

Електронний журнал «Ефективна економіка» включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України № 975 від 11.07.2019). Спеціальності – 051, 071, 072, 073, 075, 076, 292. Ефективна економіка. 2025. № 11.

DOI: <http://doi.org/10.32702/2307-2105.2025.11.124>

УДК 338.28:004

*Д. О. Сергеева,
магістр кафедри менеджменту підприємств,
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
ORCID ID: <https://orcid.org/0000-0001-8353-7994>*

*І. І. Нагорна,
к. е. н., доцент кафедри менеджменту підприємств,
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
ORCID ID: <https://orcid.org/0000-0003-3644-8440>*

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

*D. Serheyeva,
Master`s Student, Department of Management of Enterprises, National Technical
University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”
N. Nahorna,
PhD in Economics, Associate Professor of the Department of Management of
Enterprises, National Technical University of Ukraine “Igor Sikorsky Kyiv
Polytechnic Institute”*

FEATURES OF ENSURING THE ECONOMIC SECURITY OF AN ENTERPRISE IN THE CONTEXT OF DIGITAL TRANSFORMATION

У статті досліджено сутність розуміння економічної безпеки підприємства, яка є багатовимірним науковим поняттям, що інтегрує фінансові, виробничі, ринкові, кадрові, інформаційні та інші складові, забезпечуючи сприятливість суб'єкта господарювання до стабільного функціонування, розвитку та ефективного протистояння зовнішнім і внутрішнім загрозам.

Визначено, що економічна безпека в умовах цифрової трансформації проявляється не тільки в здатності підприємства уникати небажаних впливів, а й вміння адаптуватися до трансформацій зовнішнього середовища, використовувати нові можливості, забезпечувати високу ефективність діяльності та формувати стратегічні орієнтири розвитку.

В роботі було представлено методику визначення інтегрального рівня економічної безпеки підприємства, яка передбачає: декомпозицію складових безпеки підприємства; визначення критеріїв оцінки кожної складової та проведення їх розрахунків; формування шкали рівнів економічної безпеки кожної складової; ранжування рівнів економічної безпеки та інтегральну оцінку рівня економічної безпеки на основі середнього арифметичного рангів.

The article explores the essence of understanding the economic security of an enterprise, which is a multidimensional scientific concept that integrates financial, production, market, personnel, information and other components, ensuring the suitability of a business entity for stable functioning, development and effective resistance to external and internal threats.

It is determined that economic security in the context of digital transformation is manifested not only in the ability of an enterprise to avoid undesirable influences, but also in the ability to adapt to transformations of the external environment, use new opportunities, ensure high efficiency of activities and form strategic development guidelines.

The paper presents a methodology for determining the integral level of economic security of an enterprise, which involves: decomposition of the

components of enterprise security; determination of criteria for assessing each component and their calculations; formation of a scale of economic security levels for each component; ranking of economic security levels; integral assessment of the level of economic security based on the arithmetic mean of ranks.

To improve the system for ensuring the economic security of an enterprise in the context of digital transformation, an integrated economic security management system was proposed based on the principles of consistency, continuity, analytical transparency and compliance with international standards, namely the ISO/IEC 27001:2022 standard. This standard defines the requirements for the creation, maintenance and improvement of a documented information security management system that ensures the confidentiality and integrity of data through systematic risk management that arises as a result of identifying the level of economic security.

The work formalizes the algorithms for responding to identified deviations and risks of the economic security of the enterprise. In this case, the formation of prepared action scenarios for various types of risk is envisaged. Using digital technologies, it is proposed to implement a scenario approach to improve the level of economic security.

Ключові слова: *економічна безпека, трансформація, цифровізація, ризик, стратегія, економічна стійкість.*

Keywords: *economic security, transformation, digitalization, risk, strategy, economic sustainability.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. У сучасних умовах інтенсивного розвитку цифрових технологій та їх глибокої інтеграції в бізнес-процеси підприємств, необхідність переосмислення підходів до забезпечення економічної безпеки суб'єктів господарювання стає все більш актуальною. Цифрова трансформація сприяє підвищенню ефективності управління, оптимізації операційних процесів, розширенню інформаційних

можливостей, але водночас створює нові ризики та загрози, пов'язані з інформаційною вразливістю, кіберзлочинністю, порушенням бізнес-процесів та зниженням стабільності функціонування підприємства. Тому формування адаптивної системи забезпечення економічної безпеки в контексті цифрової трансформації є важливим завданням як теоретичного, так і прикладного характеру, яке потребує наукового обґрунтування та розробки практичних механізмів його реалізації.

Аналіз останніх досліджень і публікацій. Питання забезпечення економічної безпеки підприємства є предметом досліджень широкого кола вітчизняних та зарубіжних науковців.

У працях В. Ліпкана, Т. Васильціва, О. Ілляшенка сформовано теоретико-методологічні засади трактування економічної безпеки, визначено її сутнісні характеристики та структурні елементи [1-3]. Вчені розглядають економічну безпеку як багатокomпонентну категорію, що охоплює фінансову, кадрову, виробничу, ринкову, інформаційну та інші складові, забезпечуючи стійкість підприємства та його здатність протистояти загрозам внутрішнього та зовнішнього середовища.

Суттєвий внесок у розвиток концепції економічної безпеки зробили українські дослідники. В. О. Онищенко та співавтори розглядають економічну безпеку на державному, регіональному та мікрорівнях, акцентуючи увагу на інвестиційній, інноваційній, соціальній та енергетичній складових, а також на методах оцінювання безпекового стану [4]. У свою чергу, С. І. Мельник наголошує на ролі фінансової безпеки та пропонує модель адаптивного й антисипативного управління на основі багатокритеріальної системи вибору захисних заходів [5]. У роботах Л. В. Рибальченко, Е. В. Рижкова, С. М. Тютченка висвітлюються загрози економічній безпеці суб'єктів господарювання, зокрема тіньові схеми та економічні злочини [6].

