4. ***Medynska, N. V.*** (2022). Instytutsionalizatsiia ekonomichnoho mekhanizmu resursozberezhennia ta enerhoefektyvnoho pryrodokorystuvannia: investytsiinyi ta sektoralnyi vymir [Institutionalization of the economic mechanism of resource conservation and energy-efficient environmental management: Investment and sectoral dimension]. *Investytsii: praktyka ta dosvid* [Investments: Practice and Experience], (11–12), 32–38. https://doi.org/10.32702/2306-6814.2022.11-12.32

5. ***Zapashchuk, L.*** (2017). Enerhozberezhennia yak napriam pidvyshchennia efektyvnosti vyrobnychoi diialnosti [Energy saving as a direction for increasing production efficiency]. *Ekonomika i suspilstvo* [Economy and Society], 428–434.

6. ***Hrishnova, O. A.*** (2011). *Liudskyi kapital: formuvannia v systemi osvity i zainiatosti* [Human capital: Formation in the system of education and employment]. Kyiv: KNEU.

7. ***Hrishnova, O. A., & Zaichko, O. S.*** (2016). Novitni tekhnolohii v ekonomitsi personalu: novi mozhlyvosti y novi vyklyky [Modern technologies in personnel economics: New opportunities and new challenges]. *Visnyk ekonomichnoi nauky Ukrainy* [Bulletin of Economic Science of Ukraine], (2), 52–57.

8. Pro enerhetychnu efektyvnist [On Energy Efficiency]. (Law of Ukraine No. 1818-IX of October 21, 2021). https://zakon.rada.gov.ua/laws/show/1818-20

9. ISO 50001:2018. (2018). *Energy management systems – Requirements with guidance for use*. Geneva: International Organization for Standardization. https://www.iso.org/iso-50001-energy-management.html

10. Pro zatverdzhennia Metodychnykh rekomendatsii z pytan orhanizatsii pidhotovky publichnykh investytsiinykh proiektiv ta yikh rozpodilu mizh prohramamy dlia pidhotovky publichnykh investytsiinykh proiektiv [On approval of the Methodological recommendations for organizing the preparation of public investment projects and their distribution among programs for the preparation of public investment projects]. (Order of the Ministry of Economy, Environment and Agriculture of Ukraine No. 4901 of April 10, 2026). https://me.gov.ua/download/659bcfc4-ac3c-4092-841b-61205625be3f/file.pdf

11. Pro Natsionalnyi plan dii z enerhoefektyvnosti na period do 2030 roku [On the National Energy Efficiency Action Plan until 2030]. (Resolution of the Cabinet of Ministers of Ukraine No. 1803-r of December 29, 2021). https://zakon.rada.gov.ua/laws/show/1803-2021-%D1%80

12. Pro skhvalennia Stratehii rozvytku sfery innovatsiinoi diialnosti na period do 2030 rok**u** [On approval of the Strategy for the Development of Innovation Activity until 2030]. (Resolution of the Cabinet of Ministers of Ukraine No. 526-r of July 10, 2019). https://zakon.rada.gov.ua/laws/show/526-2019-%D1%80#Text

13. Pro Osnovni zasady (stratehiiu) derzhavnoi ekolohichnoi polityky Ukrainy na period do 2030 roku [On the Basic Principles (Strategy) of the State Environmental Policy of Ukraine until 2030]. (Law of Ukraine No. 2697-VIII of February 28, 2019). https://zakon.rada.gov.ua/laws/show/2697-19#Text

14. Yevropeiskyi Zelenyi Kurs [European Green Deal]. https://ukraine-eu.mfa.gov.ua/posolstvo/galuzeve-spivrobitnictvo/klimat-yevropejska-zelena-ugoda.

Abstract.

Levko A. Improving the mechanism for utilizing alternative resource-conservation sources at enterprises.

