УДК 338.24:004.9:351.86
DOI: https://doi.org/10.30838/EP.209.306-312

Семикіна М.В.
доктор економічних наук
Центральноукраїнський національний технічний університет
Semykina Maryna
Dr. of Economic Sc.
Central Ukrainian National Technical University
https://orcid.org/0000-0001-6995-1267

Дмитришин Б.В.
кандидат економічних наук
Центральноукраїнський національний технічний університет
Dmytryshyn Bohdan
PhD in Economic Sc.
Central Ukrainian National Technical University
https://orcid.org/0000-0002-9519-0104

Бугаєва М.В.
кандидат економічних наук
Центральноукраїнський національний технічний університет
Buhaieva Mariia
PhD in Economic Sc.
Central Ukrainian National Technical University
https://orcid.org/0000-0002-7460-9279

СТРАТЕГІЧНІ ІМПЕРАТИВИ ФУНКЦІОНУВАННЯ, БЕЗПЕКИ ТА ПОВОЄННОГО ВІДНОВЛЕННЯ ПІДПРИЄМСТВ ВИРОБНИЧОЇ ТА АГРАРНОЇ СФЕР В УМОВАХ ВОЄННИХ ЗАГРОЗ ТА ЦИФРОВИХ ВИКЛИКІВ

Статтю присвячено обґрунтуванню стратегічних пріоритетів у забезпеченні повоєнного відновлення підприємств реального сектору в умовах воєнних загроз та цифрових викликів. Розкрито специфіку функціонування виробничих та аграрних підприємств під час воєнного стану, визначено загрози. Обґрунтовано подвійну роль цифровізації: допомога у виживанні та адаптації бізнесу через хмарні сервіси, точне землеробство, автоматизацію та одночасне створення нових ризиків – кіберзагроз та енергозалежності. Виділено галузеві відмінності в стратегіях безпеки: дистанційний захист земель та врожаю в агросекторі та контроль обладнання в промисловості. Запропоновано концептуальне бачення повоєнного відновлення, засноване на чотирьох стратегічних імперативах: цифровій прозорості для залучення інвестицій, випереджальному управлінні ризиками, технологічній модернізації для енергетичної незалежності та розвитку цифрових компетенцій персоналу.

Ключові слова: *економічна безпека, повоєнне відновлення, аграрний сектор, виробнича сфера, цифрові виклики, воєнний стан, стратегічні імперативи, цифрова трансформація, кібербезпека, управління ризиками.*

STRATEGIC IMPERATIVES FOR FUNCTIONING, SECURITY, AND POST-WAR RECOVERY OF MANUFACTURING AND AGRICULTURAL ENTERPRISES UNDER MILITARY THREATS AND DIGITAL CHALLENGES

The article is devoted to substantiating strategic priorities in ensuring resilience and qualitative recovery of domestic real sector enterprises under the simultaneous impact of military threats and global digital transformation. Based on systematization of scientific sources and practical experience, the specifics of manufacturing and agricultural enterprises during martial law are revealed, and critical changes in the security environment are identified. The dual role of digitalization is substantiated: assisting business survival and adaptation through cloud services, precision agriculture,

ISSN друкованої версії: 2224-6282
ISSN електронної версії: 2224-6290

and automation, while simultaneously creating new risks – cyber threats and energy dependency. Sectoral differences in security strategies are highlighted: remote protection of land and harvest in the agricultural sector versus equipment control and process continuity in manufacturing. A conceptual vision for post-war recovery is proposed, based on four strategic imperatives: digital transparency to attract investments, proactive risk management, technological modernization for energy independence, and development of personnel's digital competencies. The research demonstrates that digital transformation, despite associated vulnerabilities, becomes a crucial driver of business adaptation and competitive advantage during reconstruction. Particular attention is paid to the integration of physical security measures with cyber protection mechanisms, ensuring comprehensive economic security. The article substantiates that enterprises succeeding in post-war recovery will be those capable of simultaneously addressing infrastructure restoration, technological modernization, and personnel development. The proposed strategic framework enables transformation of wartime challenges into opportunities for business modernization during post-war reconstruction. Implementation of identified imperatives requires coordinated efforts in three directions: infrastructure investment, cybersecurity infrastructure development, and human capital enhancement. The findings contribute to understanding economic security mechanisms in crisis conditions and provide practical guidance for enterprise management strategies during wartime and reconstruction periods.

