DOI: https://doi.org/10.32782/2524-0072/2026-83-23

УДК 330.342.24:338.246.027

УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ ТА МІНІМІЗАЦІЯ ВОЄННИХ РИЗИКІВ ПІДПРИЄМСТВ РЕАЛЬНОГО СЕКТОРУ ЕКОНОМІКИ В УМОВАХ ЦИФРОВИХ ЗМІН

MANAGEMENT OF ECONOMIC SECURITY AND MINIMIZATION OF WAR RISKS FOR REAL SECTOR ENTERPRISES IN THE CONDITIONS OF DIGITAL CHANGES

Семикіна Марина Валентинівна
доктор економічних наук, професор,
Центральноукраїнський національний технічний університет
ORCID: https://orcid.org/0000-0001-6995-1267

Сторожук Оксана Василівна
кандидат економічних наук, доцент,
Центральноукраїнський національний технічний університет
ORCID: https://orcid.org/0000-0002-9450-7704

Савеленко Григорій Володимирович
кандидат технічних наук, доцент,
Центральноукраїнський національний технічний університет
ORCID: https://orcid.org/0000-0001-9310-6223

Semykina Maryna, Storozhuk Oksana, Savelenko Hryhorii
Central Ukrainian National Technical University

Стаття спрямована на теоретико-методологічне обґрунтування системи управління економічною безпекою підприємств реального сектору економіки та розробку методичних підходів до мінімізації воєнних ризиків на основі інструментів цифрової трансформації. Уточнено сутність поняття «економічна безпека підприємства в умовах цифрових змін» та здійснено класифікацію специфічних воєнних ризиків за джерелом виникнення, об'єктом впливу та цифровим аспектом реалізації. Виявлено їх негативний вплив на операційну ефективність та вартість активів аграрних і промислових підприємств. Обґрунтовано інтегровано-адаптивний методологічний підхід до забезпечення безпеки, який базується на системному поєднанні традиційних методів фізичного захисту та новітніх цифрових технологій з дотриманням принципу економічної доцільності. Розроблено структурно-функціональний механізм мінімізації воєнних ризиків, що інтегрує цільову, діагностичну, організаційно-виконавчу, ресурсно-фінансову та контрольно-адаптивну підсистеми в єдиному цифровому середовищі підприємства. Визначено взаємозв'язки між елементами механізму та цифровими інструментами (IoT, Big Data, цифрові двійники), що дозволяє перейти від ситуативного реагування до системного управління стійкістю та збереження інвестиційної привабливості бізнесу.

Ключові слова: економічна безпека підприємства, воєнні ризики, реальний сектор економіки, аграрні підприємства, промислово-виробничі підприємства, цифрова трансформація, методологічний підхід, принцип економічної доцільності, структурно-функціональний механізм, стійкий розвиток.

The article is aimed at substantiating the theoretical and methodological foundations of the economic security management system of real sector enterprises and developing methodological approaches to minimizing military risks based on digital transformation tools. The essence of the concept of "economic security of an enterprise in the context of digital changes" is clarified. A classification of military risks is proposed. It is distinguished by the differentiation of threats by source (kinetic, infrastructure), object of influence (human and financial capital) and digital aspect (cybernetic, information and reputational). This ensures the completeness of identification of destructive influences. A well-founded integrated-adaptive methodological approach to ensuring the economic

security of enterprises combines traditional tools for protecting assets with modern digital technologies. Its structure covers three levels of integration: monitoring and identifying threats, protection and neutralization, as well as making management decisions based on big data analytics. It combines physical means of protection and digital risk management tools. Formalization of the principle of economic feasibility ensures optimal use of resources and the transition from situational response to systemic management of sustainability. The advantage of the approach is the reduction of transaction costs and minimization of the opportunity cost of resources. This is especially important for agricultural and industrial enterprises. A structural and functional mechanism for minimizing military risks has been developed, which integrates the target, diagnostic, organizational and executive, resource and financial and control and adaptive subsystems within a single digital environment of the enterprise. The relationships between the elements of the mechanism and digital tools (IoT, Big Data, Digital Twins) have been determined, which allows the transition from situational response to systemic sustainability management and the preservation of the investment attractiveness of the business.

Keywords: enterprise economic security, war risks, real sector of the economy, agricultural enterprises, industrial and production enterprises, digital transformation, methodological approach, principle of cost-benefit efficiency, structural-functional mechanism, sustainable development.