Зарубіжні дослідники, зокрема А. Барні, Р. Каплан, М. Портер, Д. Норт, розглядали економічну безпеку через призму конкурентних переваг, стратегічного потенціалу та збалансованості управління діяльністю підприємства [7-10]. Їхні праці присвячені формуванню системи показників,

спрямованих на раннє виявлення ризиків та загроз, забезпечення стратегічної стійкості та підвищення конкурентоспроможності підприємств.

Сучасні праці С. І. Мельника, І. А. Штангрета досліджують вплив цифровізації на систему економічної безпеки підприємства, адаптуючи класичні безпекові підходи до цифрових реалій. Науковці звертають увагу на трансформацію ринку праці, розвиток цифрових загроз, необхідність цифрової зрілості підприємств та впровадження новітніх технологій у систему захисту [11].

Попри значний обсяг наукових публікацій, питання вимірювання впливу цифрової трансформації на економічну безпеку підприємства все ще залишається недостатньо опрацьованим. Недостатньо розробленими є методологічні підходи до оцінювання структурних компонентів економічної безпеки в цифровій економіці, визначення системи показників, чутливих до цифрових змін, а також комплексних підходів до інтегрованої оцінки. Залишається фрагментарним розкриття зв'язку між рівнем цифрової зрілості підприємства та ефективністю системи економічної безпеки. Обмеженим є також спектр практичних рекомендацій щодо посилення економічної безпеки з урахуванням цифрових технологій, організаційної адаптації та розвитку інструментів управління внутрішніми ризиками.

Формулювання цілей статті (постановка завдання). Метою статті є дослідження особливостей забезпечення економічної безпеки підприємства в умовах цифрової трансформації та розробка стратегії покращення рівня економічної безпеки з використанням сценаріїв дій для її стабілізації.

Виклад основного матеріалу дослідження. Забезпечення економічної безпеки підприємства в умовах цифрової трансформації потребує створення цілісної системи, здатної своєчасно діагностувати рівень економічної безпеки, загрози, що виникають у процесі цифровізації бізнес-процесів та реагувати на швидкі зміни, як зовнішнього так і внутрішнього середовища.

Цифрова трансформація створює не лише нові можливості для підвищення рівня економічної безпеки, але й генерує нові види ризиків, насамперед кібернетичні та інформаційні, які можуть мати катастрофічні економічні наслідки для підприємства.

Нерідкими є й випадки, коли, внаслідок кібератак, українські бізнеси стикаються з необхідністю призупиняти роботу через технологічні збої та витоки конфіденційних даних. За перелічених зовнішніх загроз, сучасні підприємства зобов'язані не лише оперативне реагувати на виклики й кризові ситуації, але й забезпечувати стратегічний підхід в економічній безпеці підприємства.

Економічна безпека підприємства розглядається як комплексне та багатовимірне явище. З метою систематизації теоретичних надбань науковців, варто конкретизувати підходи до трактування економічної безпеки підприємства. Під економічною безпекою підприємства слід розуміти — багатовимірний соціально-економічний та управлінський стан системи підприємства, який характеризується здатністю зберігати, відтворювати та розвивати свої ключові ресурси, підтримувати стійку рівновагу між внутрішніми та зовнішніми чинниками впливу, протидіяти реальним потенційним загрозам та забезпечувати досягнення стратегічних цілей у довгостроковій перспективі.

Цифрова трансформація безпосередньо впливає на ключові складові економічної безпеки підприємства, з одного боку, вона виступає каталізатором підвищення продуктивності, оптимізації витрат та виходу на нові ринки, з іншого — створює нові ризики, що пов'язані з кіберзагрозами, технологічною залежністю та регуляторними обмеженнями. Для кращого розуміння даного взаємозв'язку, доцільно розглядати логіко-структурну модель впливу цифрової трансформації на систему забезпечення економічної безпеки підприємства (рис. 1).

Причинно-наслідкова схема демонструє, що цифрова трансформація виступає як каталізатор підвищення ефективності підприємства, але водночас формує й нові загрози. Її вплив на систему забезпечення економічної безпеки є амбівалентним. Ефективність такої системи потребує своєчасного проведення аналізу та діагностики з врахуванням цифрової трансформації.

Для визначення рівня економічної безпеки підприємства та її ключових складових потрібно дослідити саму природу процесу забезпечення економічної безпеки підприємства в умовах цифрової трансформації.



Рис. 1. Логіко-структурна модель впливу цифрової трансформації на систему забезпечення економічної безпеки підприємства

Джерело: Систематизовано, узагальнено та згруповано авторами

Методика визначення інтегрального рівня економічної безпеки підприємства передбачає наступні етапи:

1. Декомпозиція складових безпеки підприємства;
2. Визначення критеріїв оцінки кожної складової та проведення їх розрахунків;
3. Формування шкали рівнів економічної безпеки кожної складової;
4. Ранжування рівнів економічної безпеки;

5. Інтегральна оцінка рівня економічної безпеки на основі середнього арифметичного рангів.

Варто зауважити, що декомпозиція складових економічної безпеки може враховувати і інші аспекти, зокрема місце на ринку, правове середовище, зовнішній вплив політики та економіки, тощо. У такому випадку, методика визначення рівня складових економічної безпеки суттєво залежить від галузі та специфіки діяльності підприємства. Бажано в дослідженні враховувати практичне значення в оцінці ключових внутрішніх складових економічної безпеки підприємства.

На рис. 2 систематизовано типове розуміння економічної безпеки підприємства з призми розуміння сутності: фінансової, кадрової, виробничої та цифрової складової.



Рис. 2. Ключові внутрішні складові економічної безпеки підприємства

Джерело: Систематизовано, узагальнено та згруповано авторами

Прикладна ілюстрації методичного підходу оцінки рівня економічної безпеки підприємства буде представлена на базі ТОВ «Крупецький комбікормовий завод» за період 2022–2024 рр.