The current development of enterprises is taking place amid increasing resource constraints, rising energy costs, stricter environmental requirements, and the need to ensure competitiveness through innovative modernization of production. Under these conditions, the use of alternative resource-conservation measures takes on strategic importance; however, the effectiveness of their implementation is significantly hampered by imperfections in existing organizational and economic management mechanisms. The purpose of this article is to substantiate the theoretical and methodological foundations for improving the mechanism for utilizing alternative resource-conservation measures at enterprises based on a systematic combination of strategic, economic, organizational, and innovation- and digital-based management tools. The study conducts a functional analysis of the mechanism for utilizing alternative sources of resource conservation through the lens of key management functions: goal-setting, planning, organizing, motivating, controlling, and adapting. A model of the management cycle of energy transformation is proposed, which ensures the continuity of the processes of planning, implementation, monitoring, and improvement of the mechanism for utilizing alternative sources of resource conservation. The principles governing the mechanism's operation have been systematized at the strategic, economic, organizational-managerial, and institutional-environmental levels, forming a comprehensive foundation for its structure. An assessment of the current mechanism was conducted, and its key shortcomings were identified, including insufficient integration of resource conservation into corporate strategy, weak cross-functional coordination, limited use of digital technologies, insufficient development of human resources, and the absence of a comprehensive monitoring system. A multilevel integrative model of the mechanism is proposed, combining strategic, organizational, economic, and innovation-digital management dimensions; a typology of enterprises based on the level of development of these dimensions has also been developed. Practical directions for improving the mechanism are substantiated, covering the strategic integration of resource conservation, the development of economic incentives and financial instruments, institutional and organizational transformation of management, technological modernization of production, human capital development, and the formation of an adaptive monitoring system.

Keywords: *resource conservation, alternative sources of resource conservation, circular economy, energy efficiency, sectoral assessment, biogas, closed-loop water supply, ESG, industrial enterprises.*

Стаття надійшла до редакції / Received 29.05.2026 Прийнята до друку / Accepted 19.06.2026 Опубліковано/ Published 07.08.2026

Бібліографічний опис статті:

Левко А.В. Удосконалення механізму використання альтернативних джерел ресурсозбереження на підприємствах. Актуальні проблеми інноваційної економіки та права. 2026. № 3. С. 106-110.

Levko A. Improving the mechanism for utilizing alternative resource-conservation sources at enterprises. Actual problems of innovative economy and law. 2026. No. 3, pp. 106-110.

УДК: 005.934:005.334:658; JEL classification: H56, M10, D81 **DOI: https://doi.org/10.36887/2524-0455-2026-3-19**

ЛИЗУН Руслан Богданович, здобувач PhD ОП «Менеджмент», Полтавський університет економіки і торгівлі, https://orcid.org/0009-0005-7848-1160

КЛАСИФІКАЦІЯ ГІБРИДНИХ ЗАГРОЗ ЯК ОСНОВА ФОРМУВАННЯ МЕХАНІЗМІВ МЕНЕДЖМЕНТУ БЕЗПЕКИ ПІДПРИЄМСТВА

Лизун Р.Б. Класифікація гібридних загроз як основа формування механізмів менеджменту безпеки підприємства.

У статті досліджено теоретичні підходи до класифікації гібридних загроз у системі менеджменту безпеки підприємства. Обгрунтовано, що сучасне безпекове середовище характеризується поєднанням економічних, цифрових, інформаційних, психологічних, кадрових і логістичних впливів, які формують складну систему взаємопов'язаних ризиків. Встановлено, що наявні підходи до класифікації загроз переважно сформовані в межах національної безпеки та недостатньо враховують особливості функціонування підприємств в умовах воєнної економіки й цифрової трансформації. На основі аналізу зарубіжних та українських досліджень запропоновано авторський підхід до класифікації гібридних загроз підприємства за джерелом виникнення, сферою впливу, характером реалізації, швидкістю поширення та масштабом наслідків. Визначено основні групи гібридних загроз: економічні, цифрові, інформаційні, кадрові, психологічні, логістичні, енергетичні, правові та репутаційні. Доведено, що запропонована класифікація створює теоретичне підґрунтя для формування механізмів менеджменту безпеки підприємств і розроблення систем оцінювання їхньої адаптивної стійкості.

Ключові слова: *гібридні загрози, менеджмент безпеки, економічна безпека підприємства, адаптивна стійкість, ризик-менеджмент, класифікація загроз, резильєнтність, безпекоорієнтований менеджмент.*

This is an Open Access article distributed under the terms of the Creative Commons CC-BY 4.0

© ЛИЗУН Руслан Богданович, 2026

Постановка проблеми у загальному вигляді. Сучасний етап розвитку економіки характеризується зростанням рівня невизначеності та формуванням нової архітектури ризиків, що суттєво впливає на

функціонування підприємств. Війна, цифровізація бізнес-процесів, глобалізація ринків, кіберзагрози, інформаційні атаки, логістичні розриви та кадрова нестабільність формують складне безпекове середовище, в якому традиційні підходи до забезпечення безпеки поступово втрачають свою ефективність.

