УДК 336.1:338.24
JEL: G32; M14; O33
DOI: https://doi.org/10.32983/2222-4459-2026-5-379-387

СТРАТЕГІЯ ТА МЕХАНІЗМ ФІНАНСОВО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ ЯК ФАКТОР ФІНАНСОВОЇ СТІЙКОСТІ ДЕРЖАВИ

©2026 **БАЛАШОВА О. В.**

УДК 336.1:338.24
JEL: G32; M14; O33

Балашова О. В. Стратегія та механізм фінансово-економічної безпеки підприємств як фактор фінансової стійкості держави

У сучасних умовах функціонування вітчизняних суб'єктів господарювання питання забезпечення їхньої фінансово-економічної безпеки (ФЕБ) набуває критичного значення через повномасштабну агресію, високу волатильність ринків і системну невизначеність. Стійкість окремого підприємства сьогодні виступає фундаментальною запорукою фінансової міцності всієї держави, що потребує перегляду застарілих методів управління на користь синергетичного підходу. Мета статті полягає у формуванні та науковому обґрунтуванні цілісного механізму забезпечення ФЕБ підприємств, що базується на інтеграції математичного моделювання, цифрових інновацій та стратегічної орієнтації на корпоративну соціальну відповідальність. Використано методи: синергетичний підхід – для інтерпретації безпеки як динамічного стану системи; апарат теорії ігор – для оптимізації управлінських рішень в умовах конфлікту інтересів; багатокритеріальне оцінювання – для розрахунку інтегральних індикаторів ФЕБ; метод моделювання – при розробці архітектури цифрового контуру. Досліджено трансформацію систем захисту підприємств в умовах воєнного стану, зокрема процеси релокації та адаптації до агресивного зовнішнього середовища. За результатами дослідження сформовано трирівневу архітектуру цифрового контуру безпеки, що поєднує внутрішні ERP-дані та зовнішню аналітику платформ SupTech із використанням алгоритмів штучного інтелекту. Встановлено, що впровадження предиктивного моніторингу та щоденної генерації «профілю загрози» дозволяє трансформувати безпеку з витратної функції у стратегічний актив. Наукова новизна полягає в розробці механізму, що вперше поєднує математичну точність «змішаних стратегій» захисту із гуманітарним вектором корпоративної соціальної відповідальності (стандарт ISO 26000), що створює ефект «репутаційного щита». Практичні рекомендації включають запропоновану матрицю функціональних обов'язків у системі ФЕБ, яка забезпечує координацію між технологічними інструментами (RegTech) та соціальним вектором захисту, що є базовим чинником для повоєнного відновлення суб'єктів господарювання та зміцнення економічного суверенітету України.

Ключові слова: *фінансово-економічна безпека; синергетичний підхід; теорія ігор; штучний інтелект; корпоративна соціальна відповідальність; релокація бізнесу; цифрова стійкість; фінансова стабільність держави.*
Рис.: *2.* ***Табл.:*** *3.* ***Бібл.:*** *18.*

Балашова Олена Віталіївна *– кандидат економічних наук, доцент, доцент кафедри фінансів, обліку та бізнесу, Донбаська державна машинобудівна академія (вул. Академічна, 72, Краматорськ, 84313, Україна)*
E-mail: *dgmabalashova@gmail.com*
ORCID: *https://orcid.org/0009-0006-8928-2148*

UDC 336.1:338.24
JEL: G32; M14; O33

Balashova O. V. Strategy and Mechanism of Financial and Economic Security of Enterprises as a Factor of Financial Stability of the State

In modern conditions of functioning of domestic economic entities, the issue of ensuring their financial and economic security (FES) becomes critical due to the ongoing full-scale aggression, high market volatility, and systemic uncertainty. The resilience of an individual enterprise today is a fundamental guarantee of the financial strength of the entire State, which requires a revision of outdated management methods in favor of a synergistic approach. The aim of the article is to form and scientifically substantiate a holistic mechanism for ensuring the FES of enterprises, based on the integration of mathematical modeling, digital innovations, and strategic orientation towards corporate social responsibility. Methods used: a synergistic approach for interpreting security as a dynamic state of the system; the apparatus of game theory for optimizing managerial decisions in conflict interests; multi-criteria assessment for calculating integrated FES indicators; modeling method in developing the architecture of the digital security circuit. The transformation of enterprise protection systems under martial law, particularly the processes of relocation and adaptation to an aggressive external environment, was examined. According to the research results, a three-level architecture of the digital security circuit was formed, combining internal ERP data and external analytics of SupTech platforms using artificial intelligence algorithms. It was found that the implementation of predictive monitoring and daily generation of a "threat profile" allows transforming security from a cost function into a strategic asset. Scientific novelty lies in the development of a mechanism that for the first time combines the mathematical accuracy of «threat profile» allows transforming security from a cost function into a strategic asset. Scientific novelty lies in the development of a mechanism that for the first time combines the mathematical accuracy of «mixed strategies» effect. Practical recommendations include the proposed matrix of functional responsibilities in the FES system, which ensures coordination between technological tools (RegTech) and the social vector of protection, which is a basic factor for the postwar recovery of business entities and strengthening the economic sovereignty of Ukraine.