Keywords: *economic security, post-war recovery, agricultural sector, manufacturing sector, digital challenges, martial law, strategic imperatives, digital transformation, cybersecurity, risk management.*

JEL classification: *F52, L21, O33, Q10.*

Постановка проблеми. В умовах затяжного воєнного конфлікту та перманентної нестабільності економічна безпека українських підприємств набуває екзистенційного значення, трансформуючись із допоміжної функції у ключову умову виживання. Для виробничої та аграрної сфер, які становлять фундамент реального сектору економіки України, ці виклики є особливо гострими: руйнування логістичних ланцюгів, фізичне знищення активів, енергетичний терор та кадровий дефіцит ставлять під загрозу не лише прибутковість, але й саме існування бізнесу. Водночас глобальний тренд на цифрову трансформацію створює нову реальність, де ігнорування цифрових інструментів загрожує втратою конкурентоспроможності, а їх впровадження пов'язане з новими кіберризиками.

У цьому контексті виникає нагальна потреба не лише у ситуативному реагуванні на загрози, а й у формуванні довгострокових стратегічних імперативів. Необхідно розробити механізми, які дозволять підприємствам не тільки зберегти потенціал під час війни, але й забезпечити ефективний «старт» для повоєнного відновлення, використовуючи цифровізацію як драйвер модернізації та підвищення прозорості. Пошук балансу між фізичним захистом, економічною ефективністю та цифровим розвитком вимагає переосмислення традиційних підходів до управління безпекою.

Аналіз останніх досліджень і публікацій. Проблематика стратегічного управління та економічної безпеки в умовах турбулентності є предметом ґрунтовних наукових пошуків. Фундаментальні засади формування стратегій виживання та розвитку закладені у класичних працях І. Ансоффа [12], П. Друкера [13] та М. Портера [14]. Їхні підходи залишаються актуальними, проте потребують адаптації до унікальних умов гібридних загроз сучасності.

Специфіку функціонування аграрного сектору під час війни ґрунтовно досліджують вітчизняні вчені. Зокрема, Ю. Білявська, Ю. Уманців, В. Осецький та В. Мамчур [1] аналізують тенденції розвитку агробізнесу в умовах воєнного стану, а О. Шульга фокусується на оцінці ефективності систем економічної безпеки в аграрній сфері [11].

Питання безпеки промислових підприємств та забезпечення їх стійкості висвітлено у роботах М. Міорошніченко [8], С. Тульчинської та Т. Ткаченко [9]. Комплексний підхід до безпеки реального сектору в контексті вартісно-орієнтованого управління розкрито у монографії С. Філиппової, Л. Волощук та С. Черкасової [10].

Вагомий внесок у дослідження цифрового виміру безпеки підприємств зробили Н. Євтушенко і Д. Стеценко [3], які розглядають виклики цифрової трансформації під час війни, а також А. Максименко [7] та І. Линда [6], які акцентують увагу на загрозах цифрової економіки. Фінансово-економічні аспекти безпеки в умовах діджиталізації аналізують Н. Демчишак, Р. Шевчук та К. Гоменюк [2]. Загальні стратегії адаптації бізнесу до воєнних реалій вивчають І. Козлова та ін. [5], А. Жураковська та ін. [4].

Попри значну кількість публікацій, більшість досліджень фокусується переважно на тактичному антикризовому управлінні або вузьких аспектах цифровізації. Поза увагою науковців залишається визначення стратегічних домінант цифрової трансформації для залучення інвестицій та відбудови зруйнованого війною потенціалу підприємств. Саме недостатня розробленість комплексних підходів до відновлення та безпеки реального сектору економіки на засадах поєднання збереження активів і цифрових технологій становить актуальну наукову проблему, що потребує вирішення.

Мета статті. З огляду на необхідність вирішення зазначеної проблеми, метою дослідження є обґрунтування стратегічних імперативів функціонування, забезпечення безпеки та повоєнного відновлення підприємств виробничої та аграрної сфер в умовах конвергенції воєнних загроз та цифрових викликів.