Однією з ключових характеристик сучасного середовища є гібридний характер загроз, адже, на відміну від традиційних ризиків, які мають відносно локалізований характер, гібридні загрози поєднують різні форми впливу та реалізуються одночасно в економічній, цифровій, інформаційній, соціальній та психологічній площинах, що значно ускладнює процес їх ідентифікації, оцінювання та управління.

Аналіз останніх досліджень і публікацій. У наукових дослідженнях значна увага приділяється проблемам гібридних загроз, однак більшість наявних класифікацій сформована переважно в межах національної безпеки, міжнародних відносин або кібербезпеки, а що стосується питання класифікації гібридних загроз саме для підприємств, то воно залишається недостатньо дослідженим та потребує подальшого наукового опрацювання. Особливої актуальності ця тематика набула в умовах цифрової трансформації економіки та посилення глобальних безпекових викликів, зокрема через повномасштабну війну в Україні.

Проведений нами аналіз низки літературних джерел дозволив зробити такі висновки:

значний внесок у розвиток теоретичних засад дослідження гібридних загроз зробили зарубіжні науковці та міжнародні безпекові інституції. Так, Т. Хідашелі розглядає гібридні загрози як поєднання традиційних і нетрадиційних методів впливу, що охоплюють інформаційні операції, економічний тиск, кібератаки та психологічний вплив. Авторка наголошує, що головною особливістю гібридних загроз є їх комплексний характер та здатність впливати одночасно на декілька сфер функціонування об'єкта впливу [1];

подібної позиції дотримуються експерти НАТО, які визначають гібридні загрози як сукупність взаємопов'язаних військових і невійськових інструментів впливу, що використовуються для дестабілізації політичних, економічних і соціальних систем. У документах НАТО до основних складових гібридних загроз віднесено інформаційні кампанії, кібернетичні атаки, економічний тиск, диверсії, маніпулювання громадською думкою та використання енергетичних ресурсів як інструменту впливу [2];

важливий внесок у розвиток концептуального розуміння гібридних загроз зробили Г. Джаннопулос, Г. Сміт та М. Теохаріду, які у межах дослідження Об'єднаного дослідницького центру Європейської Комісії (JRC) запропонували концептуальну модель гібридних загроз. Науковці доводять, що сучасні гібридні загрози характеризуються високою адаптивністю, багатовекторністю та здатністю швидко змінювати форми реалізації залежно від умов середовища. Запропонована ними модель передбачає поєднання економічних, інформаційних, технологічних, політичних та соціальних впливів у межах єдиної системи дестабілізації [3];

Особливого значення для нашого дослідження набувають праці, присвячені питанням економічного виміру гібридних загроз. Так, О. Карпенко наголошує, що сучасні гібридні загрози дедалі активніше впливають на економічні процеси, формуючи нові ризики для суб'єктів господарювання. Авторка підкреслює необхідність інтеграції механізмів протидії гібридним загрозам у систему забезпечення економічної стійкості та відновлення економіки України [4].

Окремий напрям досліджень формують праці, присвячені цифровим і кібернетичним загрозам. Зокрема, Т. Д. Ле, Х. Нгуєн та П. Тран доводять, що цифровізація бізнес-процесів супроводжується зростанням масштабів кіберризиків і потребує переходу до аналітики безпеки, заснованої на даних. Автори підкреслюють необхідність використання комплексних підходів до ідентифікації ризиків, які враховують взаємозв'язки між цифровими, інформаційними та організаційними загрозами [5].

У вітчизняній науковій літературі проблематика безпеки підприємств традиційно розглядається крізь призму економічної безпеки. Так, С. Співак досліджує питання стратегічного управління економічною безпекою підприємств в умовах воєнного стану та акцентує увагу на необхідності адаптації систем управління до нових викликів зовнішнього середовища [6].

Науковий інтерес також становлять дослідження Д. Крилова, який розглядає загрози економічній безпеці підприємства як динамічну систему факторів, що потребує постійного моніторингу та оновлення інструментарію управління. Автор наголошує на необхідності уточнення класифікаційних ознак загроз як передумови побудови ефективної системи управління безпекою [7].

Разом із тим проведений аналіз літературних джерел дозволяє зробити висновок, що більшість існуючих класифікацій гібридних загроз сформовано переважно для потреб державного управління, національної безпеки або кібербезпеки. Водночас недостатньо дослідженими залишаються питання класифікації гібридних загроз саме в системі менеджменту безпеки підприємств. Зокрема, потребують подальшого наукового обґрунтування класифікаційні ознаки, які дають змогу пов'язати окремі види гібридних загроз із відповідними механізмами менеджменту безпеки підприємства. Саме ця наукова прогалина і зумовлює необхідність розроблення авторського підходу до класифікації гібридних загроз як основи формування механізмів менеджменту безпеки підприємства.