Keywords: *financial and economic security; synergistic approach; game theory; artificial intelligence; corporate social responsibility; business relocation; digital resilience; financial stability of the State.*
Fig.: *2.* ***Tabl.:*** *3.* ***Bibl.:*** *18.*

Balashova Olena V. *– PhD (Economics), Associate Professor, Associate Professor of the Department of Finance, Accounting and Business, Donbass State Academy of Machine Building (72 Akademichna Str., Kramatorsk, 84313, Ukraine)*
E-mail: *dgmabalashova@gmail.com*
ORCID: *https://orcid.org/0009-0006-8928-2148*

У сучасних умовах функціонування вітчизняних суб'єктів господарювання питання забезпечення їхньої фінансово-економічної безпеки (ФЕБ) набуває критичного значення. Повномасштабна агресія, висока волатильність ринків та системна невизначеність змушують відмовитися від застарілих кібернетичних методів управління на користь синергетичного підходу. Стійкість окремого підприємства сьогодні є не лише приватним інтересом власників, а й фундаментальною запорукою фінансової міцності всієї держави [1]. Необхідність інтеграції новітніх цифрових інструментів та принципів соціальної відповідальності в єдиний механізм захисту визначає актуальність даного дослідження.

Огляд літератури та аналіз попередніх досліджень. Дослідження теоретико-методологічних засад фінансово-економічної безпеки (ФЕБ) свідчить про глибоку трансформацію наукової парадигми: від жорсткого кібернетичного управління ресурсами до синергетичного підходу. У межах синергетики безпека розглядається як динамічний стан самоорганізації й адаптивності підприємства до агресивного середовища, що знайшло відображення у працях В. О. Гаркуші та В. Ю. Єршової [2].

Теоретичний базис формування механізмів регулювання фінансової безпеки на рівні суб'єктів господарювання ґрунтовно закладений у дослідженнях С. Т. Омарової (S. T. Omarova) [3]. Окремої уваги заслуговують особливості формування фінансових стратегій підприємств у контексті євроінтеграційних процесів, що детально розглянуто у праці В. Хаустової та М. Іванова (V. Khaustova, M. Ivanov) [4], обґрунтовано використання математичного моделювання для управління ризиками, що є критичним для забезпечення стійкості в умовах цифрової трансформації. Водночас нормативно-методичне підґрунтя оцінювання рівня захищеності підприємств проаналізовано П. Пилипишиним (P. Pylypyshyn) та співавторами [5]. Питання ідентифікації загроз у галузевому розрізі та їхнього впливу на стабільність економічного розвитку висвітлено у працях Т. Зубко (T. Zubko) [6] та О. В. Базик [7].

У сучасних роботах виокремлюються три магістральні напрями формування теоретичного підґрунтя ФЕБ:

1. ***Математично-інструментальний:*** використання математичних моделей і нейронних мереж для виявлення кіберзагроз у цифрових системах детально обґрунтовано у дослідженні Л. Загоруйко (L. Zahoruiko) та співавторів [8].

2. ***Технологічний:*** впровадження цифрових інновацій, технологій Big Data та ШІ для предиктивного моніторингу загроз (В. Федун зі співавторами, Н. О. Батьковець) [9; 10].

3. ***Соціально-орієнтований:*** інтеграція принципів корпоративної соціальної відповідальності (КСВ) та стандартів ISO 26000 як інструментів сталого розвитку та безпеки підприємства, що детально розглянуто в дослідженні Г. Назарової (G. Nazarova) та співавторів [11].

Попри значний науковий доробок, аналіз джерел дозволяє виявити низку суперечностей. Зокрема, наявні методики (наприклад, З. Шило [12]) часто фокусуються на ретроспективному аналізі фінансових показників, що в умовах воєнного стану та високої волатильності ринку має обмежену прогностичну цінність. Крім того, більшість досліджень розглядають цифровізацію (RegTech, SupTech) та соціальну відповідальність як окремі, не пов'язані між собою елементи, не пропонуючи цілісного механізму їхньої синергетичної взаємодії [13].

Таким чином, наукова прогалина спостерігається в тому, що досі залишається недостатньо вивченим питання побудови інтегрованого механізму ФЕБ, який би одночасно поєднував:

- математичну точність вибору «змішаних стратегій» захисту в умовах конфлікту інтересів;
- автоматизований цифровий контур предиктивного аналізу;
- гуманітарний вектор (КСВ) як засіб нівелювання кадрових і репутаційних ризиків.

Саме необхідність синтезу цих різновекторних інструментів у єдину адаптивну систему в умовах воєнного стану та завдань повоєнного відновлення визначає наукову новизну та напрям даного дослідження.

Мета дослідження полягає у формуванні та обґрунтуванні цілісного механізму забезпечення фінансово-економічної безпеки (ФЕБ) суб'єктів господарювання, що ґрунтується на синергії математичного моделювання, цифрових інновацій та стратегічної орієнтації на соціальну відповідальність в умовах агресивного зовнішнього середовища.

Логіка даного дослідження побудована на перевірці низки наукових припущень щодо трансформації систем захисту підприємств. Зокрема, висунуто гіпотезу, згідно з якою перехід від традиційного кібернетичного управління до синергетичного підходу дозволяє суб'єкту господарювання трансформувати статичний стан захищеності в динамічну модель самоорганізації, що здатна гнучко адаптуватися до екстремальних змін середовища.

Дослідження виконано в межах держбюджетної НДР (номер державної реєстрації Дк-02-2024 – 0124U004244). «Детермінанти забезпечення фінансово-економічної безпеки країни у контексті актуальних потреб сучасності: державний, регіональний, корпоративний вимір».

