УДК 658.5:[330.34:316.4]

І.В. Нестеренко[1]

СОЦІАЛЬНО-ЕКОНОМІЧНА БЕЗПЕКА ПІДПРИЄМСТВ В УМОВАХ КРИЗОВИХ ТРАНСФОРМАЦІЙ

[1]Національний авіаційний університет

Анотація: *Розглянуто теоретичні та практичні аспекти забезпечення соціально-економічної безпеки підприємств в умовах кризових трансформацій. Особливу увагу приділено антикризовим інноваційним стратегіям для підвищення економічної стабільності, ризик-менеджменту у сфері цифрових загроз (кібербезпеки) та формуванню екосистемного підприємництва як основи для створення мережі партнерств і спільного розвитку. Запропоновано рекомендації щодо мінімізації ризиків, підвищення інноваційного потенціалу та забезпечення стійкості підприємств до зовнішніх викликів.*

Ключові слова: соціально-економічна система, підприємство, інновації, кібербезпека, антикризові стратегії, ризик-менеджмент, екосистемне підприємництво.

Abstract. *The theoretical and practical aspects of ensuring the socio-economic security of enterprises under conditions of crisis transformations are examined. Particular attention is given to anti-crisis innovative strategies aimed at enhancing economic stability, risk management in the field of digital threats (cybersecurity), and the formation of ecosystem-based entrepreneurship as a foundation for creating partnership networks and fostering joint development. Recommendations are proposed for risk minimization, increasing innovation potential, and ensuring enterprise resilience to external challenges.*

Keywords: socio-economic systems, enterprise, innovations, cybersecurity, anti-crisis strategies, risk management, ecosystem-based entrepreneurship.

В умовах кризових трансформацій, викликаних економічними, соціальними, політичними й технологічними змінами, питання забезпечення соціально-економічної безпеки підприємств набуває особливої актуальності. Підприємства змушені шукати ефективні антикризові стратегії, розвивати ризик-менеджмент, підвищувати інноваційний потенціал та формувати екосистемні підходи до ведення бізнесу. Зростання цифрових загроз, зокрема кіберризиків, підкреслює важливість комплексного підходу до захисту інформаційної інфраструктури та збереження цілісності економічної діяльності. Ключовим завданням сьогодення стає пошук шляхів забезпечення соціально-економічної безпеки підприємств, що передбачає впровадження інновацій, оптимізацію управлінських процесів і зміцнення партнерських зв'язків для досягнення стійкості й розвитку навіть в умовах кризових викликів.

Теоретичні та практичні аспекти проблемних питань забезпечення соціально-економічної безпеки підприємств досліджували в своїх працях низка вітчизняних та зарубіжних вчених-економістів. Аналіз праць таких науковців, як Жураковська А., Лукашова Д., Павлов Р., Онищенко С., Глушко А., Кащена Н. дозволив виокремити особливості формування ефективних механізмів протидії кризовим явищам, адаптації до динамічних змін зовнішнього середовища та забезпечення стабільності функціонування бізнес-структур. Зокрема, дослідники акцентують увагу на важливості комплексного підходу до управління ризиками, впровадженні інноваційних технологій для підвищення стійкості підприємств та розвитку партнерських мереж як елемента екосистемного підприємництва [1, 2, 3]. Особливу увагу наукова спільнота приділяє ідентифікації ключових загроз соціально-економічній безпеці, серед яких виділяються фінансові ризики, цифрові загрози (кібербезпека), порушення ланцюгів постачання та нестабільність ринкового середовища [4]. Також акцентовано на важливості антикризових стратегій, що базуються на швидкій адаптації бізнес-процесів, інвестуванні у людський капітал та цифровій трансформації підприємств для забезпечення конкурентоспроможності в умовах кризових трансформацій [5]. Отже питання розробки й впровадження ефективних антикризових інструментів, удосконалення ризик-менеджменту та зміцнення соціально-економічної безпеки підприємств актуалізуються в сучасних умовах глобальних викликів, посилення економічної турбулентності та зростання залежності від цифрових технологій.