Для оцінки фінансової складової економічної безпеки пропонується адаптувати та використовувати підхід запропонований Шаталовим В. О. та Пасенченко Ю. А., який передбачає розрахунок узагальнених груп фінансових показників [12]. З метою підвищення об'єктивності оцінювання методику уточнено шляхом врахування галузевих нормативів, а також вимог,

визначених Наказом Міністерства економіки України № 14 [13]. У випадках, коли норматив подавався у вигляді діапазону, для порівняння використано нижню межу, як критичний індикатор допустимого рівня. Таблиця 1 - містить методику розрахунку та мінімальні нормативні значення для груп показників фінансової безпеки.

Таблиця 1. Розрахунок ключових фінансових показників на прикладі ТОВ «Крупницький комбікормовий завод» (2022-2024 рр.)

Група	Показник	Методика розрахунку	2022	2023	2024	Норма (min)
Показники ліквідності	коефіцієнт абсолютної ліквідності ($K_{ал}$)	$K_{ал} = (\text{Грошові кошти} + \text{Поточні фінансові інвестиції}) / \text{Поточні зобов'язання}$	0,01	0,09	0,03	0,2
	коефіцієнт покриття (швидкої ліквідності) ($K_{п}$)	$K_{п} = (\text{Оборотні активи} - \text{Запаси}) / \text{Поточні зобов'язання}$	0,58	0,73	0,42	0,6
	коефіцієнт поточної ліквідності ($K_{пл}$)	$K_{пл} = \text{Оборотні активи} / \text{Поточні зобов'язання}$	1,06	1,43	1,13	1,5
Показники фінансової стійкості	коефіцієнт фінансової стабільності ($K_{фс}$)	$K_{фс} = (\text{Власний капітал} + \text{Довгострокові зобов'язання}) / \text{Валюта балансу}$	0,66	0,77	0,71	0,7
	коефіцієнт автономії ($K_{а}$)	$K_{а} = \text{Власний капітал} / \text{Валюта балансу}$	0,66	0,77	0,71	0,5
	коефіцієнт маневреності робочого капіталу ($K_{мрк}$)	$K_{мрк} = (\text{Власний капітал} - \text{Необоротні активи}) / \text{Власний капітал}$	0,03	0,13	0,05	0,1
Показники рентабельності	коефіцієнт рентабельності активів ($K_{ра}$)	$K_{ра} = \text{Чистий прибуток} / \text{Середньорічна вартість активів}$	18%	24%	9%	10%
	коефіцієнт рентабельності власного капіталу ($K_{рвк}$)	$K_{рвк} = \text{Чистий прибуток} / \text{Середньорічна вартість власного капіталу}$	27%	34%	12%	15%
	коефіцієнт рентабельності продукції ($K_{прод}$)	$K_{прод} = \text{Чистий прибуток} / \text{Собівартість реалізованої продукції} * 100\%$	36%	41%	10%	12%

Продовження таблиці 1.

Група	Показник	Методика розрахунку	2022	2023	2024	Норма (min)
Показники ділової активності	коефіцієнт оборотності активів (K_{oa})	$K_{oa} = \text{Чистий дохід від реалізації} / \text{Середньорічна вартість активів}$	0,80	0,96	1,02	0,8
	коефіцієнт оборотності основних засобів (K_{oos})	$K_{oos} = \text{Чистий дохід від реалізації} / \text{Середньорічна вартість основних засобів}$	2,59	3,68	2,30	1,5
	коефіцієнт оборотності власного капіталу (K_{ovk})	$K_{ovk} = \text{Чистий дохід від реалізації} / \text{Середньорічна вартість власного капіталу}$	1,21	1,34	1,37	1

Джерело: сформовано авторами на основі [13]

Формування системи вагових коефіцієнтів для оцінювання фінансової безпеки здійснювалося із застосуванням методу експертних оцінок. Такий підхід є доцільним, оскільки дає змогу ранжувати показники за рівнем їх впливу та врахувати специфіку діяльності підприємства. Актуальні експертні ваги для ТОВ «Крупецький комбікормовий завод» наведено у табл. 2.

Таблиця 2. Формування вагових коефіцієнтів для оцінки фінансових показників

Показник	Ранг важливості	Вага (Фішберн)
Коефіцієнт абсолютної ліквідності (K_{al})	1	0,154
Коефіцієнт поточної ліквідності (K_{pl})	2	0,141
Коефіцієнт рентабельності продукції (K_{rp})	3	0,128
Коефіцієнт рентабельності власного капіталу (K_{rvk})	4	0,115
Коефіцієнт фінансової стабільності (K_{fs})	5	0,103
Коефіцієнт автономії (K_a)	6	0,090
Коефіцієнт швидкої ліквідності (K_p)	7	0,077
Коефіцієнт рентабельності активів (K_{ra})	8	0,064
Коефіцієнт оборотності активів (K_{oa})	9	0,051
Коефіцієнт маневреності власного капіталу (K_{mrk})	10	0,038
Коефіцієнт оборотності власного капіталу (K_{ovk})	11	0,026
Коефіцієнт оборотності основних засобів (K_{oos})	12	0,013

Джерело: сформовано авторами

З метою формування раціональної шкали для відображення рівня фінансової безпеки, вартує оцінити еталонні суми показників за наведеними мінімальними нормованими значеннями. Для цього було проведено

розрахунок суми добутків вагових коефіцієнтів на мінімальні значення діапазону норми за кожним показником. На основі проведених розрахунків було отримано базу для формування шкали рівнів фінансової безпеки — 0,53.

Таблиця 3. Шкала рівнів фінансової безпеки

Рівень безпеки	Характеристика рівня безпеки	Границі	Ранг
Критичний рівень безпеки	Низька фінансова стійкість, високий ризик припинення діяльності	0 — 0,26	1
Хитливий рівень безпеки	Більша рівновага між платіжними засобами та зобов'язаннями, однак наявні проблеми з платоспроможністю	0,27 — 0,52	2
Задовільний рівень безпеки	Достатній рівень платоспроможності та фінансової стійкості	0,53 — 0,80	3
Абсолютний рівень безпеки	Високий рівень платоспроможності, стабільний фінансовий рівень	0,81 +	4

Джерело: сформовано авторами

Рівні безпеки для наочності інтерпретації результатів було поділено на 4 умовні відрізки. Ключова ідея полягає у використанні виведеного показника 0,53 для усвідомлення порогу, вище якого рівень фінансової безпеки знаходиться на задовільному рівні. Розраховуючи за наведеною методологією, можливо виявити поточний стан фінансової безпеки на досліджуваному підприємстві.