Розвиваючи цю ідею, автор припускає (гіпотеза 2), що синергетичне поєднання технологій штучного інтелекту (AI) та принципів корпоративної соціальної відповідальності (КСВ) у межах єдиного цифрового контуру створює особливий ефект «репутаційного щита». Це не лише мінімізує поточні ризики, а й забезпечує предиктивний захист від фінансових втрат через зміцнення довіри стейкхолдерів. У межах перевірки зазначених гіпотез ключовим дослідницьким питанням статті є визначення потенціалу апарату теорії ігор у процесі оптимізації «змішаних стратегій» безпеки, що дозволило б знайти баланс інтересів та забезпечити стійкість підприємства в умовах гострого конфлікту інтересів та зовнішньої агресії.

Методи дослідження. Методологічний апарат дослідження базується на комплексному застосуванні загальнонаукових і спеціальних методів, що дозволяють розкрити багатоаспектну природу фінансово-економічної безпеки. Фундаментом роботи виступає синергетичний підхід, у межах якого безпека суб'єкта господарювання інтерпретується не як статичний показник, а як складний динамічний стан системи, що безперервно еволюціонує та адаптується до зовнішніх збурень. Для формалізації процесів прийняття управлінських рішень в умовах стратегічної невизначеності та конфліктного середовища (зокрема, у форматі «гри проти природи» або агресивного ринку) було застосовано апарат теорії ігор.

Діагностична частина дослідження реалізована через метод багатокритеріального оцінювання, що дозволив розрахувати інтегральні індикатори ФЕБ (ліквідність, автономію, ділову активність) та детермінувати їхні критичні порогові значення. Крім того, застосування методу моделювання стало підґрунтям для розробки архітектури цифрового контуру безпеки та ієрархічної структури рівнів корпоративної соціальної відповідальності.

Інформаційний базис дослідження сформовано на засадах переходу від аналізу ретроспективної звітності до опрацювання даних у режимі реального часу. Доказову базу склали внутрішні дані суб'єктів господарювання (вивантаження з ERP-систем, бухгалтерських модулів та CRM-платформ), а також зовнішні джерела – відомості державних реєстрів, результати моніторингу ринкових контирувань та аналітика цифрових платформ SupTech. Нормативну верифікацію результатів забезпечено відповідністю положенням Закону України «Про національну безпеку» [14] та міжнародного стандарту ISO 26000:2010 [15].

Обробка масивів неструктурованої інформації та автоматизація комплаєнс-контролю здійснювалися із залученням сучасного програмного інструментарію, зокрема технологій Big Data, RegTech та AI-алгоритмів (нейромереж), призначених для генерації щодобового «профілю загрози».

Емпірична перевірка запропонованих рішень базується на вибірці ретроспективних даних фінансової звітності вітчизняних підприємств за останні три роки. Це дозволило на етапі аудиту та діагностики встановити індивідуальні порогові значення показників, що є необхідним для функціонування предиктивної системи моніторингу.

Результати дослідження. Для практичної імплементації розроблених теоретичних положень пропонується концептуальний алгоритм, що дозволяє системно розпізнавати, аналізувати та нівелювати загрози (*рис. 1*). Застосування цього алгоритму забезпечує безперервність моніторингу внутрішніх бізнес-процесів та дає змогу вчасно коригувати стратегічні цілі відповідно до динамічних змін ринкової кон'юнктури. Реалізація цього механізму в межах даного дослідження включає такі розширені стадії:

1. Діагностична стадія: якісна оцінка загроз. На цьому етапі здійснюється первинна фільтрація чинників впливу. Головна мета – відокремити фоновий шум від реальних загроз, які можуть призвести до втрати платоспроможності або зупинки бізнес-процесів.

2. Аналітична стадія: кількісний аналіз. За умов високої невизначеності проводиться математичне вимірювання параметрів ризику. Використання стохастичних моделей дозволяє визначити ймовірність настання негативних подій та потенційний обсяг фінансових втрат, що є критичним для розрахунку необхідних резервів.

3. Стратегічна стадія: вибір моделі реагування. На основі синтезу якісних і кількісних даних приймається рішення щодо подальшої долі кожного ризику. Підприємство може обрати шлях активного протистояння (якщо загроза подолана) або шлях уникнення/трансформації діяльності (якщо ресурсів для захисту недостатньо).

4. Інструментальна стадія: імплементація засобів захисту. Це етап безпосереднього впливу, де застосовуються два типи інструментів: внутрішні інструменти, які спрямовані на зміцнення внутрішнього середовища підприємства (жорстке лімітування витрат, диверсифікація продуктового портфеля та формування страхових фондів (самострахування)); зовнішні інструменти – це перерозподіл ризиків у зовнішньому середовищі через механізми страхування або специфічні умови контрактів із партнерами.

Застосування такого комплексного підходу забезпечує суб'єкту господарювання високий рівень захищеності операційної та інвестиційної діяль-

