ОРГАНІЗАЦІЙНО-ЕКОНОМІЧНИЙ МЕХАНІЗМ УПРАВЛІННЯ ІННОВАЦІЙНО-ІНФОРМАЦІЙНОЮ СКЛАДОВОЮ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

ORGANIZATIONAL AND ECONOMIC MECHANISM FOR MANAGING THE INNOVATION AND INFORMATION COMPONENT OF AN ENTERPRISE'S ECONOMIC SECURITY

В умовах цифрової трансформації економіки та посилення гібридних загроз управління інноваційно-інформаційною складовою економічної безпеки підприємства набуває стратегічного значення. У статті розроблено організаційно-економічний механізм управління інноваційно-інформаційною складовою економічної безпеки підприємства, що забезпечує системний перехід від результатів кількісної діагностики до диференційованих управлінських рішень. Механізм структурований у формі чотирьох взаємопов'язаних контурів: діагностики, формування управлінського фокусу, реалізації та контролю, аналізу та адаптації. Розроблено чотирирівневу організаційну модель суб'єктів управління з чіткою специфікацією функцій стратегічного, координаційного, аналітичного та виконавчого рівнів і механізмами горизонтальної координації. Визначено систему очікуваних управлінських ефектів за стратегічним, тактичним, операційним та інтегративним рівнями. Практична цінність дослідження полягає у можливості застосування запропонованого механізму у системі стратегічного управління економічною безпекою підприємств різних галузей з урахуванням їхніх ресурсних можливостей та поточного стану інноваційно-інформаційної складової.

Ключові слова: *економічна безпека підприємства, інноваційно-інформаційна складова, організаційно-економічний механізм управління, управлінський режим, діагностика рівня безпеки, цифрова трансформація.*

In the context of digital transformation of the economy and increasing hybrid threats, managing the innovation and information component of an enterprise's economic security is becoming strategically important. However, most enterprises do not have systematic approaches that would allow them to translate security diagnostics results into specific management decisions. The purpose of this article is to develop and justify an organizational and economic mechanism for managing the innovation and information component of an enterprise's economic security. The study uses systemic, process, and situational approaches. The CRITIC-DEMATEL methodology forms the basis for the quantitative assessment of the innovation and information component of an enterprise's economic security. The article develops an organizational and economic mechanism for managing the innovation and information component of an enterprise's economic security, which ensures a systematic transition from the results of quantitative diagnostics to differentiated management decisions. The mechanism is structured in the form of four interrelated contours: diagnostics, formation of management focus, implementation and control, analysis and adaptation. A four-level organizational model of management entities is proposed, covering strategic, coordination, analytical, and executive levels with clearly defined functions, coordination tools, and feedback mechanisms. A typology of expected management effects at the strategic, tactical, operational, and integration levels with corresponding time horizons is defined. The practical value of the study lies in the applicability of the proposed mechanism to the strategic management systems of enterprises across various industries. The mechanism enables evidence-based governance of the innovation and information security component, ensures rational prioritization of managerial efforts, and facilitates a consistent transition from diagnostic results to targeted corrective actions, taking into account the specific resource constraints and current security maturity level of each enterprise.

Key words: *economic security of an enterprise, innovation and information component, organizational and economic management mechanism, management regime, security level diagnostics, digital transformation.*

УДК 338.2

DOI: https://doi.org/10.32782/dees.22-10

Немировський Ф.В.[1]
аспірант,
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Nemyrovskyi Fedir
National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute"

Постановка проблеми. В сучасній економіці, що характеризується стрімкою цифровізацією виробничих процесів та загостренням конкурентної боротьби, інноваційно-інформаційна складова набуває визначального значення у забезпеченні економічної безпеки підприємства. Втрата інформаційних активів, технологічне відставання, кіберзагрози та недостатній рівень цифрових компетенцій персоналу здатні суттєво підривати конкурентоспроможність суб'єктів господарювання. Попри це, більшість вітчизняних підприємств досі не мають систематизованого механізму управління інноваційно-інформаційною складовою економічної безпеки: діагностика стану системи здійснюється епізодично, управлінські рішення приймаються без належного кількісного обґрунтування, а відповідальність між підрозділами не розмежована. Це зумовлює потребу у розробці організаційно-економічного механізму, здатного забезпечити обґрунтований та системний перехід від результатів діагностики до диференційованих управлінських рішень.