Для оцінювання кадрової складової економічної безпеки застосовано аналогічний підхід до групування та аналізу показників. Водночас ключовою відмінністю є використання планових (цілевих) значень, визначених підприємством, замість уніфікованих нормативних порогів. Підхід зумовлений специфікою кадрової сфери, де відсутні загальноприйняті галузеві шкали, а рівень безпеки значною мірою залежить від внутрішніх особливостей організації, її стратегії розвитку та кадрової політики.

Для проведення аналізу кадрової безпеки на ТОВ «Крупецький комбікормовий завод» було використано методологічний підхід Урдуханова Р.І. [14].

На основі методу експертних оцінок було визначено важливість кожного розрахованого показника. Аналогічний метод необхідно використовувати при аналізі кадрової безпеки на досліджуваному підприємстві, з метою отримання більш точних результатів.

**Таблиця 4. Динаміка ключових кадрових показників
ТОВ «Крупецький комбікормовий завод» 2022-2024 рр.**

Складова кадрової безпеки	Показник	Формула розрахунку	2022	2023	2024	Очікувана норма
1. Соціально-мотиваційна безпека	Показник укомплектованості кадрами	Фактична чисельність / Планова чисельність	0,97	1,00	1,00	1,00
	Коефіцієнт співвідношення прийнятих і звільнених працівників	Прийняті / звільнені	0,00	1,57	0,38	1,00
	Коеф. співвідношення середньомісячної з/п підприємства і галузевої	З/п підприємства / Середньогалузева з/п	1,36	1,68	1,52	1,15
	Показник мотивації оплати праці	Працівники з преміями / Загальна чисельність	0,00	0,00	0,10	0,10
2. Професійна безпека	Частка працівників, що пройшли навчання	Навчені протягом року / Загальна чисельність	0,13	0,10	0,20	0,10
	Частка працівників, що підвищили кваліфікацію	Підвищили кваліфікацію / Загальна чисельність	0,08	0,06	0,20	0,05
	Коефіцієнт бездефектності праці	1 – (Бездефектний випуск/загальний випуск)	0,97	0,96	0,98	0,95
3. Безпека життєдіяльності	Коеф. трудової дисципліни	1 - (Порушення трудової дисципліни / Загальна чисельність)	0,97	0,96	0,97	0,95
	Коефіцієнт дотримання умов праці	Робочі місця, що відповідають нормам / Загальна кількість	0,90	0,90	1,00	1,00

Джерело: Сформовано авторами

За допомогою очікуваних нормативних показників визначається граничне значення, що дозволяє сформувати шкалу рівнів кадрової безпеки (табл. 6).

**Таблиця 5. Формування вагових коефіцієнтів для оцінки
кадрових показників**

Група показників	Вага (Фішберн)	2022	2023	2024	Відносно норми
1. Соціально-мотиваційна безпека	0,38	0,30	0,48	0,36	0,37
2. Професійна безпека	0,24	0,14	0,14	0,15	0,14
3. Безпека життєдіяльності	0,38	0,35	0,35	0,37	0,37
Загалом	1,00	0,80	0,97	0,89	0,88

Джерело: Сформовано авторами

**Таблиця 6. Шкала рівнів кадрової безпеки відносно нормованого
значення**

Рівень безпеки	Характеристика рівня безпеки	Границі	Ранг
Критичний рівень безпеки	Масовий відтік працівників, дефіцит кваліфікованих кадрів, низька дисципліна, ризик зупинки виробничих процесів	0 — 0,44	1
Хитливий рівень безпеки	Більша рівновага, однак ще наявна нестабільність чисельності персоналу, недотримання нормативів навчання чи умов праці	0,45 — 0,87	2
Задовільний рівень безпеки	Кадровий потенціал відповідає потребам підприємства, основні показники перебувають в межах норм	0,88— 1,32	3
Абсолютний рівень безпеки	Стабільний кадровий склад, високий рівень кваліфікації та мотивації, що гарантує постійний розвиток підприємства	1,32 +	4

Джерело: сформовано авторами

При проведенні аналогічних обчислень та обов'язкової адаптації методології під досліджуване підприємство, можливо дослідити рівень кадрової безпеки суб'єкта господарювання.

Для оцінки виробничої складової економічної безпеки підприємства було застосовано комплексний підхід, що базується на наукових розробках Є. Кузьміна, Н. Ю. Горбаль, О. М. Петрашової та С. М. Ілляшенка. У рамках цього підходу виробничу складову формує техніко-технологічна безпека, яка покращує систему показників, що характеризують стан та ефективність використання виробничо-технічного потенціалу. Методологія включає нормалізацію часткових показників недостатньо цільових або оптимальних значень, їх поділ на стимулятори та дестимулятори, а також подальше

агрегування в інтегральний показник техніко-технологічної безпеки. Оцінка передбачає визначення показників стану основних засобів, ефективності їх використання, рівня технологічного розвитку, інноваційної активності та автоматизації. Галузеві орієнтири визначаються на основі даних Державної служби статистики України та середніх показників підприємств [15].

Таблиця 7. Оцінка складових техніко-технологічної безпеки для ТОВ «Крупницький комбикормовий завод» (2022-2024 рр.)