Формулювання цілей статті (постановка завдання). Метою статті є обґрунтування теоретичних засад класифікації гібридних загроз у системі менеджменту безпеки підприємства та розроблення авторського підходу до їх систематизації.

Виклад основного матеріалу дослідження. Проведений вище аналіз наукових джерел дозволив зробити висновок, що наявні підходи до класифікації гібридних загроз переважно орієнтовані на сферу національної безпеки, міжнародних відносин та кібербезпеки, але діяльність підприємств характеризується власною специфікою, пов'язаною з функціонуванням виробничих, фінансових, кадрових, інформаційних і логістичних систем. Тому виникає необхідність адаптації існуючих підходів до потреб менеджменту безпеки підприємств.

На нашу думку, класифікація гібридних загроз повинна не лише відображати природу ризиків, а й створювати основу для формування відповідних механізмів їх управління, тому запропонований нами підхід базується на кількох класифікаційних ознаках, які дозволяють комплексно охарактеризувати джерела виникнення, характер реалізації та потенційні наслідки гібридних загроз (табл. 1).

Таблиця 1

Авторська класифікація гібридних загроз у системі менеджменту безпеки підприємства

Класифікаційна ознака	Вид загроз
За джерелом виникнення	зовнішні, внутрішні, змішані
За сферою впливу	економічні, цифрові, інформаційні, кадрові, психологічні, логістичні, енергетичні, правові, репутаційні
За характером впливу	прямі, опосередковані
За швидкістю реалізації	раптові, поступові
За масштабом наслідків	локальні, системні, критичні
За тривалістю впливу	короткострокові, середньострокові, довгострокові
За рівнем керованості	контрольовані, частково контрольовані, неконтрольовані

Джерело: розроблено автором.

Запропонована класифікація дозволяє не лише систематизувати різноманітні прояви гібридних загроз,

а й створити підґрунтя для їх подальшої інтеграції в систему менеджменту безпеки підприємства. На відміну від традиційних підходів, які переважно орієнтуються на окремі види ризиків, запропонований підхід враховує багатовекторний характер сучасних дестабілізаційних впливів і їхню взаємозалежність.

Особливістю гібридних загроз є те, що вони можуть одночасно реалізовуватися через кілька каналів впливу та спричиняти каскадний ефект негативних наслідків. Наприклад, цифрова загроза у вигляді кібератаки здатна спричинити втрату критично важливих даних, що, своєю чергою, може призвести до фінансових збитків, репутаційних втрат і зниження довіри з боку клієнтів і партнерів. Аналогічно кадрові загрози можуть трансформуватися у виробничі, логістичні або інформаційні ризики. У зв'язку з цим важливого значення набуває не лише ідентифікація окремих загроз, а й розуміння взаємозв'язків між ними. Саме тому класифікація гібридних загроз має розглядатися як інструмент управління, що дозволяє визначати пріоритетні напрями формування механізмів менеджменту безпеки підприємства.

Для більш глибокого розуміння специфіки гібридних загроз доцільно не лише визначити їхні види, а й оцінити характер їхнього впливу на діяльність підприємства. На відміну від традиційних ризиків, які переважно впливають на окремі підсистеми організації, гібридні загрози здатні одночасно охоплювати кілька сфер діяльності підприємства та формувати каскадний ефект негативних наслідків. Саме тому важливим є визначення основних об'єктів впливу кожного виду загроз і оцінювання потенційних наслідків їх реалізації. Результати такої систематизації наведено в табл. 2.

Таблиця 2

Характеристика гібридних загроз за рівнем впливу на діяльність підприємства

Вид загрози	Основний об'єкт впливу	Потенційні наслідки	Вид загрози
Економічні	фінансові ресурси	зниження прибутковості, фінансові втрати	Економічні
Цифрові	інформаційні системи	витік даних, зупинка процесів	Цифрові
Інформаційні	репутація, комунікації	дезінформація, втрата довіри	Інформаційні
Кадрові	персонал	дефіцит кадрів, зниження продуктивності	Кадрові
Психологічні	людський капітал	стрес, вигорання, демотивація	Психологічні
Логістичні	ланцюги постачання	затримки поставок, зрив контрактів	Логістичні
Енергетичні	виробничі процеси	простої, зупинка діяльності	Енергетичні
Правові	система управління	штрафи, додаткові витрати	Правові
Репутаційні	імідж підприємства	втрата клієнтів та партнерів	Репутаційні

Джерело: розроблено автором.