Аналіз останніх досліджень і публікацій. Тема економічної безпеки підприємства знайшла широке відображення у працях вітчизняних та зарубіжних науковців. Питання формування

[1] ORCID: http://orcid.org/0009-0008-0219-8029

складових економічної безпеки та методологічних підходів до їх оцінки досліджували Дейнега І. [1], Лєзіна А. [2], Нам'ясенко В. [3], Рудніченко Є. [4] та ін. Проблематику інноваційної безпеки та управління інноваційним розвитком підприємств розглядали Гринько Т. [5], Малиш В. [6], Тульчинська С. [7]. Інформаційну безпеку та кібербезпеку в контексті економічної діяльності вивчали Ковальчук А. [8], Мачак Т. [9], Ситнік Є. [10]. Разом з тим, більшість досліджень зосереджені або на окремих складових безпеки, або на загальних концептуальних моделях, не пропонуючи цілісного механізму, який би інтегрував діагностику, стратегічне цілепокладання, організаційну архітектуру та систему контролю в єдиний управлінський контур. Поза увагою дослідників залишається також питання диференціації управлінських режимів та інструментів залежно від поточного рівня інноваційно-інформаційної складової економічної безпеки підприємства (далі – ІІЕБП), що і визначає наукову актуальність цього дослідження.

Постановка завдання. Метою статті є розробка та обґрунтування організаційно-економічного механізму управління інноваційно-інформаційною складовою економічної безпеки підприємства, що забезпечує системний перехід від результатів кількісної діагностики до диференційованих управлінських рішень. Завданнями дослідження є: обґрунтування концептуальної логіки механізму управління ІІЕБП; розробка організаційної моделі суб'єктів управління із визначенням їхніх функцій та інструментів координації; ідентифікація очікуваних управлінських ефектів від реалізації механізму за рівнями та часовими горизонтами.

Виклад основного матеріалу дослідження. Ефективне управління інноваційно-інформаційною складовою економічної безпеки підприємства потребує не лише якісної діагностики її стану, а й чіткого організаційного інструментарію, що перетворює аналітичні результати на конкретні управлінські дії. Запропонована концептуальна схема (рис. 1) ілюструє логіку такого механізму, структуровану у формі чотирьох взаємопов'язаних контурів управління, кожен з яких виконує специфічну функцію у загальному циклі забезпечення ІІЕБП.

Контур 1 «Діагностика» охоплює процедури кількісної оцінки рівня ІІЕБП на основі розроблеої автором методики CRITIC-DEMATEL (етап 1) та трансформації числових значень інтегрального індексу у якісні характеристики стану інноваційно-інформаційної складової економічної безпеки (етап 2). Така інтерпретація кількісних даних забезпечує перехід від абстрактних числових значень до конкретних управлінських рішень.

Контур 2 «Формування управлінського фокусу» дозволяє визначити одну з 5 стратегій в залежності від рівня ІІЕБП (етап 3) та сформувати відповідні заходи (етап 4). Цінність даного контуру полягає у формуванні специфічної для конкретного підприємства конфігурації управлінських пріоритетів замість універсальних рішень, що відповідає його поточному стану та характеру загроз. Також це дозволяє встановити один з 4 управлінських режимів залежно від рівня ІІЕБП, що визначає фундаментальну спрямованість управлінських дій.

Контур 3 «Реалізація та контроль» охоплює процеси практичного впровадження прийнятих управлінських рішень у межах визначеної стратегії ІІЕБП (етап 5) та аналіз ризиків, що можуть виникнути в процесі реалізації. Цей етап передбачає диференційовану реалізацію заходів за блоками.

Контур 4 «Аналіз та адаптація» реалізується через аналіз ефективності заходів, а також проведення адаптації за потреби (етап 6).