Постановка проблеми. В умовах тривалої воєнної агресії забезпечення економічної безпеки підприємств реального сектору набуває ознак фундаментальної наукової проблеми, що потребує переосмислення крізь призму теорії ризиків та ефективності розподілу обмежених ресурсів. Порушення сталості логістичних потоків, руйнування виробничої інфраструктури та значна невизначеність зовнішнього середовища зумовлюють економічну неефективність класичних детермінованих підходів до управління безпекою. Цифрова трансформація економіки актуалізує потребу у формуванні нового методологічного підґрунтя для управління ризиками аграрних та промислово-виробничих підприємств, що дозволить переходити від витратних реактивних моделей до економічно обґрунтованих проактивних систем захисту. Проте відсутність цілісної теорії, яка б пов’язувала цифрові інструменти з показниками економічної ефективності діяльності підприємств в умовах воєнних загроз, гальмує розробку дієвих методик збереження капіталу та відновлення потенціалу реального сектору.

Аналіз останніх досліджень і публікацій. Проблемам економічної безпеки підприємств присвячено багато праць зарубіжних та вітчизняних учених. Методологічне підґрунтя стратегічного зміцнення економічної безпеки підприємств в умовах змін ринкового середовища сформували класики менеджменту І. Ансофф, П. Друкер та М. Портер [13-15]. В Україні методології забезпечення економічної безпеки підприємств реального сектору економіки присвятили свої праці Філиппова С., Волощук Л., Черкасова С. [11]. Аспекти економічної безпеки аграрних та виробничо-промислових підприємств в умовах загроз знаходяться в полі зору Білявської Ю. [1], Жураковської А. [4], Козлової І. [5], Нижник О. [9], Тульчинської С. [10]. Методи оцінки ефективності управління економічною безпекою висвітлює у своїх публікаціях Шульга О. [12]. Демчишак Н., Стеценко Д., Линда І., Максименко А. зосереджують увагу на цифрових викликах бізнесу в умовах війни [2; 3; 6; 7].

Водночас більшість публікацій зосереджена або на макроекономічних аспектах безпеки, або на галузевій специфіці, залишаючи поза увагою питання методологічного синтезу безпекової діяльності та цифрових технологій. Існує певний розрив між теоретичними моделями безпеки та економічними розрахунками доцільності їх реалізації, що вимагає поглибленого наукового пошуку.

Виділення невирішених раніше частин загальної проблеми. Попри значний науковий інтерес до проблематики, недостатньо розробленими залишаються теоретико-методологічні аспекти інтеграції цифрових інструментів у систему управління економічною безпекою з позицій оцінки їх економічної ефективності. Бракує наукового обґрунтування принципів, які б дозволили систематизувати воєнні ризики та визначити кореляцію між витратами на цифровізацію та рівнем збереження економічного потенціалу підприємства. Актуальною є потреба у формуванні методологічного підходу до побудови адаптивних систем безпеки, що базуються на раціональному використанні ресурсів та аналітиці даних.

Формулювання цілей статті (постановка завдання). Мета статті полягає в теоретико-методологічному обґрунтуванні системи управління економічною безпекою підприємств реального сектору економіки та розробці методичних підходів до мінімізації воєнних ризиків на основі інструментів цифрової трансформації.

Для досягнення поставленої мети визначено такі завдання:

– розкрити сутність поняття «економічна безпека підприємства в умовах цифрових змін», уточнивши класифікацію воєнних ризиків та їх вплив на операційну ефективність і вартість активів підприємств реального сектору;

– обґрунтувати методологічний підхід до забезпечення економічної безпеки, який базується на системній інтеграції традиційних методів захисту та новітніх цифрових технологій з дотриманням принципу економічної доцільності;

– розробити структурно-функціональний механізм мінімізації воєнних ризиків, визначивши взаємозв'язки між його елементами та цифровим середовищем підприємства для гарантування стійкого економічного розвитку.

Виклад основного матеріалу дослідження. Дослідження проблематики забезпечення стійкості підприємств реального сектору в умовах цифрових змін та перманентної воєнної загрози вимагає першочергового уточнення категоріального апарату. Класичні парадигми безпеки, сформовані в умовах відносної стабільності ринків, зазнають фундаментальних трансформацій під тиском екстремальних зовнішніх чинників.