Показник	Формула розрахунку	2022	2023	2024	Орієнтовне значення	Тип
Коефіцієнт оновлення основних засобів	Вартість нових ОЗ / Вартість ОЗ на кінець періоду	0,11	0,22	0,70	$\geq 0,08$	стимулятор
Коефіцієнт вибуття основних засобів	Вартість вибутих ОЗ / Вартість ОЗ на початок періоду	0,00	0,00	0,05	$\leq 0,08$	дестимулятор
Коефіцієнт придатності основних засобів	Залишкова вартість / Первісна вартість	0,60	0,56	0,55	$\geq 0,50$	стимулятор
Коефіцієнт зносу основних засобів	Накопичений знос / Первісна вартість	0,40	0,44	0,45	$\leq 0,50$	дестимулятор
Частка активної частини основних засобів	Активна частина ОЗ / Загальна вартість ОЗ	0,61	0,63	0,64	$\geq 0,65$	стимулятор
Фондоозброєність праці	Середня вартість ОЗ / Середньооблікова чисельність працівників	3139	3129	5732	≥ 400	стимулятор
Фондовіддача	Виручка / Середня вартість ОЗ	1,30	1,84	1,15	$\geq 1,5$	стимулятор
Фондомісткість	Середня вартість ОЗ / Виручка	0,77	0,54	0,87	$< 0,5$	дестимулятор
Коефіцієнт завантаження виробничих потужностей	Фактичний випуск / Проектна потужність	0,75	0,60	0,80	$\geq 0,80$	стимулятор
Матеріаломісткість продукції	Матеріальні витрати / Виручка	0,72	0,77	0,82	$\leq 0,60$	дестимулятор
Частка сучасного обладнання	Кількість обладнання ≤ 5 років / Загальна кількість обладнання	0,64	0,65	0,7	$\geq 0,60$	стимулятор
Рівень автоматизації виробничих процесів	Автоматизовані процеси / Загальна кількість процесів	0,72	0,72	0,75	$\geq 0,70$	стимулятор

Джерело: сформовано авторами

В рамках оцінки виробничої складової вагові коефіцієнти не визначалися, оскільки всі вибрані показники характеризують один напрямок діяльності підприємства, але мають різний характер впливу (деякі є стимуляторами, деякі – дестимуляторами) та, до того ж, є взаємозалежними. У таких умовах використання вагових коефіцієнтів є недоцільним, оскільки може спотворювати реальний вплив окремих показників.

Наступним етапом є нормування прорахованих показників. Для стимуляторів формула нормування відрізняється. У процесі нормування окремі показники могли перевищувати нормативне значення 1. У таких випадках отримане значення приводилося до 1, щоб запобігти викривленню інтегральної оцінки.

Таблиця 8. Формування шкали рівнів виробничої складової економічної безпеки підприємства

Рівень безпеки	Характеристика рівня безпеки	Границі	Ранг
Критичний рівень безпеки	Високий рівень зносу та низька ефективність використання основних фондів, а модернізація практично відсутня	0 — 0,50	1
Хитливий рівень безпеки	Наявне часткове оновлення фондів, проте ефективність їхнього використання знаходиться досі на низькому рівні, існують ризики технічних збоїв	0,51 — 0,70	2
Задовільний рівень безпеки	Достатній рівень технологічного розвитку, обладнання придатне до експлуатації, а рівень автоматизації відповідає галузевим стандартам	0,71 — 0,90	3
Абсолютний рівень безпеки	Наявне повне забезпечення сучасною технікою, процеси в більшості автоматизовані, ризик технічних збоїв є мінімальним	0,91 — 1	4

Джерело: сформовано авторами

Для аналізу цифрової безпеки, пропонується здійснювати комбіновану методику NIST Cybersecurity Framework та Cybersecurity Capability Maturity Model [16], у результаті чого можливо визначити не лише ступінь захищеності інформаційних активів, а й кількісно усвідомити рівень зрілості процесів управління цифровою безпекою. Методика передбачає оцінку за п'ятьма ключовими доменами ідентифікація (Identify), захист (Protect), виявлення (Detect), реагування (Respond) та відновлення (Recover).

Таблиця 9. Оцінка рівня цифрової безпеки ТОВ «Крупецький комбікормовий завод»

№	Домен NIST CSF	Критерій	2022	2023	2024
1	Identify	Ведеться перелік цифрових активів (програми, сервери, обладнання)	0	1	1
2	Identify	Призначено відповідального за інформаційну безпеку	0	0	0
3	Identify	Відомі зовнішні постачальники цифрових технологій	1	1	1
4	Identify	Існує внутрішня політика / інструкція з управління інформацією	0	0	0
5	Identify	Проводиться оцінка ризиків інформаційної безпеки	0	0	0
Підсумок Identify			1	2	2
6	Protect	Обмежено доступ до бухгалтерських і виробничих баз	1	1	1
7	Protect	Використовується антивірусне / мережеве ПЗ	1	1	1
8	Protect	Є політика паролів / двофакторна автентифікація	0	0	1
9	Protect	Регулярно оновлюється програмне забезпечення	0	1	1
10	Protect	Мережу сегментовано між бухгалтерією, адміністрацією, виробництвом	0	1	1
11	Protect	Контролюються зовнішні доступи постачальників (вендорів)	0	1	1
Підсумок Protect			2	5	6
12	Detect	Ведуться журнали подій / логування	0	0	0
13	Detect	Є система сповіщення про збої / підозрілу активність	0	0	0
14	Detect	Проводиться моніторинг стану мережі або серверів	0	0	0
Підсумок Detect			0	0	0
15	Respond	Існує план реагування на інциденти (IRP)	0	0	0
16	Respond	Проводяться навчання персоналу з кібербезпеки	0	0	0
17	Respond	Фіксуються інциденти безпеки, проводиться аналіз	0	0	0
Підсумок Respond			0	0	0
18	Recover	Є резервне копіювання бухгалтерських баз	1	1	1
19	Recover	Є резервні копії технологічних налаштувань	0	0	0
20	Recover	Проводяться тести відновлення резервів	0	0	0
Підсумок Recover			1	1	1
ЗАГАЛЬНИЙ РЕЗУЛЬТАТ			4/20 (20%)	8/20 (40%)	9/20 (45%)

Джерело: сформовано авторами

Таблиця 10. Формування шкали рівнів цифрової безпеки

Рівень безпеки	Характеристика рівня безпеки	Границі	Ранг
Критичний рівень безпеки	Система цифрової безпеки відсутня. Дані не є захищеними, а резервів немає	0 — 0,24	1
Хитливий рівень безпеки	Функціонують окремі елементи безпеки, але відсутня системність	0,58 — 0,49	2
Задовільний рівень безпеки	Сформовані основні політики ІБ, доступи контрольовані, резервування даних часткове	0,50 — 0,74	3
Абсолютний рівень безпеки	Повноцінна система ІБ із моніторингом, резервами та звітністю	0,75 — 1	4

Джерело: сформовано автором

Шкала рівнів цифрової безпеки представлена у таблиці 11.