Дані табл. 2 свідчать, що найбільш небезпечними для сучасних підприємств є цифрові, економічні, логістичні та репутаційні загрози, оскільки їх реалізація може спричинити не лише прямі втрати ресурсів, а й дестабілізацію ключових бізнес-процесів. Водночас особливістю гібридних загроз є їх взаємозалежність та здатність до взаємного посилення. Наприклад, цифрова атака може призвести до витоку конфіденційної інформації, що, своєю чергою, спричинить репутаційні втрати, відтік клієнтів та погіршення фінансових результатів діяльності підприємства. Аналогічно кадрові та психологічні загрози можуть трансформуватися у виробничі, інформаційні або логістичні ризики.

Таким чином, результати проведеної систематизації підтверджують необхідність розгляду гібридних загроз як комплексної системи взаємопов'язаних впливів, що потребує формування інтегрованих механізмів менеджменту безпеки підприємства. Саме це зумовлює доцільність подальшого дослідження взаємозв'язку між окремими видами гібридних загроз і механізмами їх нейтралізації.

Отже, запропонована класифікація гібридних загроз створює теоретичне підґрунтя для подальшого дослідження механізмів менеджменту безпеки підприємств і розроблення моделей оцінювання їхньої адаптивної стійкості. Крім того, варто зазначити, що запропонована класифікація гібридних загроз має не лише теоретичне, а й важливе практичне значення, оскільки створює підґрунтя для формування ефективних механізмів менеджменту безпеки підприємства. У сучасних умовах підприємства стикаються не з окремими ризиками, а зі складними системами взаємопов'язаних загроз, що вимагає переходу від фрагментарного управління безпекою до комплексного безпекоорієнтованого менеджменту. Вважаємо, що кожній групі гібридних загроз повинні відповідати певні механізми менеджменту безпеки, здатні забезпечувати своєчасне виявлення ризиків, мінімізацію їх негативних наслідків та підвищення адаптивної стійкості підприємства.

Таким чином, можемо стверджувати, що практична цінність класифікації гібридних загроз полягає не лише в їх систематизації, а й у можливості використання отриманих результатів для формування механізмів менеджменту безпеки підприємства. У сучасних умовах управління безпекою має ґрунтуватися на принципах превентивності, адаптивності та комплексності, що передбачає необхідність вибору відповідних управлінських інструментів залежно від характеру загроз. На нашу думку, кожна група гібридних загроз потребує застосування специфічних механізмів менеджменту безпеки, спрямованих на мінімізацію ризиків і підвищення рівня адаптивної стійкості підприємства. З метою систематизації взаємозв'язку між видами гібридних загроз і механізмами менеджменту безпеки побудовано відповідну матрицю (табл. 3).

Таблиця 3

Відповідність гібридних загроз та механізмів менеджменту безпеки підприємства

Вид гібридної загрози	Основний прояв	Пріоритетний механізм менеджменту безпеки	Очікуваний результат
Економічні	фінансова нестабільність, інфляція	стратегічний, ризик-орієнтований	підвищення фінансової стійкості
Цифрові	кібератаки, витік даних	цифровий, інформаційний	забезпечення кіберстійкості
Інформаційні	дезінформація, інформаційний тиск	інформаційний, комунікаційний	захист інформаційного середовища
Кадрові	дефіцит персоналу, міграція кадрів	кадровий	збереження людського капіталу
Психологічні	стрес, вигорання	психологічний	підтримка психологічної стійкості
Логістичні	порушення поставок	антикризовий, стратегічний	безперервність діяльності
Енергетичні	перебої енергопостачання	антикризовий, адаптивний	підвищення операційної стійкості
Правові та регуляторні	зміни законодавства	стратегічний, ризик-орієнтований	адаптація до регуляторних змін
Репутаційні	інформаційні атаки, дискредитація	комунікаційний, інформаційний	підтримка довіри стейкхолдерів

Джерело: розроблено автором.

Аналіз даних табл. 3 свідчить, що між окремими видами гібридних загроз і механізмами менеджменту безпеки існує прямий функціональний взаємозв'язок. Водночас жоден із механізмів не може забезпечити належний рівень безпеки самостійно, оскільки сучасні гібридні загрози мають комплексний характер і одночасно впливають на кілька сфер діяльності підприємства. Особливої уваги потребують цифрові, інформаційні та кадрові загрози, які характеризуються високою швидкістю

поширення та здатністю генерувати вторинні ризики. Так, кібератака може спричинити не лише технічні збої, а й репутаційні втрати, фінансові збитки та зниження довіри клієнтів. У свою чергу кадрові проблеми можуть трансформуватися у виробничі, інформаційні або логістичні ризики.