З огляду на динамічні зміни у зовнішньому середовищі та необхідність забезпечення стійкості підприємств, особливої уваги набувають підходи, що сприяють адаптації до викликів і підвищенню конкурентоспроможності. У цьому контексті ключову роль відіграють ефективні підходи до управління, серед яких особливе місце займають інноваційні стратегії. Основними інноваційними стратегіями є:

1. Диверсифікація діяльності - розширення асортименту продукції та вихід на нові ринки для зменшення залежності від окремих сегментів.

2. Цифровізація бізнес-процесів - використання сучасних технологій для автоматизації виробництва та оптимізації управління.

3. Впровадження принципів ESG - екологічна відповідальність, соціальна орієнтованість та ефективне корпоративне управління як засоби підвищення довіри інвесторів і споживачів.

4. Інноваційне лідерство - стимулювання внутрішніх інновацій та розвиток людського капіталу для підвищення конкурентоспроможності [6, с. 300].

Запровадження зазначених інноваційних стратегій не лише сприяє зростанню ефективності функціонування підприємств, а й забезпечує їхню стратегічну стійкість у контексті кризових трансформацій, що є критичним фактором для довготривалого розвитку в умовах нестабільного ринкового середовища. Високий рівень адаптивності до нових викликів, що супроводжується мінімізацією потенційних втрат, досягається через інтеграцію сучасних технологій управління та фінансової гнучкості. Однак у сучасній цифровій економіці, де значна частина операцій відбувається у віртуальному середовищі, особливого значення набуває система управління ризиками, орієнтована на виявлення, оцінку та нейтралізацію кіберзагроз. Впровадження ефективних механізмів кіберризик-менеджменту передбачає комплексний підхід, що включає не лише технологічні, а й організаційні та стратегічні аспекти захисту цифрової інфраструктури підприємств.

Ключовими елементами кіберризик-менеджменту є регулярний аудит інформаційної безпеки, який забезпечує виявлення та усунення вразливостей у системах підприємства, що дозволяє мінімізувати ймовірність несанкціонованого доступу до критичних даних. При цьому, важливим аспектом є навчання персоналу, яке сприяє підвищенню рівня цифрової грамотності співробітників та зниженню ризиків, пов'язаних із людським фактором у питаннях інформаційної безпеки. Використання багатофакторної аутентифікації є одним із найбільш ефективних інструментів запобігання несанкціонованому доступу до інформаційних систем, що забезпечує багаторівневий захист конфіденційної інформації. Розробка детальних планів реагування на кіберінциденти дозволяє підприємствам швидко й ефективно відновлювати функціонування після атак, мінімізуючи фінансові та репутаційні втрати. Водночас, інвестування в передові технології кіберзахисту, зокрема використання штучного інтелекту, машинного навчання та блокчейн-рішень, значно підвищує рівень стійкості підприємств до зовнішніх загроз, створюючи умови для їхньої безперервної цифрової трансформації. Отже, забезпечення кібербезпеки в умовах цифровізації є не лише технічним, а й стратегічним завданням, яке безпосередньо впливає на конкурентоспроможність підприємств та їхню стійкість у динамічному середовищі глобальної економіки.

Розширення механізмів ефективного ризик-менеджменту у сфері цифрових загроз є провідним чинником забезпечення безперервності бізнес-процесів, стабільності функціонування підприємств та підвищення рівня їхньої кіберстійкості. Однак, для досягнення довгострокової стійкості та формування конкурентних переваг недостатньо лише впровадження інструментів захисту. Доцільним є реалізація стратегічного підходу до трансформації бізнес-середовища, що включає створення нових моделей кооперації та розвитку, зокрема на засадах екосистемного підприємництва. У сучасних умовах цифрової економіки екосистемне підприємництво виступає як ефективний механізм інтеграції ресурсів, знань і технологій, що сприяє підвищенню адаптивності та інноваційного потенціалу підприємств.

Формування екосистемного підприємництва базується на створенні комплексної мережі взаємопов'язаних компаній, інституцій, стартапів, наукових установ та інших зацікавлених сторін, які співпрацюють задля досягнення спільних стратегічних цілей. Такий підхід забезпечує низку вагомих переваг, серед яких:

1. Оптимізація використання ресурсів – спільне застосування інфраструктури, капіталу та людських ресурсів сприяє зниженню трансакційних витрат та підвищенню ефективності виробничих і управлінських процесів.