На основі проведеного детального дослідження окремих складових економічної безпеки на прикладі ТОВ «Крупецький комбікормовий завод», можливо сформулювати інтегральний рівень безпеки протягом 2022-2024 років.

Таблиця 11. Інтегральний рівень економічної безпеки ТОВ «Крупецький комбікормовий завод»

Складова економічної безпеки	Рік		
	2022	2023	2024
Фінансова	2	3	2
Кадрова	2	3	3
Виробнича	4	4	4
Цифрова	1	2	2
Інтегральний показник ЕБП	2,3	3	2,8

Джерело: сформовано автором

З метою покращення забезпечення економічної безпеки підприємства в умовах цифрової трансформації, необхідно формувати інтегровану систему управління економічною безпекою з опорою на принципи системності, безперервності, аналітичної прозорості та відповідності міжнародним стандартам, а саме стандарту ISO/IEC 27001:2022. Даний стандарт визначає вимоги до створення, підтримання та вдосконалення задокументованої системи управління інформаційною безпекою, що забезпечує конфіденційність та цілісність даних шляхом системного управління ризиками, які виникають внаслідок виявлення рівня економічної безпеки.

Таким чином, для побудови стійкої системи управління рівнем економічної безпеки необхідно виконати підготовчі дії (рис. 2).



Рис. 2. Стратегія покращення рівня економічної безпеки підприємства

Джерело: сформовано авторами

Відповідно до представлених кроків, для перебудови системи необхідно забезпечити технічну базу для збору, обробки та зберігання даних, що будуть використовуватись для подальшого аналізу. Рекомендовано збирати дані на щоденній основі.

Після цього, необхідно сформувати систему показників та їхніх граничних нормативів, для подальшого оцінювання рівня економічної безпеки. Для цього можливо використовувати запропоновані у статті підходи до оцінки: опиратись на статистичні дані про нормативні показників або ж відштовхуватись від планових значень для підприємства. Вже на основі даних ERP та BI-систем формуватимуться метрики ефективності, які дозволитимуть ідентифікувати відхилення за такими напрямками, як: фінансовий, виробничий, кадровий та цифровий. У межах кроку «Аналіз даних» доцільно також розробити індивідуальне програмне рішення, що автоматично рахуватиме коефіцієнти, задля формування інтегрального рівня безпеки. Відповідно, перші два кроки вже забезпечать перехід від

суб'єктивізму та нерегулярності аналізу до систематизованого підходу у моніторингу.

Заключним етапом стане формалізація алгоритмів реагування на виявлені відхилення та ризики. В даному випадку передбачається формування заготовлених сценаріїв дій для різних видів ризику.

Вже на основі визначеного, за допомогою цифрових технологій рівня економічної безпеки, пропонується реалізовувати сценарний підхід для покращення рівня економічної безпеки. У таблиці 12 наведено приклади алгоритмів реагування.

Таблиця 12. Запропоновані сценарії дій для стабілізації рівня економічної безпеки

Складова економічної безпеки	Рівень стану	Приклади алгоритмів реагування	Приклад відповідальних виконавців
1. Фінансова	Хитливий	1. Провести оперативний аналіз фінансових показників (ліквідність, дебіторська заборгованість, рентабельність).	Фахівець з економічної безпеки, головний бухгалтер
		2. Визначити причини відхилень (зростання витрат, затримки оплат).	
		3. Прийняти короткострокові заходи: обмежити витрати, пришвидшити інкасацію, переглянути графіки платежів.	
		4. Зафіксувати результати в системі моніторингу Power BI.	
	Критичний	1. Скликати нараду керівництва.	Директор, фінансовий директор
		2. Розробити антикризовий план (скорочення витрат, оптимізація запасів, пошук фінансової підтримки).	
		3. Переглянути політику фінансування, провести переговори з банками/партнерами.	
		4. За потреби — запровадити тимчасовий контроль за платежами через окреме погодження керівництва.	

Продовження таблиці 12.

Складова економічної безпеки	Рівень стану	Приклади алгоритмів реагування	Приклад відповідальних виконавців
2. Кадрова	Хитливий	1. Виявити ознаки зниження мотивації або зростання плинності.	Відділ кадрів, фахівець з економічної безпеки
		2. Провести бесіди з працівниками, зібрати анонімний зворотний зв'язок.	
		3. Запровадити короткострокові заходи стимулювання або навчання.	
	Критичний	1. Негайно сформувати резерв заміни ключових посад.	Керівник підприємства, начальник відділу кадрів
		2. Розподілити обов'язки серед наявного персоналу.	
		3. Провести аудит компетенцій, узгодити корекційні заходи з керівництвом Агрокорпорації.	
3. Техніко-технологічна (виробнича)	Хитливий	1. Виявити ділянки з підвищеним споживанням ресурсів або збоями обладнання.	Технічний директор, інженер-технолог
		2. Провести внутрішню перевірку налаштувань та дотримання регламентів.	
		3. Скоригувати технологічний графік, виконати позапланове техобслуговування.	
	Критичний	1. Ізолювати проблему (зупинити небезпечну ділянку).	Керівник підприємства, технічний директор
		2. Активувати резервні або альтернативні потужності.	
		3. Сформувати комісію з технічного аудиту.	
		4. Здійснити відновлювальні заходи згідно з планом DRP.	
4. Цифрова	Хитливий	1. Зафіксувати потенційні інциденти (нестабільна робота мережі, збій у базі, підозрілі дії користувачів).	Фахівець із цифрової безпеки
		2. Провести первинну діагностику системи.	
		3. Відновити резервні копії та змінити паролі доступу.	
	Критичний	1. Активувати протокол кібербезпеки.	Фахівець із цифрової безпеки, директор
		2. Відключити уражені вузли, повідомити керівництво.	
		3. Відновити дані з резервних серверів.	
		4. Провести аудит цифрової інфраструктури, переглянути політику доступів.	