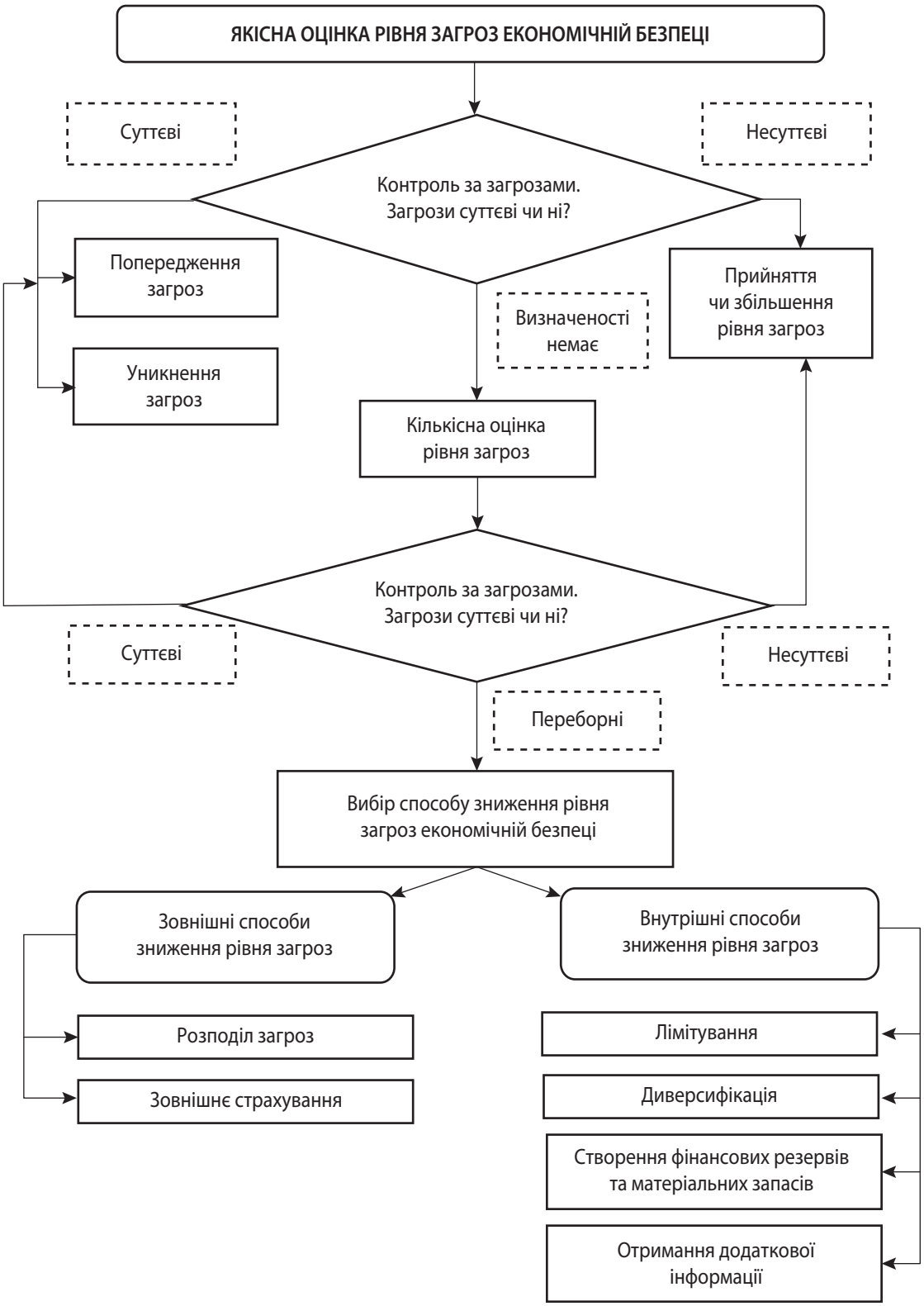

Рис. 1. Концептуальна модель ідентифікації та нівелювання загроз економічній безпеці підприємства

Джерело: сформовано автором на основі [6; 7].

ності. Більше того, масове впровадження подібних механізмів на рівні вітчизняних підприємств створює ефект «колективного імунітету» для економіки України, де стійкість окремого бізнесу стає надійним бар'єром проти загальнодержавних фінансових криз.

ЕКОНОМІКО-МАТЕМАТИЧНЕ ОБҐРУНТУВАННЯ СТРАТЕГІЧНИХ РІШЕНЬ ТА СИСТЕМА МОНІТОРИНГУ

Ключовим елементом запропонованого механізму є перехід від інтуїтивного до науково об-

ґрунтованого вибору стратегії безпеки. В умовах конфліктного середовища, де дії зовнішніх контрагентів або агресивного ринку є невизначеними, процес прийняття рішень формалізується як математична модель «гри проти природи».

Згідно з цією моделлю підприємство прагне знайти таку «змішану стратегію», яка мінімізує максимальні можливі втрати (критерій мінімаксу). Математично оптимальна стратегія P^* визначається як вектор імовірностей застосування різних інструментів захисту, що забезпечує стійкість системи навіть за найнесприятливішого сценарію розвитку подій.

Для інформаційного наповнення цієї моделі та забезпечення предиктивного (випереджального) реагування розроблено систему діагностичних показників. На відміну від стандартного фінансового аналізу дана система орієнтована на ідентифікацію «точок біфуркації» – моментів, коли показник наближається до критичної межі (*табл. 1*).

Інтеграція цих показників у єдиний моніторинговий контур дозволяє службі ФЕБ підприємства не просто констатувати факт погіршення стану, а діяти на випередження. Кожне відхилення від порогового значення стає сигналом для запуску відповідного алгоритму нівелювання загроз, описаного в попередньому блоці.

Особливе місце в цій системі посідає використання нейромережевих моделей, які здатні аналізувати кореляції між цими показниками в реальному часі, формуючи динамічний «профіль ризику» підприємства.

ЦИФРОВА ТРАНСФОРМАЦІЯ ТА СОЦІАЛЬНИЙ ВЕКТОР МЕХАНІЗМУ БЕЗПЕКИ

У межах дослідження обґрунтовано, що сучасний механізм ФЕБ не може обмежуватися лише фінансовими інструментами. Для забезпечення життєздатності підприємства в умовах воєнного стану та глобальної цифровізації запропоновано інтегровану архітектуру, що поєднує технологічний та гуманітарний аспекти.