2. Інноваційні партнерства – кооперація між підприємствами дозволяє прискорити процес розробки та впровадження інноваційних продуктів і послуг за рахунок обміну знаннями, доступу до передових технологій та використання гнучких форм фінансування.

3. Гнучкість і адаптивність – підприємства, що входять до екосистеми, мають можливість оперативно реагувати на ринкові зміни та адаптувати свої бізнес-моделі відповідно до актуальних викликів та можливостей.

4. Розширення ринкових можливостей – завдяки інтегрованому підходу підприємства отримують доступ до нових сегментів ринку, розширюють географію своєї присутності та підвищують рівень довіри серед споживачів.

5. Формування соціальної відповідальності – спільна діяльність учасників екосистеми сприяє розширенню корпоративної соціальної відповідальності, формуванню позитивного іміджу серед інвесторів та суспільства, що, у свою чергу, підвищує їхню стійкість на ринку [7].

Запровадження екосистемного підходу вимагає активної взаємодії з державними інституціями, науковими центрами, громадськими організаціями та міжнародними структурами для створення сприятливих умов розвитку. Державне стимулювання цифрової трансформації через податкові пільги, грантові програми та інституційні механізми підтримки значно посилює можливості підприємств щодо інтеграції в цифрову економіку. Водночас екосистемний підхід не лише зміцнює стійкість окремих підприємств, а й сприяє стабільному економічному зростанню загалом, зменшуючи ризики рецесії в умовах кризових трансформацій.

Таким чином, для забезпечення соціально-економічної безпеки підприємств в умовах кризових трансформацій доцільним є впровадження антикризових інноваційних стратегій, орієнтованих на підтримання макро- та мікроекономічної стабільності, диверсифікацію джерел фінансування та оптимізацію бізнес-процесів. Важливим аспектом є розвиток інтегрованого ризик-менеджменту у сфері цифрових загроз, що передбачає імплементацію протоколів кібербезпеки, використання систем штучного інтелекту для моніторингу кіберризиків та підвищення рівня інформаційної стійкості підприємств. Додатково необхідно стимулювати формування екосистемного підприємництва через розбудову стратегічних мереж партнерств, що сприятимуть синергетичному ефекту, інноваційній конвергенції та стійкому економічному зростанню.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Жураковська А., Лукашова Д., Павлов Р. Виклики та специфіка забезпечення економічної безпеки підприємства в кризових умовах. *Економіка та суспільство*. 2024, 68. DOI: https://doi.org/10.32782/2524-0072/2024-68-100
2. Онищенко С.В., Глушко А.Д. Аналітичний вимір кібербезпеки України в умовах зростання викликів та загроз. *Економіка і регіон*. 2022. № 1 (84). С. 13–20. DOI: https://doi.org/10.26906/EiR.2022.1(84).2540.
3. Kashchena N., Nesterenko I., Chmil H., Kovalevska N., Velieva V., Lytsenko O. Digitalization of Biocluster Management on Basis of Balanced Scorecard. *Journal of Information Technology Management*. 2023. Vol. 15. Is. 4. P. 80–96.
4. The Global Risks Report 2023. 18th Edition. World Economic Forum. Geneva, Switzerland. URL: https://www.weforum.org/reports/global-risks-report-2023/
5. Економічна безпека України в умовах довготривалої війни. Експертно-аналітична доповідь. К.: НІСД, 2024. 71 с. DOI: https://doi.org/10.53679/NISS-analytrep.2024.08
6. Нестеренко І.В. Детермінанти інноваційних трансформацій соціально-економічної системи підприємства. *Бізнес-навігатор*. 2024. Випуск 4 (77). С. 298-304. DOI: https://doi.org/10.32782/business-navigator.77-50
7. Соціальна відповідальність бізнесу в умовах війни. Marketer. URL: https://marketer.ua/social-responsibility-ofbusiness-in-conditions-of-war/

Нестеренко Ірина Володимирівна, кандидат економічних наук, доцент, докторант, Національний авіаційний університет, Київ, e-mail: inna0nesterenko@gmail.com.ua

Nesterenko Iryna V.- PhD, associate professor, Doctoral Candidate, National Aviation University, Kyiv, e-mail: inna0nesterenko@gmail.com.ua