Отже, можна зробити висновок, що ефективність менеджменту безпеки підприємства визначається не стільки наявністю окремих захисних інструментів, скільки рівнем інтеграції стратегічного, кадрового, цифрового, інформаційного, антикризового та адаптивно-резильєнтного механізмів управління в єдину систему забезпечення безпеки.

Саме тому важливого значення набуває концепція адаптивної стійкості підприємства, яка передбачає здатність організації зберігати функціональність, швидко відновлюватися після кризових подій та використовувати здобутий досвід для подальшого розвитку. У цьому контексті доцільно розглядати гібридні загрози не лише як джерело ризиків, а й як чинник трансформації системи управління підприємством. Їхня поява зумовлює необхідність перегляду управлінських підходів, удосконалення організаційної структури, розвитку цифрових компетентностей персоналу, впровадження сучасних інструментів аналітики та формування культури безпеки.

Таким чином, проведене в межах цієї статті дослідження дозволяє стверджувати, що ефективність менеджменту безпеки підприємства визначається не лише наявністю окремих механізмів реагування на ризики, а й рівнем їх інтеграції в єдину систему управління. Запропонована класифікація гібридних загроз створює підґрунтя для формування відповідних механізмів менеджменту безпеки, які повинні забезпечувати своєчасне виявлення загроз, мінімізацію їхніх негативних наслідків і підтримання адаптивної стійкості підприємства. З метою відображення взаємозв'язку між основними групами гібридних загроз, механізмами менеджменту безпеки та результатами їх функціонування розроблено концептуальну модель, представлену на рис. 1.

Представлена на рис. 1 концептуальна модель відображає логіку трансформації гібридних загроз у відповідні управлінські рішення через систему механізмів менеджменту безпеки підприємства.

Рис. 1. Концептуальна модель взаємозв'язку між гібридними загрозами та механізмами менеджменту безпеки підприємства. *Джерело: сформовано автором*

Центральне місце в моделі займають механізми менеджменту безпеки, які виступають сполучною ланкою між зовнішніми та внутрішніми загрозами й результатами функціонування підприємства. Особливістю запропонованої моделі є інтегрований підхід до забезпечення безпеки, відповідно до якого різні види гібридних загроз не розглядаються ізольовано, а формують єдину систему взаємопов'язаних ризиків. Саме тому нейтралізація таких загроз потребує комплексного використання стратегічного, кадрового, цифрового, інформаційного, антикризового та адаптивно-резильєнтного механізмів управління.

Запропонована модель також демонструє, що кінцевим результатом функціонування системи менеджменту безпеки є не лише захист ресурсів та активів підприємства, а й забезпечення його адаптивної стійкості, безперервності бізнес-процесів, конкурентоспроможності та здатності до довгострокового розвитку. Таким чином, гібридні загрози доцільно розглядати не лише як джерело ризиків, а і як чинник трансформації сучасних підходів до управління безпекою підприємства.

Висновки та перспективи подальших досліджень. Отже, узагальнюючи можна зробити такі висновки:

запропонована класифікація гібридних загроз може використовуватися як основа для побудови комплексної системи менеджменту безпеки підприємства, що забезпечуватиме своєчасну ідентифікацію ризиків, вибір відповідних механізмів реагування та підвищення рівня адаптивної стійкості організації;

встановлено, що гібридні загрози стають одним із ключових факторів трансформації сучасної системи менеджменту безпеки підприємств. На відміну від традиційних ризиків, вони характеризуються багатокомпонентністю, взаємозалежністю та здатністю одночасно впливати на різні сфери діяльності підприємства;

обґрунтовано доцільність розгляду гібридних загроз як комплексу взаємопов'язаних економічних, цифрових, інформаційних, кадрових, психологічних, логістичних, енергетичних, правових та репутаційних впливів, що формують нелінійну систему ризиків функціонування підприємства;

запропоновано авторський підхід до класифікації гібридних загроз за джерелом виникнення, сферою впливу, характером реалізації, швидкістю поширення, тривалістю впливу та масштабом наслідків. На основі розробленої класифікації сформовано матрицю відповідності між окремими видами загроз та механізмами менеджменту безпеки підприємства та концептуальну модель взаємозв'язку гібридних загроз та механізмів менеджменту безпеки підприємства;

доведено, що ефективність забезпечення безпеки підприємства залежить від рівня інтеграції стратегічних, кадрових, цифрових, інформаційних, антикризових та адаптивно-резильєнтних механізмів управління. Це створює передумови для переходу від традиційної моделі захисту до безпекоорієнтованого менеджменту, спрямованого на забезпечення адаптивної стійкості підприємства в умовах високої невизначеності.