Для досягнення поставленої мети визначено такі завдання:

– ідентифікувати та систематизувати ключові загрози для підприємств реального сектору економіки, спричинені поєднанням воєнних дій та глобальних цифрових трендів;

– визначити специфіку впливу цифрової трансформації на механізми забезпечення економічної безпеки в аграрній та виробничій сферах;

– розробити стратегічні імперативи функціонування, відновлення та безпеки підприємств виробничої та аграрної сфер, що базуються на впровадженні інноваційних цифрових інструментів та проактивному управлінні ризиками.

Методи дослідження. Для вирішення окреслених завдань використано комплекс загальнонаукових методів дослідження: системно-структурний аналіз – для ідентифікації та систематизації гібридних загроз та їх наслідків, що виникають внаслідок воєнних дій і цифрових викликів (перше завдання); компаративний аналіз – для виявлення галузевих відмінностей впливу цифровізації на економічну безпеку підприємств аграрної та виробничої сфер (друге завдання); абстрактно-логічний метод – при обґрунтуванні стратегічних імперативів відновлення та проактивного управління ризиками (третє завдання); методи синтезу та групування – для систематизації стратегічних заходів, а також очікуваних ефектів.

Виклад основних результатів дослідження. Сучасний етап функціонування вітчизняних підприємств характеризується безпрецедентним накладанням двох потужних дестабілізуючих факторів: руйнівного впливу повномасштабної війни та імперативу прискореної цифрової трансформації. Як слушно зазначає А. Максименко [7], цифрова економіка, яка в мирний час є драйвером зростання, в умовах війни формує специфічне поле реальних та потенційних загроз. Для підприємств виробничої та аграрної сфер це створює ефект «подвійної вразливості»: фізичне знищення активів супроводжується кібератаками на цифрову інфраструктуру, що унеможливлює ефективне управління ресурсами.

Аналіз наукових джерел [4, 6, 8] дозволяє стверджувати, що ключовою проблемою стає не просто наявність ризиків, а їх гібридний характер. Традиційна класифікація загроз економічній безпеці (фінансові, кадрові, техніко-технологічні) потребує перегляду через призму цифрової вразливості. Зокрема, Н. Євтушенко та Д. Стеценко підкреслюють, що цифрова трансформація бізнесу під час війни – це не лише можливості, але й критичні виклики, пов'язані із захистом даних та стабільністю комунікаційних мереж [3].

На основі узагальнення наукової думки нами здійснено систематизацію ключових загроз для підприємств реального сектору економіки, які виникають внаслідок поєднання воєнних дій та цифрових трендів (табл. 1).

Таблиця 1

Систематизація загроз економічній безпеці підприємств виробничої та аграрної сфер в умовах воєнно-цифрової конвергенції

Група загроз	Характеристика загрози	Специфіка прояву у виробничій сфері	Специфіка прояву в аграрній сфері	Наслідки для економічної безпеки
Кіберфізичні	Знищення цифрової інфраструктури внаслідок ракетних обстрілів та енергетичного терору	Зупинка автоматизованих ліній, пошкодження серверного обладнання, втрата контролю над технологічним процесом	Втрата зв'язку з системами точного землеробства, неможливість моніторингу посівів (дрони, GPS), збої в роботі елеваторів	Втрата виробничого потенціалу, порушення безперервності бізнес-процесів
Інформаційно-комунікаційні	Кібератаки, шпигунство, витік конфіденційної інформації через цифрові канали	Викрадення конструкторської документації, креслень, баз даних клієнтів та постачальників, блокування ERP-систем	Маніпуляції з даними земельного кадастру, крадіжка інформації про обсяги врожаю та логістику експорту	Втрата інтелектуальної власності, репутаційні ризики, фінансові збитки
Кадрово-цифрові	Дефіцит персоналу з цифровими компетенціями на тлі міграції та мобілізації	Брак операторів верстатів з ЧПК, інженерів-програмістів, фахівців з кібербезпеки промислових мереж	Гостра нестача операторів агродронів, агрономів-аналітиків, фахівців з цифрового управління технікою	Зниження продуктивності праці, неможливість впровадження інновацій
Фінансово-інвестиційні	Блокування цифрових фінансових операцій, ризики інвестування в «цифру» в зоні ризику	Неможливість міжнародних транзакцій, замороження проєктів з цифровізації (Smart Factory) через брак обігових коштів	Проблеми з електронним кредитуванням під заставу врожаю, ризик втрати дороговартісної «розумної» техніки	Декапіталізація підприємств, інвестиційна пауза, криза ліквідності

Джерело: розроблено авторами на основі [, 2, 5, 7, 10, 11].