Цифровий контур безпеки базується на впровадженні інструментів RegTech та AI-моніторингу. Це дозволяє автоматизувати комплаєнс-процедури та здійснювати предиктивний аналіз великих масивів даних (Big Data) для виявлення прихованих загроз.

Запропонована архітектура (*рис. 2*) функціонує як динамічна екосистема, де дані з внутрішніх ERP-систем і зовнішніх цифрових платформ SupTech агрегуються в «Центрі аналізу ризиків». Використання Cloud-обробки дозволяє забезпечити безперебійність моніторингу навіть за умов фізичного пошкодження локальної інфраструктури, що є критично важливим для релокованих підприємств. Ключовою перевагою такого контуру є формування щоденного «профілю загрози», який трансформує суб'єктивні оцінки менеджменту в об'єктивні цифрові індикатори.

Водночас, технологічна стійкість має бути підкріплена високим рівнем довіри з боку стейкхолдерів. У межах синергетичного підходу цифрова безпека доповнюється гуманітарним вектором – корпоративною соціальною відповідальністю (КСВ). Вона виступає не лише як етичний орієнтир, а як дієвий механізм мінімізації кадрових ризиків та зміцнення репутаційного капіталу підприємства.

Для систематизації цього впливу та визначення стратегічних пріоритетів було розроблено ієрархічну модель рівнів соціальної відповідальності (*табл. 2*). Кожен рівень цієї моделі відповідає конкретним інструментам, що безпосередньо впливають на загальний рівень захищеності суб'єкта господарювання.

Таблиця 1

Система ключових індикаторів моніторингу фінансово-економічної безпеки суб'єкта господарювання

Група показників	Ключовий індикатор	Рекомендоване (порогове) значення	Функція в системі безпеки
Фінансова стійкість	Коефіцієнт автономії	> 0,5	Визначає ступінь незалежності від зовнішніх кредиторів
Ліквідність	Коефіцієнт поточної ліквідності	1,5–2,0	Предиктивна оцінка спроможності виконувати зобов'язання
Ділова активність	Оборотність дебіторської заборгованості	Зростання в динаміці	Моніторинг ризиків втрати оборотного капіталу
Ринкова позиція	Частка ринку / Рентабельність продажів	Не нижче середньогалузевого	Оцінка конкурентної стійкості та репутаційного капіталу

Джерело: складено автором.

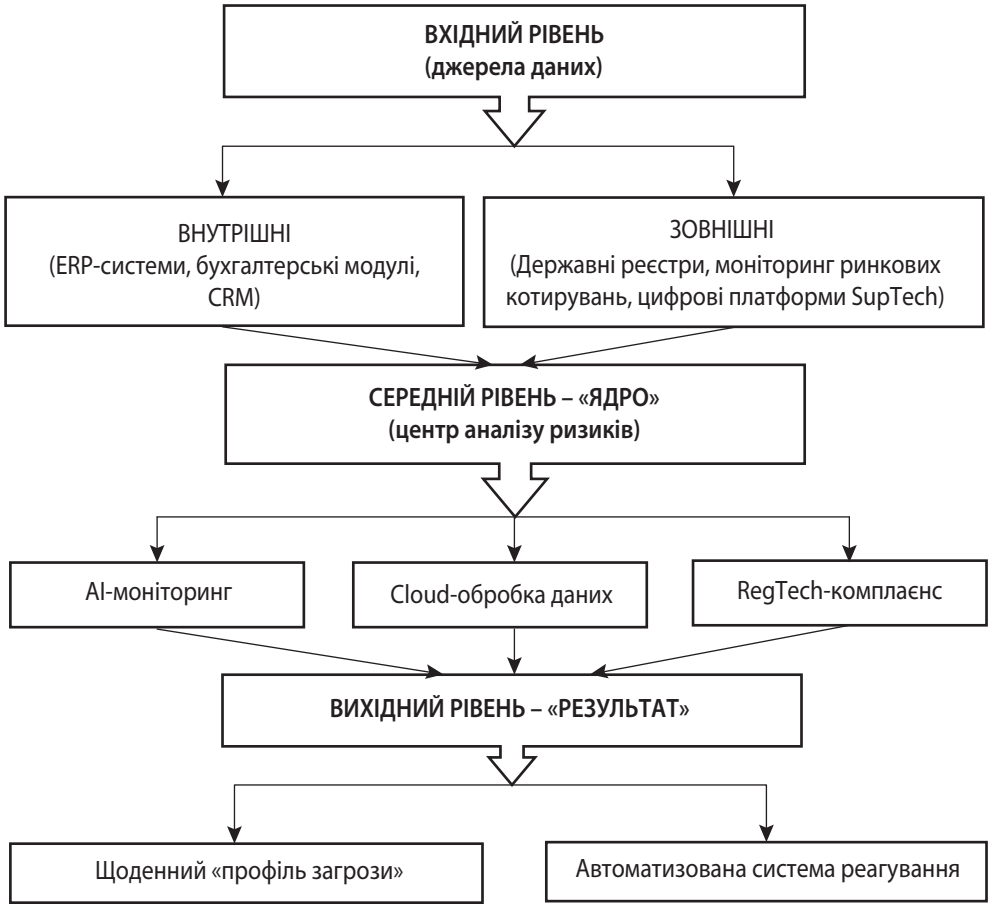

Рис. 2. Архітектура цифрового контуру фінансово-економічної безпеки підприємства

Джерело: авторська розробка.