Базис стратегічної адаптації підприємств до нестабільного середовища обґрунтували у своїх дослідженнях такі визнані вчені, як І. Ансофф, П. Друкер і М. Портер [13; 14; 15]. Спираючись на цей теоретичний фундамент, еволюція наукової думки демонструє зміну підходів до визначення сутності категорії «економічна безпека підприємства» в контексті конкурентного середовища. Доречно підкреслити, що у 90-ті роки XX ст. та на початку XXI ст. економічна безпека ототожнювалася переважно зі станом захищеності від зовнішніх загроз. Такий «статичний» підхід, представлений у працях ранніх дослідників, фокусувався на захисних функціях та збереженні комерційної таємниці. Згодом, із поглибленням ринкових відносин, науковий дискурс змістився у бік ресурсно-функціонального підходу. Вчені, зокрема Філиппова С., Волощук Л., Черкасова С., почали розглядати економічну безпеку в контексті вартісно-орієнтованого управління [11]. В цьому ж напрямі нині працюють Демчишак Н., Шевчук Р. С., Гоменюк К., проте з урахуванням цифрових інструментів та викликів [2].

Сучасний розвиток наукових поглядів відображає перехід від розуміння безпеки як «стану» до її сприйняття як «динамічної спроможності» до розвитку в умовах викликів та загроз. Такого підходу дотримуються Євтушенко Н., Линда І., Максименко А., Тульчинська С. та інші дослідники, акцентуючи увагу на адаптивності, гнучкості системи управління підприємства, здатності до змін в умовах конкуренції, ризиків та воєнних загроз [6; 7; 8; 10]. Розвиваючи цей напрям, Демчишак Н., Стеценко Д., Линда І., Максименко А. та інші науковці зосереджують увагу на трансформації механізмів управління економічною безпекою, визначаючи цифрові інструменти як дієвий засіб мінімізації ризиків бізнесу [2; 3; 6; 7].

Разом з тим, виходимо з того, що більшість існуючих в літературі дефініцій не враховують специфіку гібридної війни, де фізичне знищення активів поєднується з кібернетичними атаками, а також не відображають роль цифрової трансформації як інструменту виживання. Тому, базуючись на системно-синергетичному підході, пропонуємо таке авторське визначення: економічна безпека підприємства в умовах цифрових змін – це інтегрована характеристика системи управління, що відображає здатність суб'єкта господарювання зберігати цілісність активів та генерувати вартість в умовах воєнних загроз шляхом проактивної ідентифікації ризиків та їх нівелювання з використанням цифрових технологій.

Розуміння сутності економічної безпеки неможливе без деталізації категорії «ризик», оскільки саме наявність ризиків є передумовою формування системи безпеки. В умовах воєнного стану традиційна класифікація економічних ризиків (ринкові, кредитні, операційні) втрачає свою вичерпність. Воєнні ризики набувають статусу домінантних, поглинаючи та видозмінюючи класичні види загроз.

Враховуючи багатоаспектну природу сучасних викликів (поєднання фізичних загроз війни та віртуальних загроз цифрового простору), доцільно уточнити класифікацію воєнних ризиків та їх вплив на параметри діяльності підприємств реального сектору (таблиця 1).

Таким чином, ефективне управління економічною безпекою в сучасних умовах вимагає переходу від фрагментарного реагування на окремі загрози до побудови комплексної системи, здатної ідентифікувати та мінімізувати наведені групи ризиків, використовуючи потенціал цифрових інструментів.

Ідентифікація та класифікація воєнних ризиків засвідчує, що в сучасних умовах покладання виключно на традиційні методи фізичного та адміністративного захисту є еко-

Таблиця 1

Систематизація та класифікація воєнних ризиків підприємств реального сектору економіки в умовах цифрових змін

Критерій класифікації	Вид ризику	Сутність та особливості прояву (вплив на активи та ефективність)
За джерелом виникнення (генезис)	Кінетичні (фізичні) ризики	Пряме руйнування основних фондів, складської інфраструктури та товарних запасів внаслідок бойових дій. Призводить до миттєвої втрати вартості активів.
	Інфраструктурні ризики	Порушення енергопостачання та логістичних ланцюгів. Збільшує операційні витрати (собівартість) та знижує маржинальність виробництва.
За об’єктом впливу	Ризики людського капіталу	Втрата персоналу через мобілізацію та міграцію. Знижує продуктивність праці та інтелектуальний потенціал підприємства.
	Ризики фінансової стійкості	Дефіцит обігових коштів, валютні коливання, ускладнення доступу до кредитування. Призводить до касових розривів та загрози банкрутства.
За середовищем реалізації (цифровий аспект)	Кібернетичні ризики воєнного часу	Спрямовані атаки на цифрову інфраструктуру (ERP-системи, бази даних) з метою паралізації управління або шпигунства.
	Інформаційно-репутаційні ризики	Дезінформаційні кампанії, маніпуляції даними для підриву довіри партнерів та споживачів. Впливає на нематеріальні активи (гудвіл).