Особливої уваги потребує аналіз галузевих відмінностей у сприйнятті цих загроз.

Для *виробничої сфери* (промисловості) критичною є залежність від енергопостачання та стабільності Інтернет-з'єднання. Сучасне промислове обладнання інтегроване в єдині цифрові екосистеми (IoT). Як зазначають М. Мірошніченко [8] та С. Тульчинська, Т. Ткаченко [9], воєнний стан загострив проблему фізичної безпеки серверів: багато підприємств змушені були терміново мігрувати у хмарні середовища, що, у свою чергу, підвищило ризики доступу до даних третіх сторін. Порушення цифрових протоколів управління внаслідок кібератаки або фізичного пошкодження мереж в умовах воєнних реалій може призвести до техногенних аварій та повної зупинки виробничого циклу.

Для *аграрної сфери* спектр загроз має свою

специфіку, пов'язану з територіальною роззосередженістю активів. Ю. Білявська, Ю. Уманців, В. Осецький, В. Мамчур [1] вказують на те, що агробізнес стикається з проблемою замінованих полів, що унеможливлює використання наземної техніки, а заборона на польоти дронів у багатьох регіонах нівелює переваги технологій точного землеробства. Крім того, цифрові реєстри (наприклад, земельний кадастр) стають об'єктом маніпуляцій на тимчасово окупованих територіях, що створює загрозу втрати права власності на землю – головний актив аграріїв.

Окремий пласт загроз формується у площині *фінансово-економічної безпеки.* Як підкреслюють Н. Демчишак, Р. Шевчук та К. Гоменюк [2], впровадження вартісно-орієнтованого управління потребує точних даних у реальному часі. Однак в умовах війни інформаційні потоки часто порушуються або викривлюються, що призводить до прийняття помилкових управлінських рішень. І. Линда підкреслює [6], що цифрова трансформація економіки створює нові канали для фінансового шахрайства, які активізуються в періоди нестабільності.

Отже, ідентифіковані загрози загалом свідчать про те, що механічна імплементація цифрових інструментів без урахування воєнного контексту може не посилити, а, навпаки, послабити економічну безпеку підприємства. Це актуалізує необхідність переходу до розроблення адаптивних стратегій.

Між тим цифрові технології докорінно змінюють саму будову механізмів економічної безпеки. Вони переводять її із площини простого реагування на події у площину активного управління даними та вартістю бізнесу. Якщо раніше, згідно з класичними підходами менеджменту, викладеними зокрема у працях І. Ансоффа [12], П. Друкера [13], безпека трималася переважно на фізичній охороні та паперовому контролі, то сьогодні головним захисником стають комп'ютерні алгоритми. Однак, як показує аналіз джерел [5, 10], впровадження цих змін має свої особливості залежно від галузі.

У виробничій сфері цифровізація насамперед змінює технічні та виробничі підходи до безпеки.

По-перше, відбувається перехід від планових ремонтів до попереджувального обслуговування. Завдяки датчикам, що підключені до Інтернету, заводи можуть стежити за станом верстатів у реальному часі, що для промисловості життєво важливо [8], адже дозволяє уникнути раптових поломок, які під час війни можуть повністю зупинити підприємство.

По-друге, використання технологій «цифрових двійників» (точних віртуальних копій обладнання) дозволяє перевіряти стійкість виробництва до криз без ризику для реальних машин. Це створює новий інструмент антикризового управління: керівники можуть змоделювати ситуацію (наприклад, перебої з постачанням деталей) на комп'ютері та знайти рішення ще до того, як проблема виникне в цеху. Це узгоджується з ідеями М. Портера [14]: перемагає той, хто швидше пристосовується.