Таблиця 2

Ієрархічна модель рівнів соціальної відповідальності в системі ФЕБ

Рівень КСВ	Основні інструменти та заходи	Вплив на безпеку підприємства
Економічний	Сплата податків, створення робочих місць, етична бізнес-практика	Зниження регуляторних ризиків, прозорість діяльності
Юридичний	Дотримання трудового права, антикорупційні заходи	Захист від правових зазіхань, мінімізація судових витрат
Етичний	Підтримка релокованих працівників, волонтерство, екологічні ініціативи	Зміцнення репутаційного капіталу («репутаційний щит»)
Філантропічний	Грантові програми, підтримка громад, розвиток інфраструктури	Формування лояльного середовища стейкхолдерів

Джерело: сформовано автором на основі [11; 13].

Синергія цифрового контуру та соціального вектора дозволяє службі безпеки підприємства не лише нівелювати прямі фінансові втрати, а й створювати стратегічний запас стійкості (гудвіл), що є вирішальним фактором у кризові періоди. Таке поєднання технологічних та етичних інструментів трансформує безпеку з витратної функції у стратегічний актив.

Проте успішна реалізація запропонованого механізму неможлива без чіткого розподілу функціональних обов'язків усередині підприємства. Організаційний етап передбачає трансформацію традиційного відділу охорони в повноцінну *службу фінансово-економічної безпеки*.

Важливо підкреслити, що така реорганізація потребує не лише зміни назви підрозділу, а й якіс-

ного оновлення компетенцій персоналу. Ключовий акцент переміщується з фізичного нагляду на інтелектуально-аналітичну підтримку бізнес-процесів та предиктивне реагування. Кожен фахівець оновленої служби має оперувати даними цифрового контуру, інтегруючи результати AI-моніторингу в конкретні управлінські рішення. Для забезпечення координації між технологічними та соціальними векторами захисту діяльність служби базується на матриці відповідальності (*табл. 3*).

Таблиця 3

Організаційне забезпечення та розподіл функцій у системі ФЕБ підприємства

Підрозділ / Посада	Ключові функції в межах механізму	Очікуваний результат
Аналітик з ризиків (AI-оператор)	Моніторинг цифрового контуру, верифікація сигналів від нейромережі	Щоденний звіт про «профіль загрози»
Спеціаліст з комплаєнсу (RegTech)	Автоматизована перевірка контрагентів, контроль за дотриманням норм	Мінімізація юридичних і штрафних санкцій
Менеджер із соціальної відповідальності	Реалізація програм КСВ, взаємодія зі стейкхолдерами	Зміцнення репутаційного щита
Керівник служби ФЕБ	Прийняття стратегічних рішень за результатами теоретико-ігрового моделювання	Оптимальна модель реагування на загрози

Джерело: складено автором.

Запропонована структура розподілу обов'язків дозволяє уникнути дублювання функцій та забезпечує комплексне охоплення всіх аспектів безпеки – від кіберзахисту до управління соціальним капіталом.

Обговорення. Отримані результати підтверджують і розширюють сучасні наукові погляди на природу фінансово-економічної безпеки суб'єктів господарювання. Перехід від кібернетичної до синергетичної парадигми, запропонований у роботі, корелює із висновками О. Ареф'євої, В. Титикало та Коваленко Н. [16] щодо необхідності адаптивного управління в умовах нестабільності. Проте, на відміну від наявних підходів, які часто обмежуються фінансовим моніторингом, наш механізм інтегрує технологічний (AI, RegTech) та гуманітарний (КСВ) контури в єдину систему.

Використання апарату теорії ігор для вибору стратегій безпеки дозволяє подолати суб'єктивізм управлінських рішень, на який звертає увагу О. Ю. Самборська [17]. Застосування критерію «мінімаксу» є особливо актуальним для підприємств України, що працюють в умовах воєнного стану, оскільки воно орієнтує менеджмент на виживання та збереження капіталу за найгірших сценаріїв.

Особливої уваги заслуговує питання релокації та збереження кадрового потенціалу. Як зазначають Н. Смочко та Т. Лужанська [18], для підприємств, що переміщені в безпечніші регіони (зокрема, у Закарпаття), соціальна відповідальність стає критичним чинником утримання фахівців. Наша модель підтверджує цей факт, демонструючи, що етичний рівень КСВ (див. табл. 2) створює «репутаційний щит», який нівелює кадрові ризики та сприяє швидшій адаптації на нових ринках.

Обмеження дослідження. Попри комплексність запропонованого механізму, його імплементація має певні обмеження. *По-перше*, ефективність цифрового контуру (див. рис. 2) критично залежить від якості та повноти вхідних даних (Big Data), що може бути проблематичним для малого бізнесу з низьким рівнем автоматизації. *По-друге*, математичні моделі теорії ігор потребують періодичного перегляду параметрів «гри» через надвисоку швидкість зміни зовнішніх загроз у воєнний час.

ВИСНОВКИ

У ході проведеного дослідження сформовано цілісний механізм забезпечення фінансово-економічної безпеки суб'єктів господарювання, що дозволяє зробити такі висновки:

1. Наукова новизна роботи полягає в переході від пасивного захисту ресурсів до формування адаптивної системи безпеки на засадах синергетичного підходу. Обґрунтовано, що в умовах екстремальної нестабільності безпека підприємства має базуватися на принципах самоорганізації, де цифрова стійкість поєднується з високою соціальною відповідальністю.