Джерело: сформовано на основі [3-7] та аналізу практики воєнного часу

номічно недоцільним та функціонально обмеженим. Фізична охорона не здатна захистити від кібератак, а паперовий документообіг стає критичною вразливістю при руйнуванні офісних приміщень. Відтак, вирішення другого завдання дослідження полягає в обґрунтуванні методологічного підходу, який забезпечить поєднання фізичного та цифрового контурів безпеки.

В інтересах забезпечення економічної безпеки підприємств нами пропонується інтегровано-адаптивний методологічний підхід.

Сутність цього підходу полягає у системному поєднанні перевірених часом традиційних інструментів захисту активів з новітніми цифровими технологіями, де вибір конкретної комбінації інструментів визначається критерієм економічної доцільності.

Структура запропонованого методологічного підходу базується на трьох рівнях інтеграції. Розкриємо їх сутність:

1) Рівень моніторингу та ідентифікації загроз. Традиційний метод передбачає періодичний аудит та фізичний нагляд, що є ресурсомістким. Інтегрований підхід передбачає впровадження систем інтернету речей та супутникового моніторингу. Це дозволяє отримувати дані про стан активів (полів, складів, техніки) у режимі реального часу, знижуючи витрати на фізичну логістику та персонал.

2) Рівень захисту та нейтралізації. На цьому рівні відбувається поєднання фізичних бар'єрів із цифровими протоколами. Це включає міграцію даних у хмарні сховища для захисту інформаційного капіталу та використання цифрових двійників підприємства для моделювання наслідків фізичного ураження і розробки оптимальних планів відновлення.

3) Рівень прийняття управлінських рішень. Замість інтуїтивного прийняття рішень пропонується перехід до управління на основі аналітики великих даних, що дозволяє розрахувати вартість ризику та обрати найдешевший сценарій реагування.

Реалізація окресленого підходу вимагає чіткої формалізації принципу економічної доцільності, адже в умовах дефіциту ліквідності будь-які інвестиції у безпеку повинні генерувати вимірюваний економічний ефект. Сутність цього принципу та механізми його практичної імплементації наведено в таблиці 2.

Враховуючи неоднорідність реального сектору економіки, застосування цього методологічного підходу має враховувати галузеву специфіку. Аграрні та промислово-виробничі

Таблиця 2

Реалізація принципу економічної доцільності в системі управління економічною безпекою підприємства

Складова принципу	Економічна сутність	Практична реалізація (інструментарій)
Оптимізація граничних витрат	Витрати на впровадження цифрового інструменту захисту не повинні перевищувати вартість активів під ризиком або розмір потенційних збитків від реалізації загрози.	Заміна фізичної охорони периметра на системи відеоспостереження з автоматичною аналітикою; перехід від утримання власної серверної інфраструктури до оренди хмарних потужностей.
Мінімізація альтернативної вартості	Ресурси, спрямовані на безпеку, не повинні вилучатися з основної операційної діяльності у критичних обсягах. Безпека має підтримувати бізнес-процеси.	Впровадження інтегрованих систем управління ресурсами, де модуль безпеки є частиною загальної системи, що дозволяє уникнути дублювання функцій та даних.
Швидкість капіталізації рішень	Часовий проміжок між виявленням загрози та реагуванням має бути мінімальним, оскільки кожна година простою в умовах війни генерує прямі збитки.	Використання автоматизованих сценаріїв реагування (наприклад, автоматичне перемикання на резервні канали зв'язку або енергоживлення) без очікування ручної санкції.
Масштабованість захисту	Зростання обсягів бізнесу або розширення географії діяльності не повинно призводити до пропорційного зростання витрат на безпеку.	Використання платформних рішень, які дозволяють підключати нові філії або активи до системи безпеки без значних капітальних витрат.