Важливим є і систематичний моніторинг внутрішніх та зовнішніх сигналів (етап 7). Після корекції система повертається до етапу 1, ініціюючи новий управлінський цикл.

Запропонований організаційно-економічний механізм управління ІІЕБП синтезує переваги системного підходу (цілісність, емерджентність), процесного (структурованість етапів, вимірюваність результатів) та ситуаційного (адаптивність до змін), що узгоджується з підходами, застосованими у дослідженнях [5; 7].

Ефективність організаційно-економічного механізму управління ІІЕБП можлива за чітко визначених відповідальних суб'єктів. Запропонована організаційна модель (рис. 2) ілюструє чотирирівневу ієрархічну структуру суб'єктів управління ІІЕБП.

Стратегічний рівень (Правління / Генеральний директор) відповідає за затвердження стратегічних цілей у сфері ІІЕБП, визначення управлінського режиму, встановлення цільових значень інтегрального індексу та включення управління ІІЕБП у корпоративну стратегію.

Координаційний рівень (Директор з економічної безпеки / CSO) забезпечує трансформацію стратегічних рішень у тактичні плани, координацію між функціональними підрозділами через матрицю RACI, моніторинг виконання та формування консолідованої звітності.

Аналітичний рівень (підрозділ стратегічного аналізу ризик-менеджменту) здійснює кількісну оцінку ІІЕБП за методикою CRITIC-DEMATEL, ідентифікацію загроз та підготовку аналітичних рекомендацій.

Виконавчий рівень представлений п'ятьма функціональними підрозділами (IT, інноваційні підрозділи, HR, служба безпеки, управлінські служби), кожен з яких відповідає за реалізацію заходів у межах відповідного блоку ІІЕБП та охоплюють ключові напрями забезпечення [4; 8].

Механізми горизонтальної координації між підрозділами реалізуються через міжфункціональні