В аграрній сфері вплив нових технологій зосереджено на захисті ресурсів та землі. Сільське господарство сильно залежить від кліматичних умов, зміни погоди та займає великі площі, які важко контролювати завдяки фізичним зусиллям людей. В умовах війни, коли поля можуть бути замінованими або піддаватись ракетним обстрілам, традиційний огляд угідь часто стає практично неможливим.

Як вказують Ю. Білявська та співавтори [1], цифрові інструменти (супутникові знімки, електронні карти, дрони) стають чи не єдиним способом захистити земельні активи. Вони дозволяють:

- дистанційно стежити за станом посівів;
- прогнозувати майбутній врожай;
- виявляти крадіжки або пошкодження полів без виїзду людей на небезпечні території.

Дослідник О. Шульга, у свою чергу, справедливо додає, що цифровізація перевезень (відстеження вантажівок через супутник, електронні накладні) формує механізм *безпеки збуту* [11]. Це зменшує ризик втрати зерна дорогою до порту чи елеватора.

Спільним для обох сфер є оновлення підходів до *фінансово-економічної безпеки*. Згідно з дослідженнями Н. Демчишак, Р. Шевчука та К. Гоменюк [2], цифрові технології (великі дані, блокчейн) роблять рух грошей прозорим і дозволяють миттєво бачити, як кожне рішення впливає на вартість компанії. В умовах війни це дає змогу:

- швидко знаходити зайві витрати;
- надавати чесну звітність для інвесторів (що необхідно для отримання коштів на відбудову);
- автоматично дотримуватися правил і законів, уникаючи штрафів.

Проте є і зворотний бік. І. Линда попереджає: цифровізація робить безпеку залежною від комп'ютерних мереж [6]. Якщо раніше збій сервера був просто незручністю, то зараз це може означати зупинку заводу або втрату керування сільгосптехнікою.

Отже, цифрова трансформація не просто змінює робочі місця, додає нові пристрої, ґаджети, а й змінює саму логіку безпеки: у промисловості головним стає безперервність роботи механізмів завдяки віртуальному контролю, а в агросекторі – дистанційний нагляд за землею та врожаєм, коли фізичний доступ обмежений.

Повоєнне відновлення українських підприємств не може обмежуватися простим поверненням до довоєнного стану («як було»). Руйнування інфраструктури та зміни на світових ринках вимагатимуть пошуку нових технологічних рішень для прискореної відбудови економіки, вибору нових підходів в питаннях відновлення функціонування її виробничої та аграрної сфер. Як зазначають дослідники [5, 13], криза завжди відкриває нові можливості для якісного «стрибка» в економічному розвитку підприємств. Тому стратегія відновлення має будуватися на принципі «відбудувати краще», де цифрові технології мають стати фундаментом нової безпеки та ефективності.

Спираючись на проведений аналіз загроз та галузевої специфіки, ми визначили ключові стратегічні імперативи (табл. 2).

Таблиця 2

Стратегічні імперативи функціонування, відновлення та безпеки підприємств виробничої та аграрної сфер в умовах цифрових викликів

Стратегічний імператив	Зміст заходів відновлення та розвитку	Очікуваний ефект для економічної безпеки
Цифрова прозорість та інвестиційна відкритість	Впровадження єдиних цифрових систем управління (ERP); створення електронних паспортів активів; цифровізація звітності.	Залучення дешевих кредитів та грантів на відбудову; довіра міжнародних партнерів; унеможливлення внутрішніх крадіжок.
Випереджальне (проактивне) управління ризиками	Сценарне планування дій на випадок криз; створення цифрових копій даних (хмарні резерви); моніторинг ринків через великі дані.	Миттєве відновлення керованості після інцидентів; зниження збитків від коливання цін; збереження ключової інформації бізнесу.
Технологічна та енергетична автономність	Заміна старого обладнання на автоматизовані лінії; використання дронів замість наземної техніки (в агро); власна генерація енергії.	Зменшення залежності від дефіциту кадрів та електроенергії; безпечна робота на ризикових територіях; зниження собівартості.
Розвиток цифрових компетенцій персоналу	Навчання працівників роботі з новими програмами; впровадження правил кібергігієни; дистанційна робота для офісного персоналу.	Захист від кібератак через помилки людей; утримання цінних фахівців (навіть тих, хто виїхав); ріст продуктивності праці.