Джерело: сформовано авторами

*Примітка. Формалізація принципу економічної доцільності в межах запропонованого підходу може бути представлена нерівністю:

$C_{int} < L_{pot} \times P_{risk}$, де

C_{int} – вартість впровадження інтегрованої системи безпеки (сукупність витрат на організаційні, інженерно-технічні та програмні засоби захисту);

L_{pot} – потенційні економічні втрати (вартість втрачених активів + втрачена вигода);

P_{risk} – ймовірність реалізації ризикової події (визначається на основі предиктивної аналітики).

підприємства стикаються з різними типами воєнних ризиків, що зумовлює відмінність завдань їхньої економічної безпеки та цифрових інструментів, що застосовуються (табл. 3).

Таким чином, запропонований методологічний підхід дозволяє трансформувати систему економічної безпеки з витратного центру в інструмент підвищення операційної ефективності. Для аграріїв цифровізація безпеки означає збереження контролю над активами без фізичної присутності, а для промисловців – можливість гнучкого управління виробничими фондами в умовах енергетичного та ресурсного дефіциту.

Водночас, практичне застосування запропонованого підходу для аграрних та промислово-виробничих підприємств неможливе без відповідного організаційного забезпечення. Методологічні засади визначають загальну логіку та правила побудови системи безпеки, але для їх безпосереднього впровадження у бізнес-процеси необхідна чітка структура управління, застосування адекватного інструментарію.

Реалізація обґрунтованого вище методологічного підходу вимагає розробки прикладного інструментарію, здатного трансформувати теоретичні принципи у конкретні управлінські дії. Таким інструментарієм, на нашу думку, має виступати структурно-функціональний механізм мінімізації воєнних ризиків. Вибір саме такої конструкції зумовлений необхідністю поєднання статики (організаційної структури, підрозділів, ресурсів) та динаміки (конкретних функцій, процесів, алгоритмів дій). В умовах

Таблиця 3

Специфіка завдань та цифрових інструментів забезпечення економічної безпеки підприємств аграрного та промислового секторів

Характеристика	Аграрний сектор	Промисловий сектор
Специфічні воєнні ризики	– замінування полів та неможливість обробітку; – крадіжка врожаю на окупованих територіях; – блокування експортних коридорів; – знищення елеваторних потужностей.	– ракетні удари по виробничих цехах; – критична залежність від стабільного електропостачання; – розрив ланцюгів постачання комплектуючих; – дефіцит кваліфікованих інженерних кадрів.
Пріоритетні завдання економічної безпеки	Збереження земельного банку та врожаю. Забезпечення фізичної доступності полів та моніторинг стану посівів без ризику для життя персоналу.	Забезпечення виробничої стійкості. Мінімізація часу простоїв, швидка релокація потужностей або перепрофілювання виробництва.
Цифрові інструменти реалізації	Системи управління агровиробництвом: супутниковий моніторинг полів для оцінки збитків без виїзду на місце. Безпілотні літальні апарати: для виявлення мін та охорони врожаю. Електронні карти полів: для фіксації злочинів та документування збитків.	Цифрові двійники: моделювання виробничих процесів для оптимізації енергоспоживання. Розумне виробництво: датчики стану обладнання для прогнозування ремонтів в умовах дефіциту запчастин. 3D-друк: виготовлення відсутніх деталей на місці.

Джерело: сформовано авторами

війни фрагментарні, несистемні заходи безпеки не забезпечують належного рівня захисту активів, а часто призводять до дезорганізації управління та непродуктивного витрачання обмежених фінансових ресурсів. Тому виникає потреба у створенні регламентованої системи, де кожен структурний елемент виконує чітко визначену функцію з протидії загрозам, що дозволяє досягти синергетичного ефекту в управлінні безпекою.

Мета розробки структурно-функціонального механізму мінімізації воєнних ризиків полягає, передусім, у створенні цілісної системи управління, яка забезпечує безперервність бізнес-процесів та стійкий економічний розвиток підприємств шляхом нівелювання впливу воєнних загроз. Специфіка запропонованого механізму визначається його глибокою інтеграцією з цифровим середовищем. На відміну від традиційних моделей, де інформаційні технології виконують допоміжну роль, у цьому механізмі цифровий простір виступає інтегруючим базисом. Він об'єднує всі елементи механізму (суб'єкти, об'єкти, методи) через наскрізні потоки даних. Взаємозв'язок між елементами механізму та цифровим середовищем реалізується через перетворення фізичних подій (наприклад, рух техніки, зміна складських залишків) у цифрові сигнали, які обробляються аналітичними системами для прийняття миттєвих економічно обґрунтованих рішень. Структура запропонованого механізму передбачає наявність п'яти функціональних підсистем: цільову, діагностичну, організаційно-виконавчу, ресурсно-фінансову та контрольно-адаптивну. Їх зміст та взаємодію із цифровим середовищем представлено у таблиці 4.

Застосування розробленого механізму дозволяє підприємствам реального сектору перейти від реактивного ситуативного реагування до системного управління стійкістю. Головним практичним наслідком його впровадження є зниження операційних втрат та збереження інвестиційної привабливості активів навіть в умовах підвищеного ризику.

Ефективність дії механізму залежить від своєчасного коригування його параметрів. Коригування дії механізму необхідне у таких випадках: зміна географії бойових дій (наближення лінії фронту вимагає активації процедур релокації); поява нових типів загроз (наприклад, нові види кібератак або зміна тактики обстрілів енергосистеми); технологічне оновлення цифрового середовища (впровадження нових версій програмного забезпечення або обладнання). Отже, запропонований механізм є динамічною системою,

Таблиця 4

Структурно-функціональний механізм мінімізації воєнних ризиків підприємств реального сектору в умовах цифрових змін

Структурні складові	Функціональне призначення та сутність функціонування	Взаємозв'язок із цифровим середовищем
1. Цільова підсистема (вектор розвитку)	Визначення стратегічних пріоритетів безпеки: збереження вартості активів, забезпечення ліквідності, утримання частки ринку. Формування політики безпеки, що узгоджується із загальною стратегією бізнесу.	Цифрове середовище забезпечує моделювання сценаріїв розвитку подій. Використання інструментів стратегічного планування на основі даних дозволяє кількісно визначити допустимий рівень ризик-апетиту підприємства.
2. Діагностична підсистема (моніторинг)	Безперервний аудит зовнішнього та внутрішнього середовища. Ідентифікація загроз (фізичних, кібернетичних, кадрових) на ранніх стадіях. Оцінка ймовірності настання ризикових подій та розрахунок потенційних збитків.	Інтеграція із зовнішніми базами даних та системами супутникового моніторингу. Отримання інформації про лінію фронту, повітряні тривоги та стан інфраструктури в режимі реального часу. Автоматизована аналітика вразливостей IT-мережі.
3. Організаційно-виконавча підсистема (дія)	Реалізація конкретних заходів протидії: фізична релокація потужностей, диверсифікація ланцюгів постачання, захист інформаційного периметра, зміна графіків роботи персоналу.	Використання цифрових двійників для тестування планів евакуації. Управління логістикою через хмарні платформи. Впровадження електронного документообігу для забезпечення мобільності управлінських процесів.
4. Ресурсно-фінансова підсистема (забезпечення)	Акумуляція та розподіл фінансових, матеріальних та кадрових ресурсів для реалізації заходів безпеки. Створення резервних фондів. Страхування воєнних ризиків.	Використання смарт-контрактів для автоматизації страхових виплат. Захист фінансових транзакцій через технології розподіленого реєстру. Оптимізація бюджету безпеки за допомогою алгоритмів аналізу витрат.
5. Контрольно-адаптивна підсистема (зворотний зв'язок)	Моніторинг ефективності вжитих заходів. Порівняння фактичних втрат із плановими показниками. Коригування стратегії безпеки при зміні лінії фронту або технологічних умов.	Панелі моніторингу (дашборди) для відображення ключових індикаторів безпеки керівництву. Системи штучного інтелекту для автоматичного коригування параметрів захисту без участі людини (наприклад, блокування підозрілого трафіку).

Джерело: сформовано авторами

що забезпечує стійкий економічний розвиток підприємства через збалансоване поєднання матеріальної (або ресурсної) складової безпеки та цифрових технологій.

Висновки. У статті вирішено актуальне науково-прикладне завдання щодо теоретико-методологічного обґрунтування системи управління економічною безпекою підприємств реального сектору та розробки інструментарію мінімізації воєнних ризиків в умовах цифрових змін. Основні результати дослідження зводяться до наступного:

Поглиблено теоретичні засади економічної безпеки. Уточнено сутність поняття «економічна безпека підприємства в умовах цифрових змін» як динамічної здатності суб'єкта господарювання зберігати цілісність активів та генерувати вартість в умовах екзогенних шоків. Розроблено класифікацію воєнних ризиків, яка, на відміну від існуючих, диференціює загрози за джерелом виникнення (кінетичні, інфраструктурні), об'єктом впливу (людський, фінансовий капітал) та цифровим аспектом реалізації (кібернетичні, інформаційно-репутаційні). Це дозволило ідентифікувати специфічні вектори деструктивного впливу на операційну ефективність та вартість активів підприємств реального сектору.

Обґрунтовано методологічний підхід до забезпечення безпеки. Запропоновано інтегровано-адаптивний підхід, що базується на системному поєднанні традиційних (фізичних) та новітніх (цифрових) методів захисту. Визначальним критерієм вибору інструментарію визначено принцип економічної доцільності, формалізований через співставлення витрат на впровадження системи безпеки з потенційними втратами від реалізації ризиків. Доведено, що для аграрних та промислових підприємств цифрова трансформація безпекової функції дозволяє знизити трансакційні витрати та мінімізувати альтернативну вартість ресурсів.

Розроблено структурно-функціональний механізм мінімізації ризиків. Сформовано механізм, який інтегрує цільову, діагностичну, організаційно-виконавчу, ресурсно-фінансову та контрольно-адаптивну підсистеми в єдиному цифровому середовищі підприємства. Визначено, що практична цінність механізму полягає у переході від ситуативного реагування до системного управління стійкістю, що забезпечується використанням цифрових двійників, IoT-моніторингу та аналітики великих даних. Це дозволяє підприємствам підтримувати безперервність бізнес-процесів навіть в умовах критичної невизначеності.

Перспективи подальших досліджень у цьому напрямі доцільно зосередити на дослідженні специфіки управління економічною безпекою підприємств в період повоєнного відновлення економіки України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Білявська Ю., Уманців Ю., Осецький В., Мамчур В. Тенденції розвитку агробізнесу України в умовах воєнного стану. *Економіка АПК.* 2025. № 5. Т. 32. С. 48–62. https://doi.org/10.32317/ekon.apk/5.2025.48

2. Демчишак Н. Б., Шевчук Р. С., Гоменюк К. В. Цифрові технології та інструменти забезпечення фінансової безпеки підприємств у контексті вартісно-орієнтованого управління. *Економіка та суспільство*. 2025. Вип. 73. https://doi.org/10.32782/2524-0072/2025-73-53

3. Євтушенко Н. М., Стеценко Д. І. Цифрова трансформація бізнесу в умовах війни в Україні: виклики та можливості. *Економічний простір.* 2024. № 191. С. 211–216.

4. Жураковська А., Лукашова Д., Павлов Р. Виклики та специфіка забезпечення економічної безпеки підприємства в кризових умовах. *Економіка та суспільство.* 2024. № 68. https://doi.org/10.32782/2524-0072/2024-68-100

5. Козлова І. М., Велика О. Ю., Козлов Н. В. Особливості стратегічного розвитку підприємств в умовах воєнного стану. *Бізнес Інформ*. 2023. № 5. С. 134–140. https://doi.org/10.32983/2222-4459-2023-5-134-140

6. Линда І. С. Нові виклики та загрози цифрової трансформації економіки для системи фінансово-економічної безпеки підприємництва. Академічні візії. 2025. Вип. 50. https://doi.org/10.5281/zenodo.17909029

7. Максименко А. П. Реальні та потенційні загрози цифрової економіки в умовах війни. *Економічний простір.* 2023. № 188. С. 41–49.

8. Мірошніченко М. В. Економічна безпека промислової галузі як ключовий елемент економічної безпеки національної економіки. *Економічний простір.* 2025. № 206. С. 244–250. https://doi.org/10.30838/EP.206.244-250

9. Нижник О., Нижник І. Формування організаційно-економічного механізму та стратегій безпечного інноваційного розвитку соціально-економічних систем. *Вісник Хмельницького національного університету. Економічні науки.* 2024. № 2. С. 126–130. https://elar.khmnu.edu.ua/handle/123456789/16070

10. Тульчинська С., Ткаченко Т. Принципи системи економічної безпеки промислових підприємств в умовах конкуренції. *Вісник Хмельницького національного університету. Економічні науки.* 2023. № 3. С. 226–230.