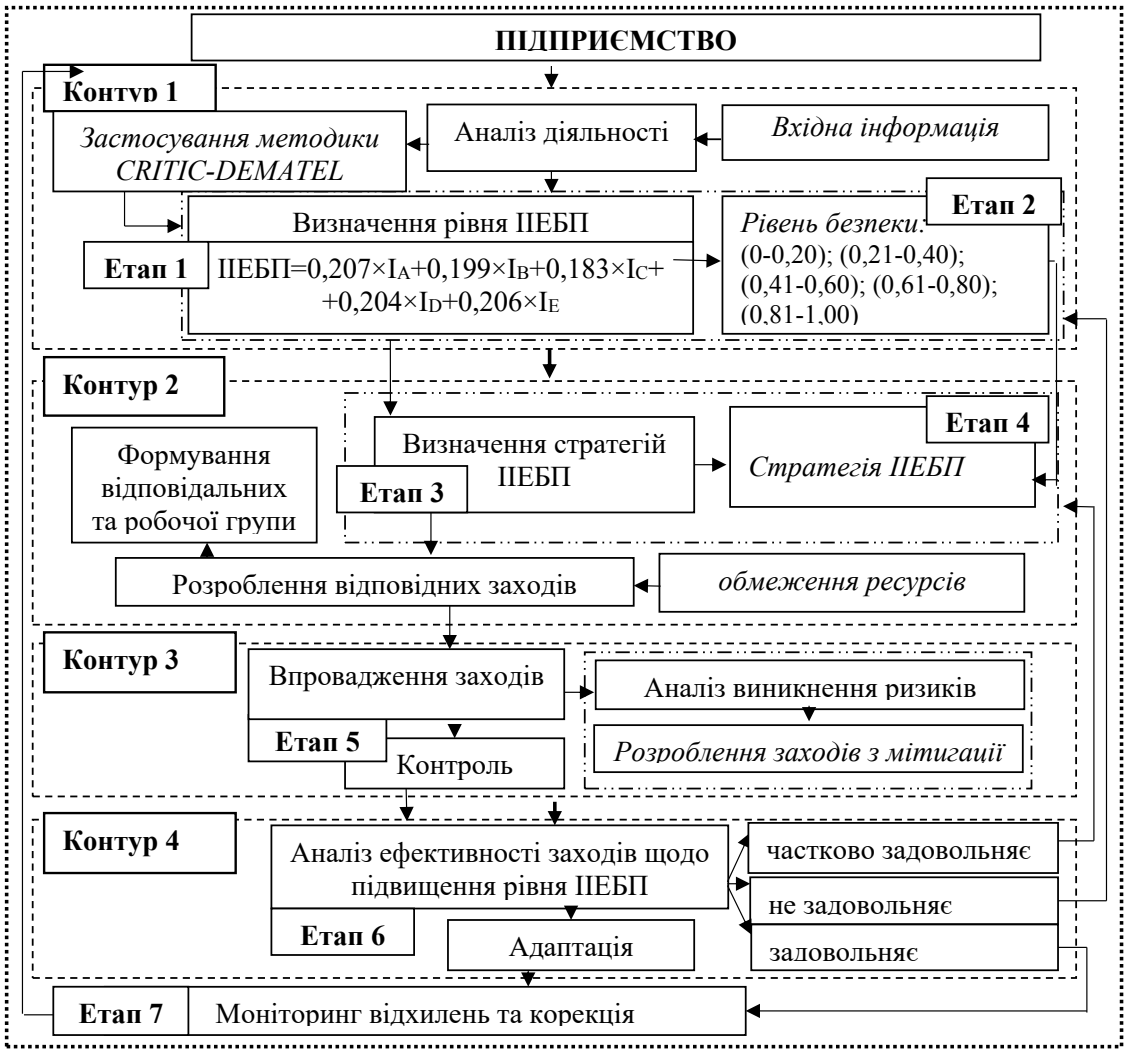

Рис. 1. Організаційно-економічний механізм управління ІІЕБП

Джерело: розроблено автором

робочі групи, спільні KPI для суміжних функцій та інтегровані інформаційні системи. Система зворотного зв'язку включає щотижневі звіти виконавчого рівня координаційному, щомісячні – координаційного стратегічному, щоквартальні звіти про результати оцінки ІІЕБ та сигнали про критичні відхилення у режимі реального часу.

Запропонована організаційна модель забезпечить чіткість розподілу управлінських ролей між рівнями ієрархії та функціональними підрозділами, специфікацію функцій та інструментів для кожного суб'єкта управління, а також формалізацію механізмів вертикальної та горизонтальної координації, що створює організаційну основу для ефективної реалізації концептуальної логіки управління ІІЕБП.

Завершальним елементом розробки організаційно-економічного механізму управління ІІЕБП виступає обґрунтування очікуваних управлінських ефектів від його впровадження. На відміну від традиційних підходів, що обмежуються оцінкою виключно економічних ефектів (фінансова вигода, ROI), запропонований підхід використовує багаторівневу систему ефектів, структуровану за рівнями управління (стратегічний, тактичний, операційний) та часовими горизонтами (довгострокові, середньострокові, короткострокові).

Концептуальна схема системи очікуваних управлінських ефектів представлена на рисунку 3.

На стратегічному рівні (2–3 роки) формується перехід від інтуїтивного до доказового управління ІІЕБП, керована траєкторія послідовного переходу між режимами та інтеграція управління ІІЕБП у корпоративну стратегію.

На тактичному рівні (6–18 місяців) досягається підвищення узгодженості дій функціональних підрозділів та зниження рівня системних ризиків – скорочення кількості критичних інцидентів безпеки на 30–50% та зростання частки превентивно нейтралізованих загроз до 60% і більше, що корелює з результатами досліджень інформаційної безпеки [9; 10].