Джерело: розроблено авторами на основі [2-8, 10, 12]

З огляду розробленої таблиці, основними серед визначених імперативів є:

– по-перше, *цифрова прозорість для залучення інвестицій*. Головною проблемою після війни стане брак коштів. Міжнародні донори та інвестори вимагатимуть повної прозорості використання грошей. Паперова звітність вже не викликає довіри. Тому підприємствам необхідно переходити на цифрові системи обліку, які неможливо підробити, та відкривати дані про свої активи (наприклад, електронні карти полів або цифрові паспорти заводів);

– по-друге, *випереджальне управління ризиками.* Війна довела, що реагувати на проблему після її появи – занадто дорого. Стратегія має змістити акцент на передбачення. Це означає використання комп'ютерного моделювання для прорахунку різних варіантів розвитку подій (сценарне планування) та створення цифрових резервів даних, щоб бізнес міг відновити роботу за лічені години після будь-якого інциденту;

– по-третє, *технологічна модернізація виробничої бази.* Відновлювати зруйновані цехи зі старим, енергоємним обладнанням немає сенсу. Нова техніка має бути енергоощадною та автоматизованою, щоб зменшити залежність від персоналу та блекаутів. Для аграріїв це означає використання безпілотної техніки на територіях, де є ризик замінування.

Реалізація цих імперативів дозволить українським підприємствам трансформувати виклики війни та цифровізації у конкурентні переваги на етапі повоєнного відновлення. Розвиток цифрових компетенцій персоналу має супроводжувати реалізацію усіх запланованих заходів.

Висновки. Проведене дослідження дозволило сформувати стратегічне бачення розвитку та відновлення підприємств реального сектору економіки в умовах війни. Основні результати роботи полягають у наступному:

✓ *По-перше,* систематизовано загрози, що виникли через поєднання бойових дій та стрімкого розвитку цифрових технологій. Доведено, що сучасні підприємства стикаються з подвійним викликом: фізичне руйнування майна посилюється ризиками кібератак та втрати даних. Це вимагає зміни підходів до безпеки, де захист комп'ютерних мереж стає таким же важливим, як і фізична охорона заводів чи складів.

✓ *По-друге*, визначено особливості впливу нових технологій на безпеку в різних галузях. Встановлено, що для промисловості головним завданням є безперервність роботи завдяки дистанційному контролю стану обладнання, що дозволяє уникнути аварій. Для аграрного сектору цифрові інструменти (супутникові знімки, дрони) стають головним засобом нагляду за полями та врожаєм, особливо там, де доступ людей обмежений через міни або обстріли.

✓ *По-третє,* запропоновано засади стратегії повоєнного відновлення підприємств виробничої та аграрної сфер, яка передбачає не просто відбудову старого, а якісне оновлення бізнесу. Обґрунтовано необхідність переходу до нової моделі управління, що спирається на такі принципові вимоги: повна прозорість діяльності для отримання інвестицій; вміння передбачати ризики, а не лише реагувати на них; оновлення техніки для енергонезалежності; навчання персоналу цифровим навичкам.

Перспективи подальших досліджень полягають у розробці конкретних сценаріїв відновлення (оптимістичного, реалістичного та песимістичного) для підприємств різних регіонів України, а також у створенні методики оцінки їхньої готовності до впровадження запропонованих цифрових інструментів безпеки.

Список використаних джерел:

1. Biliavska, Y., Umantsiv, Y., Osetskyi, V., & Mamchur, V. (2025). Trends in the development of Ukrainian agribusiness in the conditions of martial law. Ekonomika APK, No. 5. Iss. 32. Pp. 48–62. DOI: https://doi.org/10.32317/ekon.apk/5.2025.48
2. Демчишак Н.Б., Шевчук Р.С., Гоменюк К.В. (2025). Цифрові технології та інструменти забезпечення фінансової безпеки підприємств у контексті вартісно-орієнтованого управління. Економіка та суспільство, Вип. 73. DOI: https://doi.org/10.32782/2524-0072/2025-73-53
3. Євтушенко Н.М., Стеценко Д.І. (2024). Цифрова трансформація бізнесу в умовах війни в Україні: виклики та можливості. Економічний простір, № 191. С. 211–216. DOI: https://doi.org/10.32782/2224-6282/191-34
4. Жураковська А., Лукашова Д., Павлов Р. (2024). Виклики та специфіка забезпечення економічної безпеки підприємства в кризових умовах. Економіка та суспільство, № 68. DOI: https://doi.org/10.32782/2524-0072/2024-68-100
5. Козлова І.М., Велика О.Ю., Козлов Н.В. (2023). Особливості стратегічного розвитку підприємств в умовах воєнного стану. Бізнес Інформ, № 5. С. 134–140. DOI: https://doi.org/10.32983/2222-4459-2023-5-134-140
6. Линда І.С. (2025). Нові виклики та загрози цифрової трансформації економіки для системи фінансово-економічної безпеки підприємництва. Академічні візії, Вип. 50. DOI: https://doi.org/10.5281/zenodo.17909029
7. Максименко А.П. (2023). Реальні та потенційні загрози цифрової економіки в умовах війни. Економічний простір, № 188. С. 41–49. DOI: https://doi.org/10.32782/2224-6282/188-7
8. Мірошніченко М.В. (2025). Економічна безпека промислової галузі як ключовий елемент економічної безпеки національної економіки. Економічний простір, № 206. С. 244–250. DOI: https://doi.org/10.30838/EP.206.244-250
9. Тульчинська С., Ткаченко Т. (2023). Принципи системи економічної безпеки промислових підприємств в умовах конкуренції. Вісник Хмельницького національного університету. Економічні науки, № 3. С. 226–230. DOI: https://doi.org/10.31891/2307-5740-2023-318-3-35
10. Філиппова С.В., Волощук Л.О., Черкасова С.О. (2015). Економічна безпека підприємств реального сектору економіки в умовах вартісно-орієнтованого управління : монографія. Одеса : ФОП Бондаренко М.О., 196 с. URL: https://economics.net.ua/files/scientific-base/monogr/filippova_voloschuk_cherkasova_2015.pdf
11. Шульга О. (2025). Оцінка ефективності системи управління економічною безпекою аграрного сектора національної економіки. Економіка та суспільство, № 81. DOI: https://doi.org/10.32782/2524-0072/2025-81-4
12. Ansoff, H.I. (2007). Strategic Management. Classic Edition. London : Palgrave Macmillan. DOI: https://doi.org/10.1057/9780230590601
13. Drucker, P.F. (2012). Managing in Turbulent Times. New York : Routledge. 252 p. DOI: https://doi.org/10.4324/9780080938158
14. Porter, M.E. (1990). Competitive Strategy : Techniques for Analyzing Industries and Competitors. New York : Free Press. URL: http://ijevanlib.ysu.am/wp-content/uploads/2023/02/Michael-E.-Porter-Competitive-Strategy.pdf

References:

1. Biliavska, Y., Umantsiv, Y., Osetskyi, V., & Mamchur, V. (2025). Trends in the development of Ukrainian agribusiness in the conditions of martial law. Ekonomika APK, No. 5. Iss. 32. Pp. 48–62. DOI: https://doi.org/10.32317/ekon.apk/5.2025.48 [in English].
2. Demchyshak, N.B., Shevchuk, R.S., & Homeniuk, K. V. (2025). Tsyfrovi tekhnolohii ta instrumenty zabezpechennia finansovoi bezpeky pidpryiemstv u konteksti vartisno-oriientovanoho upravlinnia [Digital technologies and tools for ensuring financial security of enterprises in the context of value-oriented management]. Economy and society, No. 73. DOI: https://doi.org/10.32782/2524-0072/2025-73-53 [in Ukrainian].
3. Yevtushenko, N.M., & Stetsenko, D.I. (2024). Tsyfrova transformatsiia biznesu v umovakh viiny v Ukraini: vyklyky ta mozhlyvosti [Digital transformation of business in wartime in Ukraine: challenges and opportunities]. Economic space, No. 191. Pp. 211–216. DOI: https://doi.org/10.32782/2224-6282/191-34 [in Ukrainian].
4. Zhurakovska, A., Lukashova, D., & Pavlov, R. (2024). Vyklyky ta spetsyfika zabezpechennia ekonomichnoi bezpeky pidpryiemstva v kryzovykh umovakh [Challenges and specifics of ensuring economic security of an enterprise in crisis conditions]. Economy and society, No. 68. DOI: https://doi.org/10.32782/2524-0072/2024-68-100 [in Ukrainian].
5. Kozlova, I.M., Velyka, O.Yu., & Kozlov, N.V. (2023). Osoblyvosti stratehichnoho rozvytku pidpryiemstv v umovakh voiennoho stanu [Features of strategic development of enterprises under martial law]. Business Inform, No. 5. Pp. 134–140. DOI: https://doi.org/10.32983/2222-4459-2023-5-134-140 [in Ukrainian].
6. Lynda, I.S. (2025). Novi vyklyky ta zahrozy tsyfrovoi transformatsii ekonomiky dlia systemy finansovo-ekonomichnoi bezpeky pidpryiemnytstva [New challenges and threats of digital transformation of the economy for the system of financial and economic security of entrepreneurship]. Academic visions, No. 50. DOI: https://doi.org/10.5281/zenodo.17909029 [in Ukrainian].
7. Maksymenko, A.P. (2023). Realni ta potentsiini zahrozy tsyfrovoi ekonomiky v umovakh viiny [Real and potential threats of the digital economy in wartime]. Economic space, No. 188. Pp. 41–49.

DOI: https://doi.org/10.32782/2224-6282/188-7 [in Ukrainian].

8. Miroshnichenko, M.V. (2025). Ekonomichna bezpeka promyslovoi haluzi yak kliuchovyi element ekonomichnoi bezpeky natsionalnoi ekonomiky [Economic security of the industrial industry as a key element of the economic security of the national economy]. Economic space, No. 206. Pp. 244–250. DOI: https://doi.org/10.30838/EP.206.244-250 [in Ukrainian].

9. Tulchynska, S., & Tkachenko, T. (2023). Pryntsypy systemy ekonomichnoi bezpeky promyslovykh pidpryiemstv v umovakh konkurentsii [Principles of the economic security system of industrial enterprises in competitive conditions]. Bulletin of Khmelnytskyi National University. Economic Sciences, No. 3. Pp. 226–230. DOI: https://doi.org/10.31891/2307-5740-2023-318-3-35 [in Ukrainian].

10. Filyppova, S.V., Voloshchuk, L.O., & Cherkasova, S.O. (2015). Ekonomichna bezpeka pidpryiemstv realnoho sektoru ekonomiky v umovakh vartisno-oriientovanoho upravlinnia [Economic security of real sector enterprises in conditions of value-oriented management] : monograph. Odesa: FOP Bondarenko M.O. Retrieved from: https://economics.net.ua/files/scientific-base/monogr/filippova_voloschuk_cherkasova_2015.pdf [in Ukrainian].

11. Shulha, O. (2025). Otsinka efektyvnosti systemy upravlinnia ekonomichnoiu bezpekoiu ahrarnoho sektora natsionalnoi ekonomiky [Assessment of the effectiveness of the economic security management system of the agricultural sector of the national economy]. Economy and society, No. 81. DOI: https://doi.org/10.32782/2524-0072/2025-81-4 [in Ukrainian].

12. Ansoff, H.I. (2007). Strategic Management (Classic Edition). Palgrave Macmillan. DOI: https://doi.org/10.1057/9780230590601 [in English].

13. Drucker, P.F. (2012). Managing in Turbulent Times. Routledge. DOI: https://doi.org/10.4324/9780080938158 [in English].

14. Porter, M.E. (1980). Competitive Strategy: Techniques for Analyzing Industries and Competitors. Free Press. Retrieved from: https://www.hbs.edu/faculty/Pages/item.aspx?num=195 [in English].

Дата надходження статті: 05.01.2026 р.
Дата прийняття статті до друку: 26.01.2026 р.