2. Доведено ефективність використання апарату теорії ігор для формалізації управлінських рішень. Застосування стратегії «мінімаксу» дозволяє менеджменту обирати оптимальні сценарії захисту в умовах конфлікту інтересів, що мінімізує потенційні втрати капіталу навіть за найбільш несприятливих зовнішніх обставин.

3. Розроблено архітектуру цифрового контуру ФЕБ, що інтегрує технології Штучного Інтелекту, Big Data та RegTech. Це трансформує систему моніторингу з ретроспективної у предиктивну, дозволяючи формувати щоденний «профіль загрози» та автоматизувати комплаєнс-процедури, що є критичним для підприємств, які пройшли через релокацію та цифрову трансформацію.

4. Встановлено, що корпоративна соціальна відповідальність (згідно з ISO 26000) відіграє роль «репутаційного щита». Вона не лише нівелює кадрові ризики, а й створює стратегічний запас довіри (гудвіл), що забезпечує життєздатність бізнесу в періоди криз та є фундаментом для його повоєнного відновлення.

Практичне значення отриманих результатів полягає в можливості впровадження запропонованої матриці організаційного забезпечення в діяльність вітчизняних підприємств. Це дозволить службам ФЕБ діяти на випередження, забезпечуючи фінансову стійкість окремих суб'єктів господарювання як необхідну умову зміцнення економічної безпеки держави в цілому.

Перспективи подальших досліджень полягають у деталізації алгоритмів машинного навчання для специфічних галузевих загроз і розробці методик кількісного оцінювання впливу КСВ на ринкову вартість підприємства в умовах воєнного стану. ■

БІБЛІОГРАФІЯ

1. Економічна безпека України в умовах високих воєнних ризиків та глобальної нестабільності : експ.-аналіт. доп. / за заг. ред. Я. Жаліла. Київ : НІСД, 2025. 104 с. DOI:https://doi.org/10.53679/NISS-analytrep.2025.03
2. Гаркуша В. О., Єршова Н. Ю. Систематизація наукових поглядів щодо сутності поняття «економічна безпека підприємства». *Економіка та суспільство*. 2021. Вип. 28. DOI: https://doi.org/10.32782/2524-0072/2021-28-34
3. Omarova S. T. Technology v Technocracy: Fintech as a Regulatory Challenge. *Journal of Financial Regulation*. 2020. Vol. 6. Iss. 1. P. 75–124. DOI: https://doi.org/10.1093/jfr/fjaa004
4. Khaustova V., Ivanov M. Mathematical modeling of risk management processes in IT companies. *Management of Economy: Theory and Practice*. 2023. No. 9. DOI: https://doi.org/10.54929/2786-5738-2023-9-04-16
5. Pylypyshyn P., Hanushchyn S., Bek U. et al. Legal regulation of the financial and economic security of Ukraine. *Financial and Credit Activity: Problems of Theory and Practice*. 2022. Vol. 1. No. 42. P. 510–521. DOI:https://doi.org/10.55643/fcaptp.1.42.2022.3747
6. Zubko T. The diagnosis of economic security of the enterprise. *Herald of Herald of Kyiv National University of Trade and Economics*. 2019. No. 6. P. 85–92. DOI: https://doi.org/10.31617/visnik.knute.2019(128)08
7. Базик О. В. Фінансово-економічна безпека у забезпеченні стабільності економічного розвитку підприємства. *Інвестиції: практика та досвід*. 2024. № 15. С. 172–177. DOI: https://doi.org/10.32702/2306-6814.2024.15.172
8. Zahoruiko L., Martianova T., Al-Hiari M. et al. Mathematical model and structure of a neural network for detection of cyber attacks on information and communication systems. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska*. 2024. Vol. 14. No. 3. P. 49–55. DOI: https://doi.org/10.35784/iapgos.6155
9. Федун В., Люба А., Ковтонюк І. Цифрові інновації та їх вплив на бухгалтерський облік. *Економічний аналіз*. 2024. Т. 34. № 2. С. 440–452. DOI: https://doi.org/10.35774/econa2024.02.440
10. Батьковець Н. О. Інформаційне забезпечення бізнес-процесів підприємств торговельної сфери. *Вісник Львівського торговельно-економічного університету. Серія «Економічні науки»*. 2024. № 77. С. 62–66. DOI: https://doi.org/10.32782/2522-1205-2024-77-09
11. Nazarova G., Nazarov N., Semenchenko A. et al. The role definition of corporate social responsibility in ensuring sustainable development of an enterprise. *Technology Audit and Production Reserves*. 2025. Vol. 4. No. 4. P. 6–12. DOI: https://doi.org/10.15587/2706-5448.2025.332953
12. Шило Ж. Методика комплексної оцінки рівня економічної безпеки підприємства. *International Science Journal of Management, Economics & Finance*. 2022. Vol. 1. No. 4. P. 17–25. DOI: https://doi.org/10.46299/j.isjmef.20220104.03
13. Холявко Н., Колоток М., Островська Н. RegTech і SupTech: переваги та напрями використання. *Науковий вісник Полісся*. 2021. № 1. С. 114–126. DOI: https://doi.org/10.25140/2410-9576-2021-1(22)-114-126
14. Закон України «Про національну безпеку України» від 21.06.2018 р. № 2469-VIII (зі змінами та доповненнями). URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
15. ISO 26000:2010. Guidance on social responsibility. URL: https://www.iso.org/standard/42546.html
16. Ареф'єва О., Титикало В., Коваленко Н. Економічний механізм забезпечення фінансової безпеки підприємств при нестабільності зовнішнього середовища. *Адаптивне управління: теорія і практика. Серія «Економіка»*. 2023. Вип. 16. DOI: https://doi.org/10.33296/2707-0654-16(32)-03
17. Самборська О. Ю. Принципові засади імплементації механізму управління бізнес-процесами у забезпеченні економічної безпеки підприємства. *Український журнал прикладної економіки та техніки*. 2024. Т. 9. № 4. С. 355–362. DOI: https://doi.org/10.36887/2415-8453-2024-4-54