Перспективи подальших досліджень пов'язані з розробленням методичних підходів до оцінювання рівня впливу гібридних загроз на діяльність підприємства, побудовою системи індикаторів адаптивної стійкості та формуванням інтегрального індексу безпеки підприємства в умовах гібридних загроз.

Література.

1. ***Khidasheli, T.*** *Hybrid Threats and Resilience*. Tbilisi: Friedrich Naumann Foundation for Freedom South Caucasus, 2024. 54 p. https://www.freiheit.org/sites/default/files/2024-12/hybrid-threats-and-resilience-final.pdf.
2. NATO. *Countering Hybrid Threats*. Brussels: NATO, 2025. https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats.
3. ***Giannopoulos, G., Smith, H., & Theocharidou, M.*** *The Landscape of Hybrid Threats: A Conceptual Model*. Luxembourg: Publications Office of the European Union, 2021. 64 p. DOI: https://doi.org/10.2760/44985.
4. ***Karpenko, O.*** European Experience in Countering Hybrid Threats for Ukraine's Economic Recovery. *International Economic Policy*. 2024. (41). P. 188–207. DOI: https://doi.org/10.33111/iep.2024.41.12.
5. ***Le, T. D., Nguyen, H., & Tran, P.*** Cybersecurity Analytics for the Enterprise Environment: A Systematic Literature Review. *Electronics*. 2025. 14(11). Article 2252. DOI: https://doi.org/10.3390/electronics14112252.
6. ***Співак, С.*** Удосконалення стратегії управління економічною безпекою підприємств в умовах воєнного стану. *Галицький економічний вісник*. 2025. Т. 97(2). С. 152–164. https://doi.org/10.33108/galicianvisnyk_tntu2025.06.211.
7. ***Крилов, Д.*** Характеристика загроз економічній безпеці підприємства в сучасних умовах. *Проблеми сучасних трансформацій. Серія: Економіка та управління*. 2024. (13). С. 54–63. DOI: https://doi.org/10.54929/2786-5738-2024-13-04-07.

References.

1. ***Khidasheli, T.*** (2024). *Hybrid Threats and Resilience*. Tbilisi: Friedrich Naumann Foundation for Freedom South Caucasus. https://www.freiheit.org/sites/default/files/2024-12/hybrid-threats-and-resilience-final.pdf.
2. NATO. (2025). *Countering Hybrid Threats*. Brussels: NATO. https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats.
3. ***Giannopoulos, G., Smith, H., & Theocharidou, M.*** (2021). *The Landscape of Hybrid Threats: A Conceptual Model*. Luxembourg: Publications Office of the European Union. https://doi.org/10.2760/44985.
4. ***Karpenko, O.*** (2024). European experience in countering hybrid threats for Ukraine's economic recovery. *International Economic Policy*, (41), 188–207. https://doi.org/10.33111/iep.2024.41.12.
5. ***Le, T. D., Nguyen, H., & Tran, P.*** (2025). Cybersecurity analytics for the enterprise environment: A systematic literature review. *Electronics, 14*(11), Article 2252. https://doi.org/10.3390/electronics14112252.
6. ***Spivak, S.*** (2025). Improving the strategy of economic security management of enterprises under martial law. *Galician Economic Bulletin, 97*(2), 152–164. https://doi.org/10.33108/galicianvisnyk_tntu2025.06.211.
7. ***Krylov, D.*** (2024). Characteristics of threats to the economic security of enterprises in modern conditions. *Problems of Modern Transformations. Series: Economics and Management*, (13), 54–63. https://doi.org/10.54929/2786-5738-2024-13-04-07.

Abstract.

Lyzun R. Classification of hybrid threats as a basis for the formation of enterprise security management mechanisms.

The article investigates theoretical approaches to the classification of hybrid threats within the enterprise security management system. It is substantiated that the contemporary security environment is characterized by a combination of economic, digital, informational, psychological, personnel-related, and logistical influences that create a complex system of interconnected risks. The study demonstrates that existing approaches to threat classification are primarily developed within the framework of national security, international relations, and cybersecurity, while insufficiently considering the specific features of enterprise functioning under conditions of wartime economy, digital transformation, and increasing environmental uncertainty. Based on the analysis of foreign and Ukrainian scientific research, an authorial approach to the classification of hybrid threats is proposed. The classification is developed according to the source of origin, sphere of influence, nature of impact, speed of implementation, duration, controllability, and scale of consequences. It is argued that such a multidimensional approach enables a more comprehensive understanding of the complex and nonlinear nature of hybrid threats affecting enterprise activities. The study identifies the main groups of hybrid threats to enterprises, including economic, digital, informational, personnel-related, psychological, logistical, energy, legal, regulatory, and reputational threats. It is emphasized that these threats do not exist independently but interact with each other, generating cascading effects and increasing the overall level of uncertainty within the enterprise environment. Particular attention is paid to the relationship between hybrid threats and enterprise security management mechanisms. The article substantiates that the classification of threats should serve not only as an analytical tool but also as a foundation for the formation of appropriate security management mechanisms. An authorial matrix of correspondence between hybrid threats and security management mechanisms is developed, which allows determining priority managerial responses to various categories of threats. The results of the study prove that the effectiveness of enterprise security management depends on the degree of integration of strategic, risk-oriented, personnel, digital, informational, communication, crisis-management, and adaptive-resilience mechanisms. The proposed classification provides a theoretical basis for developing security-oriented management systems, assessing enterprise adaptive resilience, and designing integrated security management models under hybrid threats.

Keywords: *hybrid threats, security management, enterprise security, economic security, security-oriented management, adaptive resilience, resilience, risk management, cybersecurity, crisis management, enterprise security management mechanisms, hybrid risk classification.*

Стаття надійшла до редакції / Received 09.06.2026 Прийнята до друку / Accepted 22.06.2026 Опубліковано/ Published 07.08.2026

Бібліографічний опис статті:

Лизун Р.Б. Класифікація гібридних загроз як основа формування механізмів менеджменту безпеки підприємства. Актуальні проблеми інноваційної економіки та права. 2026. № 3. С. 110-114.

Lyzun R. Classification of hybrid threats as a basis for the formation of enterprise security management mechanisms. Actual problems of innovative economy and law. 2026. No. 3. pp. 110-114.

УДК: 339.564:338.43; JEL classification: Q13, F14, O13, Q17, M31 DOI: https://doi.org/10.36887/2524-0455-2026-3-20

ЛЯХОВ Віктор Костянтинович, аспірант кафедри міжнародних економічних відносин та іноземних мов Центральноукраїнського національного технічного університету (ЦНТУ), https://orcid.org/0009-0003-2920-6803
МИЦЕНКО Валерій Іванович, канд. пед. наук, доцент, доцент кафедри міжнародних економічних відносин та іноземних мов, Центральноукраїнський національний технічний університет, https://orcid.org/0000-0001-6034-0224

ФОРМУВАННЯ КОНКУРЕНТОСПРОМОЖНОСТІ СІЛЬСЬКОГОСПОДАРСЬКОЇ ПРОДУКЦІЇ НА СВІТОВИХ РИНКАХ

Ляхов В. К., Миценко В. І. формування конкурентоспроможності сільськогосподарської продукції на світових ринках.

Статтю присвячено обґрунтуванню умов, факторів і механізму формування конкурентоспроможності сільськогосподарської продукції на світових ринках у контексті трансформації глобального попиту, технологічних змін, посилення санітарних, фітосанітарних та екологічних вимог, цінової волатильності й геополітичних ризиків. Метою дослідження є систематизація складових міжнародної конкурентоспроможності аграрної продукції, визначення сучасних тенденцій світових аграрних ринків та оцінювання структурних характеристик українського агропродовольчого експорту. Використано методи системного аналізу, узагальнення, порівняння, структурно-динамічного аналізу, а також розрахунку експортної спеціалізації та товарної концентрації. Інформаційну основу становлять матеріали OECD-FAO Agricultural Outlook 2026-2035, FAOSTAT, FAO Food Price Index, Світової організації торгівлі, Codex Alimentarius, Міністерства економіки та Державної митної служби України. Встановлено, що конкурентоспроможність сільськогосподарської продукції визначається не лише ціновими перевагами, а й поєднанням продуктивності,

This is an Open Access article distributed under the terms of the Creative Commons CC-BY 4.0

© ЛЯХОВ Віктор Костянтинович, МИЦЕНКО Валерій Іванович, 2026