11. Філиппова С. В., Волощук Л. О., Черкасова С. О. Економічна безпека підприємств реального сектору економіки в умовах вартісно-орієнтованого управління: монографія. Одеса : ФОП Бондаренко М. О., 2015. 196 с.

12. Шульга О. Оцінка ефективності системи управління економічною безпекою аграрного сектора національної економіки. *Економіка та суспільство.* 2025. (81). https://doi.org/10.32782/2524-0072/2025-81-4

13. Ansoff H. I. Strategic Management. Classic Edition. London : Palgrave Macmillan, 2007. DOI: https://doi.org/10.1057/9780230590601.

14. Drucker P. F. Managing in Turbulent Times. New York : Routledge, 2012. DOI: https://doi.org/10.4324/9780080938158.

15. Porter M. E. Competitive Strategy: Techniques for Analyzing Industries and Competitors. New York : Free Press, 1980. URL: https://www.hbs.edu/faculty/Pages/item.aspx?num=195.

REFERENCES:

1. Biliavska, Yu., Umantsiv, Yu., Osetskyi, V., & Mamchur, V. (2025). Tendentsii rozvytku ahrobiznesu Ukrainy v umovakh voiennoho stanu [Trends in agribusiness development in Ukraine under martial law]. *Ekonomika APK,* 32(5), 48–62. https://doi.org/10.32317/ekon.apk/5.2025.48

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 the financial security of enterprises in the context of value-based management]. *Ekonomika ta suspilstvo*, (73). https://doi.org/10.32782/2524-0072/2025-73-53

3. Fylyppova, 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 under value-based management] (Monograph). Odesa: FOP Bondarenko M. O.

4. 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]. *Biznes Inform*, (5), 134–140. https://doi.org/10.32983/2222-4459-2023-5-134-140

5. 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 financial and economic security system of entrepreneurship]. *Akademichni vizii*, (50). https://doi.org/10.5281/zenodo.17909029

6. Maksymenko, A. P. (2023). Realni ta potentsiini zahrozy tsyfrovoi ekonomiky v umovakh viiny [Real and potential threats of the digital economy in wartime]. *Ekonomichnyi prostir,* (188), 41–49.

7. Miroshnichenko, M. V. (2025). Ekonomichna bezpeka promyslovoi haluzi yak kliuchovyi element ekonomichnoi bezpeky natsionalnoi ekonomiky [Economic security of the industrial sector as a key element of national economic security]. *Ekonomichnyi prostir,* (206), 244–250. https://doi.org/10.30838/EP.206.244-250

8. Nyzhnyk, O., & Nyzhnyk, I. (2024). Formuvannia orhanizatsiino-ekonomichnoho mekhanizmu ta stratehii bezpechnoho innovatsiinoho rozvytku sotsialno-ekonomichnykh system [Formation of an organizational-economic mechanism and strategies for safe innovative development of socio-economic systems]. *Visnyk Khmelnytskoho natsionalnoho universytetu. Ekonomichni nauky*, (2), 126–130. https://elar.khmnu.edu.ua/handle/123456789/16070

9. 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]. *Ekonomika ta suspilstvo*, (81). https://doi.org/10.32782/2524-0072/2025-81-

10. 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]. *Visnyk Khmelnytskoho natsionalnoho universytetu. Ekonomichni nauky*, (3), 226–230.

11. Yevtushenko, N. M., & Stetsenko, D. I. (2024). Tsyfrova transformatsiia biznesu v umovakh viiny v Ukraini: vyklyky ta mozhlyvosti [Digital transformation of business in the conditions of war in Ukraine: challenges and opportunities]. *Ekonomichnyi prostir,* (191), 211–216.

12. Zhurakovska, A., Lukashova, D., & Pavlov, R. (2024). Vyklyky ta spetsyfika zabezpechennia ekonomichnoi bezpeky pidpryiemstva v kryzovykh umovakh [Challenges and specifics of ensuring enterprise economic security in crisis conditions]. *Ekonomika ta suspilstvo*, (68). https://doi.org/10.32782/2524-0072/2024-68-100

13. Ansoff, H. I. (2007). Strategic Management (Classic Ed.). Palgrave Macmillan. https://doi.org/10.1057/9780230590601

14. Drucker, P. F. (2012). Managing in Turbulent Times. Routledge. https://doi.org/10.4324/9780080938158

15. 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

Дата надходження статті: 02.02.2026
Дата прийняття статті: 20.02.2026
Дата публікації статті: 26.02.2026