18. Смочко Н., Лужанська Т. Релокація українського бізнесу як інструмент економічної безпеки в умовах військового стану. *Journal of Scientific Papers "Social Development and Security".* 2022. Vol. 12. No. 4. P. 112–118. DOI: https://doi.org/10.33445/sds.2022.12.4.10

REFERENCES

Arefieva O., Tytykalo V. & Kovalenko N. (2023). Ekonomichnyi mekhanizm zabezpechennia finansovoi bezpeky pidpryiemstv pry nestabilnosti zovnishnoho seredovyshcha [Economic mechanism of ensuring financial security of enterprises under instability of the external environment]. *Adaptyvne upravlinnia: teoriia i praktyka. Seriia «Ekonomika», 16*. https://doi.org/10.33296/2707-0654-16(32)-03

Batkovets N. O. (2024). Informatsiine zabezpechennia biznes-protsesiv pidpryiemstv torhovelnoi sfery [Information support of business processes of trade enterprises]. *Visnyk Lvivskoho torhovelno-ekonomichnoho universytetu. Seriia «Ekonomichni nauky», 77*, 62–66. https://doi.org/10.32782/2522-1205-2024-77-09

Bazyk O. V. (2024). Finansovo-ekonomichna bezpeka u zabezpechenni stabilnosti ekonomichnoho rozvytku pidpryiemstva [Financial and economic security in ensuring the stability of economic development of an enterprise]. *Investytsii: praktyka ta dosvid, 15*, 172–177. https://doi.org/10.32702/2306-6814.2024.15.172

Fedun V., Liuba A. & Kovtoniuk I. (2024). Tsyfrovi innovatsii ta yikh vplyv na bukhhalterskyi oblik [Digital innovations and their impact on accounting]. *Ekonomichnyi analiz, 2*(34), 440–452. https://doi.org/10.35774/econa2024.02.440

Harkusha V. O. & Yershova N. Yu. (2021). Systematyzatsiia naukovykh pohliadiv shchodo sutnosti poniattia «ekonomichna bezpeka pidpryiemstva» [Systematization of scientific views regarding the essence of the concept of "economic security of an enterprise"]. *Ekonomika ta suspilstvo, 28*. https://doi.org/10.32782/2524-0072/2021-28-34

iso.org. (2010). *ISO 26000:2010. Guidance on social responsibility*. https://www.iso.org/standard/42546.html

Khaustova V. & Ivanov M. (2023). Mathematical modeling of risk management processes in IT companies. *Management of Economy: Theory and Practice, 9*. https://doi.org/10.54929/2786-5738-2023-9-04-16

Kholiavko N., Kolotok M. & Ostrovska N. (2021). RegTech i SupTech: perevahy ta napriamy vykorystannia [RegTech and SupTech: advantages and directions of use]. *Naukovyi visnyk Polissia, 1*, 114–126. https://doi.org/10.25140/2410-9576-2021-1(22)-114-126

Nazarova G., Nazarov N. & Semenchenko A. (2025). The role definition of corporate social responsibility in ensuring sustainable development of an enterprise. *Technology Audit and Production Reserves, 4*(4), 6–12. https://doi.org/10.15587/2706-5448.2025.332953

Omarova S. T. (2020). Technology v Technocracy: Fintech as a Regulatory Challenge. *Journal of Financial Regulation, 1*(6), 75–124. https://doi.org/10.1093/jfr/fjaa004

Pylypyshyn P., Hanushchyn S. & Bek U. (2022). Legal regulation of the financial and economic security of Ukraine. *Financial and Credit Activity: Problems of Theory and Practice, 42*(1), 510–521. https://doi.org/10.55643/fcaptp.1.42.2022.3747

Samborska O. Yu. (2024). Pryntsypovi zasady implementatsii mekhanizmu upravlinnia biznes-protsesamy u zabezpechenni ekonomichnoi bezpeky pidpryiemstva [Principle bases of implementation of business process management mechanism in ensuring economic security of an enterprise]. *Ukrainskyi zhurnal prykladnoi ekonomiky ta tekhniky, 4*(9), 355–362. https://doi.org/10.36887/2415-8453-2024-4-54

Shylo Zh. (2022). Metodyka kompleksnoi otsinky rivnia economicnoi bezpeky pidpryiemstva [Methodology of complex assessment of the level of economic security of an enterprise]. *International Science Journal of Management, Economics & Finance, 4*(1), 17–25. https://doi.org/10.46299/j.isjmef.20220104.03

Smochko N. & Luzhanska T. (2022). Relokatsiia ukrainskoho biznesu yak instrument ekonomichnoi bezpeky v umovakh viiskovoho stanu [Relocation of Ukrainian business as a tool of economic security under martial law conditions]. *Journal of Scientific Papers "Social Development and Security", 4*(12), 112–118. https://doi.org/10.33445/sds.2022.12.4.10

Zahoruiko L., Martianova T. & