагнення цілей енергетичної політики під впливом цих змін (наприклад, зростання нестабільності режимів роботи електричних мереж);
- загроза означає реальну можливість зменшення надійності, стійкості, доступності, безпечності енергопостачання, завдання шкоди енергетичній системі або порушення її функціонування (наприклад, аварійне вимкнення споживачів і, як наслідок, економічні збитки та зниження рівня енергетичної безпеки).

Науковці Національного інституту стратегічних досліджень пропонують використовувати ці терміни у взаємному зв'язку [24–26].

У загальному розумінні виклик (challenge) – це сукупність зовнішніх або внутрішніх чинників, тенденцій чи обставин, які змінюють умови функціонування системи та потребують адаптації, мобілізації ресурсів або прийняття нових рішень, але самі по собі ще не створюють безпосередньої небезпеки її існуванню чи розвитку.

Якщо стисло, виклик є сукупністю обставин, що формують особливі вимоги до умов функціонування об'єкта управління. Наприклад, викликом для України є здійснення енергетичного переходу (energy transition), орієнтованого на масштабне використання розподіленої генерації, інтелектуалізацію інфраструктури, формування децентралізованих висококонкурентних енергетичних ринків.

За своїми ключовими ознаками виклик: сигналізує про необхідність змін; може мати як негативні, так і позитивні наслідки; не передбачає обов'язкового завдання шкоди.

Реагування суб'єктів управління на виклик або бездіяльність стосовно нього може мати як позитивні, так і негативні результати, наприклад, призвести до появи та/або загострення загроз безпеці.

Виходячи з цього, виклик безпеці – сукупність обставин і чинників, що формують особливі вимоги до умов функціонування й розвитку об'єкта управління, і потенційно здатні призвести до появи загроз його безпеці [24].

У загальному розумінні, загроза (threat, risk source) – це сукупність чинників, процесів або дій, здатних завдати шкоди життєво важливим інтересам, ресурсам, функціям чи цілям системи та можуть спричинити негативні наслідки у разі їхньої реалізації. При цьому процеси, що є втіленням загрози, можуть відбуватися стихійно, внаслідок цілеспрямованих дій (зокрема зловмисних) або необґрунтованої бездіяльності суб'єкта управління.

За своїми ключовими ознаками загроза має чітко виражений негативний характер; пов'язана з можливістю заподіяння шкоди; характеризується відносно високим рівнем визначеності негативних наслідків; потребує заходів запобігання, мінімізації або нейтралізації.

Якщо загроза в разі її реалізації здатна негативно вплинути відразу на декілька держав та/чи галузей економіки впродовж 5...10 років (long-term), її вважають надсистемною (глобальною). Прикладами таких загроз є екстремальні погодні явища, техногенні аварії, епідемії та пандемії. Загрозу, яка в разі її реалізації здатна негативно впливати на об'єкт управління до одного року, вважають короточасною (short-term), а до п'яти років – тривалою (medium-term).

Якщо загроза виникла в неконтрольованій суб'єктом управління сфері, її вважають зовнішньою щодо системи (об'єкта управління). Наприклад, блокада іншими країнами постачання товарів стратегічного імпорту (ядерного палива чи нафти й нафтопродуктів).

Якщо загроза стала наслідком дій чи необґрунтованої бездіяльності суб'єкта управління, її вважають внутрішньою щодо системи (об'єкта управління). Наприклад, недотримання норм обслуговування захисної дамби водосховища становить загрозу її здатності забезпечувати низовини від затоплення.

У рамках системного підходу [24] будь-який об'єкт (підсистема) нижчого рівня та його складові (елементи та зв'язки, функції й ролі, процеси й матеріал) можуть, унаслідок непроєктного функціонування, стати джерелом загроз для об'єкта вищого рівня та його складових. Утім, для об'єкта вищого рівня такі загрози є внутрішніми. Водночас функціонуванню такого об'єкта можуть завадити й зовнішні (для нього) загрози, джерелом яких є система (об'єкт) ще більш високого рівня.

У застосуванні до предмета енергетичної безпеки такими підсистемами, що послідовно розширюються є ресурсна (і технологічна) достатність, економічна доступність, економічна (та енергетична) ефективність, екологічна (і соціальна) прийнятність, енергетична стійкість, захищеність національних інтересів (в енергетиці) [24].

Виходячи з цього, загрози енергетичній безпеці – короточасні або тривалі, реальні або потенційні обставини, явища, чинники або події, що можуть порушити безпеку та стійкість функціонування енергетичного сектору країни, обмежити або порушити енергозабезпечення споживачів, призвести до аварій та інших негативних наслідків [24; 25].

Загроза впливає на об'єкт управління (систему) через його уразливість (vulnerability) – чутливість об'єкта управління до впливів, слабкі місця в його захисті від загроз, відсутність «запобіжників» від них. Наприклад, для об'єкта «захисна дамба водосховища» загроза «недотримання норм обслуговування», що може спричинити порушення сталості захисної дамби (деградація опірних спроможностей), реалізується через уразливість «відсутність системи контролю за дотриманням норм обслуговування захисної дамби».

Якщо об'єкт є уразливим до впливів, реалізація загрози, зазвичай, призводить до негативних наслідків.

Наслідок (consequence, impact) – результат впливу загрози на цілі функціонування об'єкта управління. Його можна виміряти, оцінивши втрати від такого впливу, зокрема: заподіяння фізичної шкоди; майнових чи грошових збитків; погіршення рівня енергоефективності ВВП; зростання вартості витрат що йде на оплату житлово-комунальних послуг тощо. Наприклад, для об'єкта «захисна дамба водосховища» наслідком впливу загрози «недотримання норм обслуговування» є «порушення сталості захисної дамби (деградація опірної спроможності)», яке може бути виражено

або через оцінку втрат, спричинених руйнуванням дамби, або у відсотках зменшення опірності порівняно з проектним рівнем.

Утім, загроза реалізується не завжди, об'єкти управління вразливі не до всіх загроз, і не всі загрози призводять до негативних наслідків (зокрема, через застосування заходів із запобігання реалізації загроз). Відповідну ймовірність наслідків впливу загрози визначають, оцінюючи ризики.

У загальному розумінні ризик (risk) – це обумовлена невизначеністю можливість виникнення події або сукупності подій, які можуть негативно вплинути на досягнення цілей системи, причому ступінь такого впливу визначається ймовірністю настання події та масштабом її негативних наслідків. Якщо стисло, ризик відображає вплив невизначеностей на цілі об'єкта управління.

За своїми ключовими ознаками ризик характеризується невизначеністю; має ймовірнісний характер; поєднує ймовірність і наслідки; може бути оцінений якісно або кількісно.

За потреби кількісної оцінки ризик подають у вигляді $R = LC$, де L – загальна ймовірність реалізації конкретної загрози; C – сукупний негативний наслідок реалізації загрози (consequence), результат уразливого впливу на об'єкт управління.

Ризик є тим більшим, чим вища ймовірність реалізації загрози й більші спричинені нею наслідки. Таким чином, за величиною ризику можна визначати рівень загрози, щоб встановити значущість її впливу на цілі об'єкта управління, і ранжувати загрози за цією значущістю.

З урахуванням викладеного вище, ризик у сфері енергетичної безпеки – це можливість переростання викликів енергетичній безпеці у загрози, реалізації загроз енергетичній безпеці й настання інших обставин, здатних негативно вплинути на стан енергетичної безпеки [24; 25].

Мета управління ризиком полягає в його визначенні й установленні того, яка величина ризику є прийнятною для суб'єкта управління.

Систематичне оцінювання ризиків дозволить:

- розробляти заходи, спрямовані на підвищення рівня національної безпеки та/чи нейтралізації загроз;
- порівнювати рівні загроз у різні періоди часу для визначення тенденцій і наближеності поточного рівня енергетичної безпеки до цільового, оцінювання впливу дестабілізуючих чинників, результатів й наслідків вжитих заходів;
- вибирати владні рішення, найкращі з точки зору гарантування енергетичної безпеки;
- прогнозувати стан енергетичної безпеки за різних сценаріїв розвитку паливно-енергетичного комплексу й національної економіки в цілому;
- вибирати варіанти розвитку держави з урахуванням забезпечення енергетичної безпеки.

Описане вище розмежування категорій «виклик», «уразливість», «ризик», «загроза», «наслідки» [24–26] узгоджується із сучасними підходами, які застосовуються в документах Європейської Комісії, МАГАТЕ та МЕА для аналізування безпеки енергетичних систем [13–15; 23], хоча зазначені організації не користуються єдиною ієрархією цих категорій. Попри це, всі вони застосовують близький за логікою ризик-орієнтований підхід [10], згідно з яким ідентифікують, визначають, аналізують та оцінюють:

- зміни середовища функціонування енергетичної системи (drivers, trends, emerging challenges);
- уразливості систем і мереж (vulnerabilities);
- ризики досягнення цілей енергетичної політики (risks);
- конкретні загрози надійності й безпеці постачання (threats, disruptions);
- наслідки реалізації загроз (impacts, consequences);
- заходи з метою забезпечення стійкості (resilience measures).

Висновки. Критичний аналіз сучасних наукових підходів до визначення понять «виклик», «ризик» і «загроза» дозволив виявити такі особливості їхнього використання: відсутність загальноприйнятого трактування зазначених понять; часте використання категорій як синонімічних або близьких за змістом; недостатнє розмежування між потенційними та актуалізованими формами небезпеки; переважання описового над аналітичним підходом; відсутність усталеної ієрархії між

викликами, ризиками та загрозами; залежність змісту понять від предметної сфери дослідження (державне управління; менеджмент; національна, інформаційна, енергетична безпека).

Попри спільну належність до категоріального апарату безпекових досліджень, поняття «виклик», «ризик», «загроза» відображають різні аспекти взаємодії об'єкта безпеки із зовнішнім і внутрішнім середовищем. Спільною ознакою всіх трьох категорій є їхній зв'язок із можливістю негативного впливу на стан і функціонування системи, тоді як відмінності полягають у ступені визначеності, характері впливу та рівні актуалізації небезпеки.

Виявлено домінування нормативно-описового підходу в застосуванні зазначених категорій. Установлено, що їх використовують без належного методологічного розмежування, що проявляється у формі семантичної конвергенції, змішуванні ризиків і загроз або розширеному трактуванні загроз як універсальної категорії небезпеки.

Термінологічна невизначеність негативно впливає на методологію дослідження та оцінювання безпеки, ускладнює побудову моделей прогнозування, розроблення сценаріїв розвитку та визначення пріоритетів політики. Відсутність чіткого розмежування між викликами, ризиками, загрозами знижує аналітичну цінність досліджень та обмежує можливості застосування ризик-орієнтованих підходів у сфері управління безпекою.

Згідно з авторським розмежуванням досліджуваних категорій: виклик розглядають як сукупність змін або тенденцій у середовищі, що потребують реагування з боку об'єкта управління; ризик – як імовірність виникнення небажаних наслідків у разі реалізації таких викликів; загрозу – як сукупність чинників, процесів або дій, здатних завдати шкоди життєво важливим інтересам, функціонуванню чи розвитку відповідної системи.

Ієрархічну модель «виклик → ризик → загроза», що відображає логіку ескалації небезпечних процесів, рекомендовано використати як методологічну основу для безпекових досліджень.

У зв'язку з цим Кабінету Міністрів України доцільно ініціювати уніфікацію понятійного апарату у сфері безпеки шляхом гармонізації термінології, що використовується у стратегічних документах, державних програмах, методиках оцінювання безпеки.

Міністерству енергетики України рекомендовано впровадити розмежування категорій «виклик», «ризик» і «загроза» під час підготовки документів прогнозного та програмного спрямування, а також під час формування системи моніторингу енергетичної безпеки.

У процесі оновлення стратегічних документів у сфері енергетичної безпеки доцільно передбачити впровадження єдиної методології аналізу безпекового середовища, яка забезпечуватиме послідовний перехід від виявлення викликів до оцінювання ризиків і визначення загроз, що сприятиме підвищенню обґрунтованості владних рішень та стійкості енергетики України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Диха М.В. Виклики та загрози виробничій безпеці підприємств нафтогазового комплексу України у системі забезпечення їх економічної безпеки. *Київський економічний науковий журнал*. 2026. № 12. С. 42–50. DOI: <https://doi.org/10.32782/2786-765X/2026-12-6>.
2. Роговець М., Євдокимов В. Модель управління викликами, ризиками та загрозами державній безпеці України. *Society and Security*. 2026. № 1 (13). С. 52–59. DOI: [https://doi.org/10.26642/sas-2026-1\(13\)-52-59](https://doi.org/10.26642/sas-2026-1(13)-52-59).
3. Базиченко В.В. Загрози та виклики державному управлінню в сфері національної безпеки України в умовах глобальних та регіональних викликів. *Вісник Херсонського національного технічного університету*. 2025. № 2 (93), Ч. 1. С. 344–348. DOI: <https://doi.org/10.35546/kntu2078-4481.2025.2.1.46>.
4. Маслій О.А., Максименко А.П. Ризики та загрози економічній безпеці України у цифровій сфері в умовах війни. *Ринкова економіка: сучасна теорія і практика управління*. 2022. Т. 21, № 3 (52). С. 179–199. DOI: [https://doi.org/10.18524/2413-9998.2022.3\(52\).275802](https://doi.org/10.18524/2413-9998.2022.3(52).275802).
5. Босак І.М. Інформаційна безпека України: загрози та методи протидії. *Київський економічний науковий журнал*. 2025. № 9. С. 33–39. DOI: <https://doi.org/10.32782/2786-765X/2025-9-4>.
6. Пархоменко-Куцевіл О.І. Сучасні виклики національній безпеці України в умовах цифрових викликів: державно-управлінський аспект. *Публічне управління: концепції, парадигма, розвиток, удосконалення*. 2025. № 12. С. 116–123. DOI: <https://doi.org/10.31470/2786-6246-2025-12-116-123>.
7. Бобиль В.В., Лоскутова Г.А., Дронь М.А. Ризики та джерела загроз зовнішньоекономічній безпеці України. *Review of Transport Economics and Management*. 2022. № 8 (24). С. 12–19. DOI: <https://doi.org/10.15802/rtem2022/257978>.
8. Онищенко С.В., Глушко А.А. Аналітичний вимір кібербезпеки України в умовах зростання викликів та загроз. *Економіка і регіон*. 2022. Т. 1, № 84. С. 13–20. URL: <https://journals.nupp.edu.ua/eir/article/view/2540> (дата звернення: 15.06.2026).

9. Найчук А.В., Маркітантов В.Ю. Ключові фактори ескалації безпекової ситуації в Східній Європі та загрози державним інтересам України. *Політологічний вісник*. 2022. № 88. С. 175–188. DOI: <https://doi.org/10.17721/2415-881x.2022.88.175-188>.
10. ISO 31000. Risk management. URL: <https://www.iso.org/iso-31000-risk-management.html> (дата звернення: 15.06.2026).
11. Fernandez de Henestrosa M., Sischka P. E., Steffgen G. Examining the challenge-hindrance-threat distinction of job demands alongside job resources. *Frontiers in Psychology*. 2023. Vol. 14. P. 1011815. DOI: <https://doi.org/10.3389/fpsyg.2023.1011815>.
12. Bojanić D. Theoretical and methodological analysis of challenges, risks and threats. *Vojno delo*. 2022. Vol. 74 (2). P. 1–17. DOI: <https://doi.org/10.5937/vojdelo2202001B>.
13. Securing Clean Energy Technology Supply Chains. Paris: IEA, 2022. DOI: <https://doi.org/10.1787/be931bdc-en>.
14. Climate Resilience for Energy Security. Paris: IEA, 2022. DOI: <https://doi.org/10.1787/2a931f53-en>.
15. Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC. URL: <https://eur-lex.europa.eu/eli/reg/2019/941/oj/eng> (дата звернення: 15.06.2026).
16. Aven T. Is the definition of risk still contested? *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*. 2023. Vol. 237, Issue 1. P. 3. DOI: <https://doi.org/10.1177/1748006X221125865>.
17. Xu Y., Reniers G., Yang M. A. Multidisciplinary Review into the Evolution of Risk Concepts and Their Assessment Methods. *Processes*. 2024. Vol. 12. P. 2449. DOI: <https://doi.org/10.3390/pr12112449>.
18. Zanotti G., Chiffi D., Schiaffonati V. AI-Related Risk: An Epistemological Approach. *Philosophy & Technology*. 2024. Vol. 37, Issue 66. DOI: <https://doi.org/10.1007/s13347-024-00755-7>.
19. Geiger G. Catastrophic risk: indication, quantitative assessment and management of rare extreme events using a non-expected utility framework. *Annals of Operations Research*. 2024. Vol. 343. P. 223–261. DOI: <https://doi.org/10.1007/s10479-024-06259-z>.
20. Dekker M., Alevizos L. A threat-intelligence driven methodology to incorporate uncertainty in cyber risk analysis and enhance decision-making. *Security and Privacy*. 2024. Vol. 7, Issue 1. e333. DOI: <https://doi.org/10.1002/spy2.333>.
21. Martínez C. A., Van Prooijen J., Van Lange P. A. A threat-based hate model: How symbolic and realistic threats underlie hate and aggression. *Journal of Experimental Social Psychology*. 2022. Vol. 103. P. 104393. DOI: <https://doi.org/10.1016/j.jesp.2022.104393>.
22. Connelly B., Shi W. Threats and responses in organizational research. *Journal of Management*. 2022. Vol. 48, Issue 6. P. 1366–1381. DOI: <https://doi.org/10.1177/01492063221080431>.
23. Risk informed approach for nuclear security measures for nuclear and other radioactive material out of regulatory control : implementing guide. *Nuclear Security Series*. No. 24-G. Vienna: International Atomic Energy Agency, 2015. 69 p. URL: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1678_web.pdf (дата звернення: 15.06.2026).
24. Енергетична безпека України: перспективна модель управління ризиками: монографія / [О.М. Суходоля, Ю.М. Харазішвілі, Г.Л. Рябцев]; за ред. О.М. Суходолі. Київ: НІСД, 2023. 152 с. DOI: <https://doi.org/10.53679/NISS-book.2023.01>.
25. Визначення рівня та оцінювання загроз енергетичній безпеці: зб. аналіт. доп. / [О.М. Суходоля, Г.Л. Рябцев, Ю.М. Харазішвілі та ін.]. Київ: НІСД, 2022. 160 с. DOI: <https://doi.org/10.53679/NISS-analytrep.2022.13>.
26. Enhancing Security in Sustainable Energy Systems for Central European Business: An Adaptive Response Methodology under National Economy / Y. Kharazishvili, O. Sukhodolia, G. Riabtsev, et al. *Central European Business Review*. 2025. Vol. 14 (4). P. 25–63. DOI: <https://doi.org/10.18267/j.cebr.396>.

REFERENCES

1. Dykha, M.V. (2026). Vykylyky ta zahrozy vyrobnychii bezpetsi pidpriemstv naftohazovoho kompleksu Ukrainy u systemi zabezpechennia yikh ekonomichnoi bezpeky [Challenges and threats to the production security of oil and gas enterprises of Ukraine in the system of ensuring their economic security]. *Kyivskyi ekonomichnyi naukovi zhurnal – Kyiv Economic Scientific Journal*, (12), 42–50. <https://doi.org/10.32782/2786-765X/2026-12-6> [in Ukrainian].
2. Rohovets, M., & Yevdokymov, V. (2026). Model upravlinnia vykylykamy, ryzykamy ta zahrozamy derzhavnoi bezpetsi Ukrainy [A model for managing challenges, risks, and threats to the state security of Ukraine]. *Society and Security*, 1(13), 52–59. [https://doi.org/10.26642/sas-2026-1\(13\)-52-59](https://doi.org/10.26642/sas-2026-1(13)-52-59) [in Ukrainian].
3. Bazychenko, V.V. (2025). Zahrozy ta vykylyky derzhavnomu upravlinniu v sferi natsionalnoi bezpeky Ukrainy v umovakh hlobalnykh ta rehionalnykh vykylykiv [Threats and challenges to public administration in the field of national security of Ukraine under global and regional challenges]. *Visnyk Khersonskoho natsionalnoho tekhnichnoho universytetu – Bulletin of Kherson National Technical University*, 2(93), 344–348. <https://doi.org/10.35546/kntu2078-4481.2025.2.1.46> [in Ukrainian].
4. Maslii, O.A., & Maksymenko, A.P. (2022). Ryzyky ta zahrozy ekonomichnoi bezpetsi Ukrainy u tsyfrovii sferi v umovakh viiny [Risks and threats to the economic security of Ukraine in the digital sphere under wartime conditions]. *Rynkova ekonomika: Suchasna teoriia i praktyka upravlinnia – Market Economy: Contemporary Theory and Management Practice*, 21(3), 179–199. [https://doi.org/10.18524/2413-9998.2022.3\(52\).275802](https://doi.org/10.18524/2413-9998.2022.3(52).275802) [in Ukrainian].
5. Bosak, I.M. (2025). Informatsiina bezpeka Ukrainy: Zahrozy ta metody protydyi [Information security of Ukraine: Threats and countermeasures]. *Kyivskyi ekonomichnyi naukovi zhurnal – Kyiv Economic Scientific Journal*, (9), 33–39. <https://doi.org/10.32782/2786-765X/2025-9-4> [in Ukrainian].
6. Parkhomenko-Kutsevil, O.I. (2025). Suchasni vykylyky natsionalnoi bezpetsi Ukrainy v umovakh tsyfrovyykh vykylykiv: Derzhavno-upravlinnyi aspekt [Contemporary challenges to the national security of Ukraine under digital challenges: A public administration perspective]. *Publichne upravlinnia: Kontseptsii, paradyhma, rozvytok, udoskonalennia – Public Administration: Concepts, Paradigms, Development, and Improvement*, (12), 116–123. <https://doi.org/10.31470/2786-6246-2025-12-116-123> [in Ukrainian].

7. Bobyl, V.V., Loskutova, H.A., & Dron, M.A. (2022). Ryzyky ta dzherela zahroz zovnishnoekonomichnoi bezpeky Ukrainy [Risks and sources of threats to the foreign economic security of Ukraine]. *Review of Transport Economics and Management*, 8(24), 12–19. <https://doi.org/10.15802/rtem2022/257978> [in Ukrainian].
8. Onyshchenko, S.V., & Hlushko, A.A. (2022). Analitichniy vymir kiberbezpeky Ukrainy v umovakh zrostantia vyklykiv ta zahroz [Analytical dimension of cybersecurity of Ukraine amid growing challenges and threats]. *Ekonomika i rehion – Economics and the Region*, 1(84), 13–20. <https://journals.nupp.edu.ua/eir/article/view/2540> [in Ukrainian].
9. Naichuk, A.V., & Markitantov, V.Yu. (2022). Kliuchovi faktory eskalatsii bezpekovoї sytuatsii v Skhidnii Yevropi ta zahrozy derzhavnym interesam Ukrainy [Key factors of escalation of the security situation in Eastern Europe and threats to the national interests of Ukraine]. *Politolohichniy visnyk – Political Science Bulletin*, 88, 175–188. <https://doi.org/10.17721/2415-881x.2022.88.175-188> [in Ukrainian].
10. International Organization for Standardization. (n.d.). *ISO 31000: Risk management*. <https://www.iso.org/iso-31000-risk-management.html> [in English].
11. Fernandez de Henestrosa, M., Sischa, P.E., & Steffgen, G. (2023). Examining the challenge-hindrance-threat distinction of job demands alongside job resources. *Frontiers in Psychology*, 14:1011815. <https://doi.org/10.3389/fpsyg.2023.1011815> [in English].
12. Bojanić, D. (2022). Theoretical and methodological analysis of challenges, risks and threats. *Vojno delo*, 74(2), 1–17. <https://doi.org/10.5937/vojdela2202001B> [in English].
13. International Energy Agency. (2022). *Securing clean energy technology supply chains*. <https://doi.org/10.1787/be931bdc-en> [in English].
14. International Energy Agency. (2022). *Climate resilience for energy security*. <https://doi.org/10.1787/2a931f53-en> [in English].
15. European Parliament & Council of the European Union. (2019). *Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC*. <https://eur-lex.europa.eu/eli/reg/2019/941/oj/eng> [in English].
16. Aven, T. (2023). Is the definition of risk still contested? *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 237(1), 3. <https://doi.org/10.1177/1748006X221125865> [in English].
17. Xu, Y., Reniers, G., & Yang, M.A. (2024). A multidisciplinary review into the evolution of risk concepts and their assessment methods. *Processes*, 12, 2449. <https://doi.org/10.3390/pr12112449> [in English].
18. Zanotti, G., Chiffi, D., & Schiaffonati, V. (2024). AI-related risk: An epistemological approach. *Philosophy & Technology*, 37(66). <https://doi.org/10.1007/s13347-024-00755-7> [in English].
19. Geiger, G. (2024). Catastrophic risk: Indication, quantitative assessment and management of rare extreme events using a non-expected utility framework. *Annals of Operations Research*, 343, 223–261. <https://doi.org/10.1007/s10479-024-06259-z> [in English].
20. Dekker, M., & Alevizos, L. (2024). A threat-intelligence driven methodology to incorporate uncertainty in cyber risk analysis and enhance decision-making. *Security and Privacy*, 7(1), e333. <https://doi.org/10.1002/spy2.333> [in English].
21. Martínez, C.A., Van Prooijen, J., & Van Lange, P.A.M. (2022). A threat-based hate model: How symbolic and realistic threats underlie hate and aggression. *Journal of Experimental Social Psychology*, 103, Article 104393. <https://doi.org/10.1016/j.jesp.2022.104393> [in English].
22. Connelly, B., & Shi, W. (2022). Threats and responses in organizational research. *Journal of Management*, 48(6), 1366–1381. <https://doi.org/10.1177/01492063221080431> [in English].
23. International Atomic Energy Agency. (2015). *Risk informed approach for nuclear security measures for nuclear and other radioactive material out of regulatory control: Implementing guide* (Nuclear Security Series No. 24-G). IAEA. https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1678_web.pdf [in English].
24. Sukhodolia, O.M. (Ed.). (2023). *Enerhetychna bezpeka Ukrainy: Perspektyvna model upravlinnia ryzykamy* [Energy security of Ukraine: A prospective risk management model] (O.M. Sukhodolia, Yu.M. Kharazishvili, & G.L. Riabtsev). NISD, Kyiv, Ukraine. <https://doi.org/10.53679/NISS-book.2023.01> [in Ukrainian].
25. Sukhodolia, O.M., Riabtsev, G.L., Kharazishvili, Yu.M., et al. (2022). *Vyznachennia rivnia ta otsiniuvannia zahroz enerhetychnii bezpetsi* [Determining the level and assessing threats to energy security]. NISD, Kyiv, Ukraine. <https://doi.org/10.53679/NISS-analytrep.2022.13> [in Ukrainian].
26. Kharazishvili, Yu., Sukhodolia, O., Riabtsev, G., et al. (2025). Enhancing security in sustainable energy systems for Central European business: An adaptive response methodology under national economy. *Central European Business Review*, 14(4), 25–63. <https://doi.org/10.18267/j.cebr.396> [in English].

Історія статті / Article history:

Подано до редакції / Submitted to the editorial office (25.06.2026);

Прийнято до друку / Accepted for publication (20.09.2026);

Опубліковано / Published (10.10.2026)