Продовження таблиці 12.

Складова економічної безпеки	Рівень стану	Приклади алгоритмів реагування	Приклад відповідальних виконавців
5. Ринкова	Хитливий	1. Моніторинг попиту, цін конкурентів, відгуків клієнтів.	Відділ збуту, маркетинголог
		2. За потреби — коригування обсягів виробництва чи асортименту.	
		3. Підсилення маркетингової активності через CRM.	
	Критичний	1. Провести терміновий аналіз ринку.	Керівник підприємства, комерційний відділ
		2. Визначити причини втрати клієнтів або обсягів продажів.	
		3. Розробити план дій: знижки, партнерські програми, експортні канали.	
		4. Затвердити нову ринкову стратегію на рівні керівництва.	

Джерело: сформовано авторами

Висновки та перспективи подальших розвідок у даному напрямі.

Цифрова трансформація має значний вплив на систему забезпечення економічної безпеки підприємства, водночас вона відкриває широкі можливості для її забезпечення але при цьому створює нові ризики її безпеці. В роботі було представлено загальні підходи до інтерпретації економічної безпеки підприємства, окреслено її ключові складові та виявлено особливості забезпечення в контексті цифрової трансформації. Досліджено методологічні підходи до розрахунку інтегрованої оцінки економічної безпеки, зокрема з точки зору нормалізації показників, що дозволяє проводити комплексну оцінку рівня економічної безпеки підприємства та формувати обґрунтовані управлінські рішення. З метою покращення забезпечення економічної безпеки підприємства в умовах цифрової трансформації була розроблена стратегія покращення рівня економічної безпеки з використанням сценаріїв дій для її стабілізації.

Таким чином, результати дослідження формують основу для подальшого науково-практичного розвитку методів оцінки та управління економічною безпекою в умовах постійно зростаючої цифровізації економічних процесів.

Література

1. Сонюк О. В. Понятійно-категоріальний апарат безпекознавства. *СЕ. Зовнішня торгівля: економіка, фінанси, право*. 2021. Т. 117, № 4. С. 85-95. URL: [https://doi.org/10.31617/zt.knute.2021\(117\)08](https://doi.org/10.31617/zt.knute.2021(117)08) (дата звернення: 01.11.2025).
2. Фінансово-економічна безпека підприємств України: стратегія та механізми забезпечення : монографія / Т. Г. Васильців та ін. Львів : «Ліга-Прес», 2012. 387 с. URL: <https://ird.gov.ua/irdp/p20120802.pdf> (дата звернення: 01.11.2025).
3. Економічна безпека підприємства за загальною редакцією доктора економічних наук А. М. Дідика : підручник / А. М. Дідик та ін. Львів : "Вид. група "Бухгалтери України", 2019. 624 с. URL: <https://elar.navs.edu.ua/server/api/core/bitstreams/2b2cf7c7-010b-4d1e-8d46-41c79e4b0fb4/content> (дата звернення: 01.11.2025).
4. Онищенко В. О., Козаченко Г. В. Економічна безпека: держава, регіон, підприємство : монографія. Полтава : Полтав. нац. техн. ун-т ім. Юрія Кондратюка, 2016. Т. 1 : Економічна безпека: держава, регіон, підприємство :. 280 с. URL: <https://reposit.nupp.edu.ua/handle/PoltNTU/4003> (дата звернення: 01.11.2025).
5. Мельник С. І. Управління фінансовою безпекою підприємств: теорія, методологія, практика : монографія. Львів : "Растр-7", 2020. 284 с. URL: <http://dspace.lvduvs.edu.ua/handle/1234567890/3284> (дата звернення: 01.11.2025).
6. Безпека підприємництва : монографія / О. С. Гавриш та ін. Дніпро : СПД Біла К. О., 2020. 180 с. URL: <http://info.dgu.edu.ua/handle/123456789/30> (дата звернення: 01.11.2025).
7. Барні Дж. Ресурси підприємства та стійка конкурентна перевага // *Journal of Management*. 1991. Т. 17, № 1. С. 99-120. URL: <https://doi.org/10.1177/014920639101700108> (дата звернення: 01.11.2025).

8. Каплан Р. С., Нортон Д. П. Трансформація системи збалансованих показників від інструменту вимірювання результативності до стратегічного управління: Частина I // Accounting Horizons. 2001. Т. 15, № 1. С. 87-104. URL: <https://doi.org/10.2308/acch.2001.15.1.87> (дата звернення: 01.11.2025).

9. Сігалас К., Пападакіс В. Емпіричне дослідження взаємозв'язків між конкурентною перевагою та вищою результативністю // Journal of Strategy and Management. 2018. Т. 11, № 1. С. 81-111. URL: <https://doi.org/10.1108/jsma-01-2017-0010> (дата звернення: 01.11.2025).

10. Норт Д. К. Інституції, інституційні зміни та економічна ефективність // Population and Development Review. 1991. Т. 17, № 4. С. 742. URL: <https://doi.org/10.2307/1973612> (дата звернення: 01.11.2025).

11. Мельник С. І., Штангрет І. А. Економічна безпека підприємства в умовах цифрової трансформації економіки: теоретичні та практичні аспекти : монографія. Львів : Растр-7, 2025. 256 с. URL: <https://dspace.lvduvs.edu.ua/handle/1234567890/8735> (дата звернення: 01.11.2025).

12. Шаталов В. О, Пасенченко Ю. А. Моделювання економічної безпеки підприємства з використанням багатофакторної нечіткомножинної модел. *Актуальні проблеми економіки та управління : збірник наукових праць молодих вчених*. 2017. Т. 1, № 11. С. 1-9. URL: <https://ela.kpi.ua/items/62c2da0e-e71a-4e40-876d-f9cb21f49732> (дата звернення: 01.11.2025).

13. Про Методичні рекомендації щодо виявлення ознак неплатоспроможності підприємств та ознак дій з приховування банкрутства, фіктивного банкрутства чи доведення до банкрутства : Лист Вищ. арбітр. суду України від 11.04.2001 № 01-8/451. URL: <https://zakon.rada.gov.ua/rada/show/v0014665-06#Text> (дата звернення: 01.11.2025).

14. Урдуханов Р. І. Система індикаторів оцінювання стану кадрової безпеки на підприємстві. *Економіка і організація управління*. 2022. № 3. С. 104-113. URL: <https://doi.org/10.31558/2307-2318.2022.3.11> (дата звернення: 01.11.2025).

15. Кузьмін О. Є. Управління міжнародною конкурентоспроможністю підприємства : підручник. Львів : Вид-во "Компакт-ЛВ", 2005. – 304 с.

16. Модель зрілості кібербезпекових можливостей у відповідності до NIST Cybersecurity Framework. NIST | NCCoE. URL: <https://www.nccoe.nist.gov/news-insights/cybersecurity-capability-maturity-model-nist-cybersecurity-framework-mapping> (дата звернення: 01.11.2025).

References

1. Sonuk, S.V. (2021), “Conceptual and categorical apparatus of security science”, *Foreign Trade: Economics, Finance, Law*, vol. 117, no. 4, pp. 85-95. doi: 10.31617/zt.knute.2021(117)08.

2. Vasylytsiv, T.H. (2012), *Finansovo-ekonomichna bezpeka pidpryiemstv Ukrainy: stratehiia ta mekhanizmy zabezpechennia* [Financial and economic security of Ukrainian enterprises: strategy and mechanisms of ensuring], Liha-Pres, Lviv, Ukraine, available at: ird.gov.ua/irdp/p20120802.pdf (Accessed 01 November 2025).

3. Didyk, A.M. (2019), *Ekonomichna bezpeka pidpryiemstva* [Enterprise economic security], Vydavnycha hrupa “Bukhgaltery Ukrainy”, Lviv, Ukraine, available at: elar.navs.edu.ua/server/api/core/bitstreams/2b2cf7c7-010b-4d1e-8d46-41c79e4b0fb4/content (Accessed 01 November 2025).

4. Onyshchenko, V.O., and Kozachenko, H.V. (2016), *Ekonomichna bezpeka: derzhava, rehion, pidpryiemstvo* [Economic security: state, region, enterprise], vol. 1, Poltava National Technical University named after Yuriy Kondratyuk, Poltava, Ukraine, available at: reposit.nupp.edu.ua/handle/PolNTU/4003 (Accessed 01 November 2025).

5. Melnyk, S.I. (2020), *Upravlinnia finansovoiu bezpekoiu pidpriemstv: teoriia, metodolohiia, praktyka* [Financial security management of enterprises: theory, methodology, practice], Rastr-7, Lviv, Ukraine, available at: dspace.lvduvs.edu.ua/handle/1234567890/3284 (Accessed 01 November 2025).
6. Havrysh, O.S. (2020), *Bezpeka pidpriemnytstva* [Enterprise security], SPD Bila K.O., Dnipro, Ukraine, available at: info.dgu.edu.ua/handle/123456789/30 (Accessed 01 November 2025).
7. Barney, J. (1991), "Firm resources and sustained competitive advantage", *Journal of Management*, vol. 17, no. 1, pp. 99-120. doi: 10.1177/014920639101700108.
8. Kaplan, R.S. and Norton, D.P. (2001), "Transforming the Balanced Scorecard from Performance Measurement to Strategic Management: Part I", *Accounting Horizons*, vol. 15, no. 1, pp. 87-104. doi: 10.2308/acch.2001.15.1.87.
9. Sigalas, C. and Papadakis, V. (2018), "Empirical investigation of relationship patterns between competitive advantage and superior performance", *Journal of Strategy and Management*, vol. 11, no. 1, pp. 81-111. doi: 10.1108/jsma-01-2017-0010.
10. North, D.C. (1991), "Institutions, institutional change and economic performance", *Population and Development Review*, vol. 17, no. 4, p. 742. doi: 10.2307/1973612.
11. Melnyk, S.I. and Shtanhret, I.A. (2025), *Ekonomichna bezpeka pidpriemstva v umovakh tsyfrovoy transformatsii ekonomiky: teoretychni ta praktychni aspekty* [Economic security of enterprises under digital economic transformation: theoretical and practical aspects], Rastr-7, Lviv, Ukraine, available at: dspace.lvduvs.edu.ua/handle/1234567890/8735 (Accessed 01 November 2025).
12. Shatalov, V.O. and Pasenchenko, Yu.A. (2017), "Modeling the economic security of an enterprise using a multi-factor fuzzy model", *Aktualni problemy ekonomiky ta upravlinnia*, vol. 1, no. 11, pp. 1-9, available at: ela.kpi.ua/items/62c2da0e-e71a-4e40-876d-f9cb21f49732 (Accessed 01 November 2025).

13. The High Arbitration Court of Ukraine (2001), Letter “On methodological recommendations for identifying signs of insolvency of enterprises and signs of actions to conceal bankruptcy, fictitious bankruptcy or bringing to bankruptcy”, available at: zakon.rada.gov.ua/rada/show/v0014665-06#Text (Accessed 01 November 2025).

14. Urdukhanov, R.I. (2022), “System of indicators for assessing personnel security at an enterprise”, *Ekonomika i orhanizatsiia upravlinnia*, vol. 3, pp. 104–113. doi: 10.31558/2307-2318.2022.3.11.

15. Kuzmin, O.E. (2005), *Upravlinnia mizhnarodnoi konkurentospromozhnistiu pidpriemstva* [Managing international competitiveness of the enterprise], Kompakt-LV, Lviv, Ukraine.

16. NIST (2025), “Cybersecurity Capability Maturity Model to NIST Cybersecurity Framework Mapping”, *NIST | NCCoE*, available at: nccoe.nist.gov/news-insights/cybersecurity-capability-maturity-model-nist-cybersecurity-framework-mapping (Accessed 01 November 2025).

Стаття надійшла до редакції 12.11.2025 р.