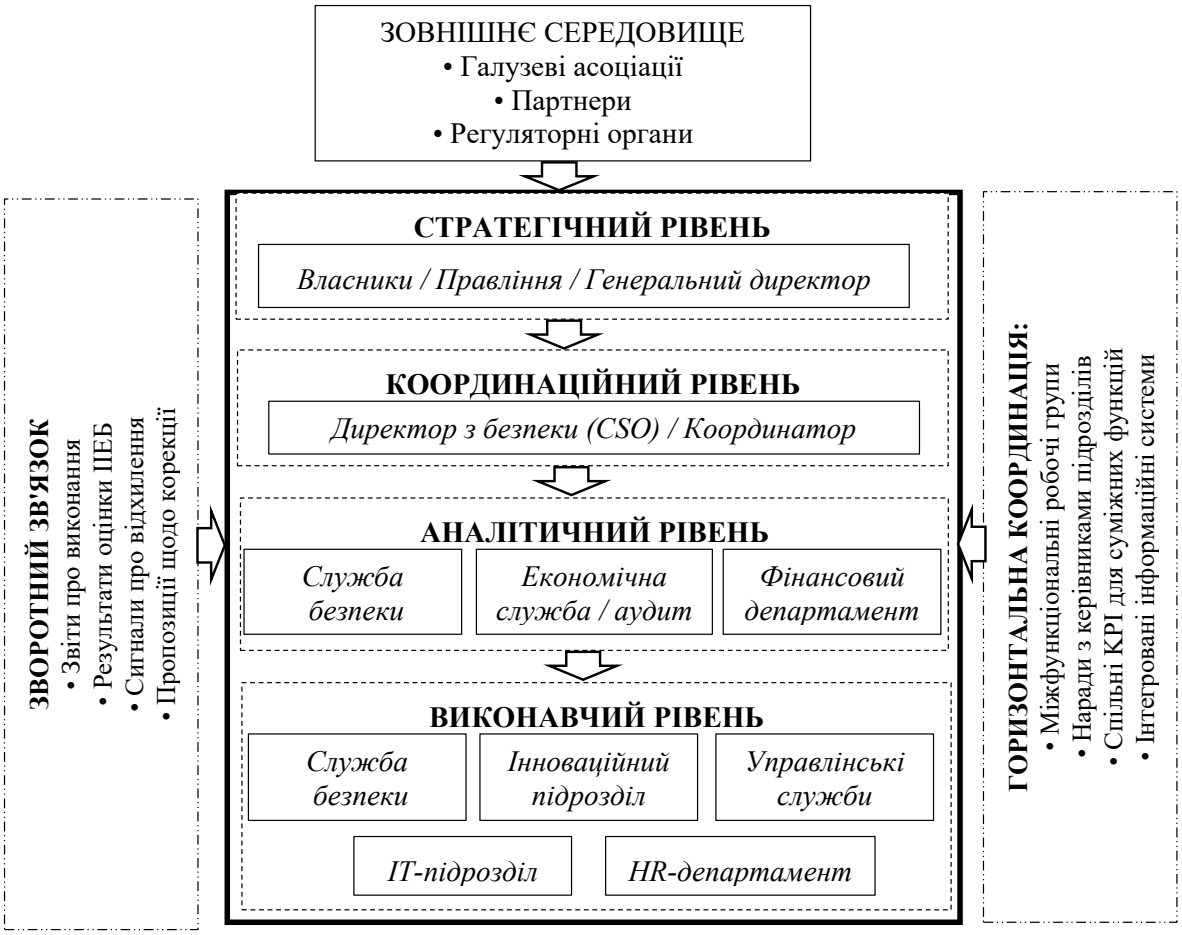

Рис. 2. Організаційна модель суб'єктів управління інноваційно-інформаційною складовою економічної безпеки підприємства

Джерело: розроблено автором

На операційному рівні (1–6 місяців) підвищується адаптивність до змін, оптимізується розподіл ресурсів на пріоритетні блоки (не менше 70%) та скорочується термін прийняття управлінських рішень.

Інтегративний ефект полягає у трансформації парадигми управління економічною безпекою – від реактивного до проактивного превентивного управління, від фрагментованих дій окремих підрозділів до системної скоординованої роботи всіх суб'єктів управління.

Загалом, запропонований організаційно-економічний механізм управління інноваційно-інформаційною складовою економічної безпеки підприємства формує основу для практичної реалізації стратегій нівелювання загроз ІІЕБП, що сприятиме зміцненню його конкурентних позицій та формуванню стійкості до зовнішніх і внутрішніх загроз в умовах цифрової трансформації економіки.

Висновки. У результаті проведеного дослідження сформовано цілісний організаційно-економічний механізм управління інноваційно-інформаційною складовою економічної безпеки підприємства, що усуває розрив між діагностикою стану системи та практичними управлінськими діями. Його впровадження створює передумови для формування стійкої та керованої системи безпеки підприємства в умовах мінливого зовнішнього середовища.

Разом з тим, дослідження має певні обмеження. Запропонований механізм розроблено як універсальну концептуальну модель, що потребує адаптації до галузевої специфіки підприємства, його розміру та організаційної зрілості. Крім того, ефективність механізму значною мірою залежить від наявності кваліфікованих фахівців, що може бути обмежуючим чинником для малих і середніх підприємств.

Перспективами подальших досліджень є апробація механізму на вибірці підприємств із різним рівнем ІІЕБП, розробка галузево-специфічних модифікацій організаційної моделі, а також формування системи диференційованих стратегій нівелювання загроз, адаптованих до кожного з п'яти рівнів економічної безпеки підприємства.

Рис. 3. Типологія управлінських ефектів реалізації організаційно-економічного механізму управління інноваційно-інформаційною складовою економічної безпеки підприємства

Джерело: розроблено автором

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Дейнега І., Пиртко М. Економічна безпека підприємства: зміна парадигми. *Цифрова економіка та економічна безпека*. 2025. № 4(19). С. 124–130. DOI: https://doi.org/10.32782/dees.19-19

2. Лєзіна А. Генеза розвитку дефініції «економічна безпека підприємства». *Сталий розвиток економіки*. 2024. № 2(49). С. 101–106. DOI: https://doi.org/10.32782/2308-1988/2024-49-16

3. Нам'ясенко В. Економічна безпека підприємства в умовах воєнного стану. *Економіка України*. 2025. № 6(763). С. 25–38. DOI: https://doi.org/10.15407/economyukr.2025.06.025

4. Рудніченко Є., Яремчук О., Гайдук О.А., Петяк А. Економічна безпека підприємства: теоретичні основи і сучасний погляд. *Development Service Industry Management*. 2024. № 4. С. 316–320. DOI: https://doi.org/10.31891/dsim-2024-8(47)

5. Гринько Т., Гвініашвілі Т., Бірюкова П. Інноваційна складова економічної безпеки підприємства. *Innovation and Sustainability*. 2024. № 2. С. 20–32. DOI: https://doi.org/10.31649/ins.2024.2.20.32

6. Малиш В., Самойлович О. Інноваційний розвиток як фактор забезпечення економічної безпеки промислових підприємств. *Проблеми і перспективи економіки та управління*. 2024. № 1(37). С. 81–89. DOI: https://doi.org/10.25140/2411-5215-2024-1(37)-81-89

7. Тульчинська С., Солосіч О., Чорній В. Вплив діджиталізації управлінських процесів на систему забезпечення економічної безпеки підприємства. *Інвестиції: практика та досвід*. 2021. № 9. С. 54–58. DOI: https://doi.org/10.32702/2306-6814.2021.9.54

8. Ковальчук А.М. Чинники стратегічного управління економічною безпекою підприємства в умовах змін. *Економічний вісник НТУУ «Київський політехнічний інститут»*. 2021. Вип. 18. С. 88–93. DOI: https://doi.org/10.20535/2307-5651.18.2021.247231

9. Мачак Т., Дубина О., Юрченко С. Інформаційне забезпечення управління системою економічної безпеки підприємства та його удосконалення. *Економіка та суспільство*. 2024. № 61. DOI: https://doi.org/10.32782/2524-0072/2024-61-66

10. Ситнік Є. Обґрунтування стратегії управління системою економічної безпеки підприємства на основі використання інноваційних цифрових технологій. *Сталий розвиток економіки*. 2025. № 5(56). С. 302–306. DOI: https://doi.org/10.32782/2308-1988/2025-56-41

REFERENCES:

1. Deineha I., Pyrtko M. (2025). Ekonomichna bezpeka pidpryiemstva: zmina paradyhmy [Economic security of an enterprise: a paradigm shift]. *Tsyfrova ekonomika ta ekonomichna bezpeka*, no. 4(19), pp. 124–130. DOI: https://doi.org/10.32782/dees.19-19

2. Liezina A. (2024). Heneza rozvytku definitsii «ekonomichna bezpeka pidpryiemstva» [Genesis of

the development of the definition "economic security of an enterprise"]. *Stalyi rozvytok ekonomiky*, no. 2(49), pp. 101–106. DOI: https://doi.org/10.32782/2308-1988/2024-49-16

3. Namiasenko V. (2025). Ekonomichna bezpeka pidpryiemstva v umovakh voiennoho stanu [Economic security of an enterprise under martial law]. *Ekonomika Ukrainy*, no. 6(763), pp. 25–38. DOI: https://doi.org/10.15407/economyukr.2025.06.025

4. Rudnichenko Ye., Yaremchuk O., Haiduk O.A., Petiak A. (2024). Ekonomichna bezpeka pidpryiemstva: teoretychni osnovy i suchasnyi pohliad [Economic security of an enterprise: theoretical foundations and modern perspective]. *Development Service Industry Management*, no. 4, pp. 316–320. DOI: https://doi.org/10.31891/dsim-2024-8(47)

5. Hrynko T., Hviniashvili T., Biriukova P. (2024). Innovatsiina skladova ekonomichnoi bezpeky pidpryiemstva [Innovation component of enterprise economic security]. *Innovation and Sustainability*, no. 2, pp. 20–32. DOI: https://doi.org/10.31649/ins.2024.2.20.32

6. Malysh V., Samoilovych O. (2024). Innovatsiinyi rozvytok yak faktor zabezpechennia ekonomichnoi bezpeky promyslovykh pidpryiemstv [Innovative development as a factor of ensuring economic security of industrial enterprises]. *Problemy i perspektyvy ekonomiky ta upravlinnia*, no. 1(37), pp. 81–89. DOI: https://doi.org/10.25140/2411-5215-2024- 1(37)-81-89

7. Tulchynska S., Solosich O., Chornii V. (2021). Vplyv didzhytalizatsii upravlinskykh protsesiv na systemu zabezpechennia ekonomichnoi bezpeky pidpryiemstva [The impact of digitalization of management processes on the enterprise economic security system]. *Investytsii: praktyka ta dosvid*, no. 9, pp. 54–58. DOI: https://doi.org/10.32702/2306-6814.2021.9.54

8. Kovalchuk A.M. (2021). Chynnyky stratehichnoho upravlinnia ekonomichnoiu bezpekoiu pidpryiemstva v umovakh zmin [Factors of strategic management of enterprise economic security in conditions of change]. *Ekonomichnyi visnyk NTUU «Kyivskyi politekhnichnyi instytut»*, no. 18, pp. 88–93. DOI: https://doi.org/10.20535/2307-5651.18.2021.247231

9. Machak T., Dubyna O., Yurchenko S. (2024). Informatsiine zabezpechennia upravlinnia systemoiu ekonomichnoi bezpeky pidpryiemstva ta yoho udoskonalennia [Information support for managing the enterprise economic security system and its improvement]. *Ekonomika ta suspilstvo*, no. 61. DOI: https://doi.org/10.32782/2524-0072/2024-61-66

10. Sytnik Ye. (2025). Obgruntuvannia stratehii upravlinnia systemoiu ekonomichnoi bezpeky pidpryiemstva na osnovi vykorystannia innovatsiinykh tsyfrovykh tekhnolohii [Substantiation of the management strategy of the enterprise economic security system based on the use of innovative digital technologies]. *Stalyi rozvytok ekonomiky*, no. 5(56), pp. 302–306. DOI: https://doi.org/10.32782/2308-1988/2025-56-41

Дата надходження статті: 20.02.2026
Дата прийняття статті: 09.03.2026
Дата публікації статті: 19.03.2026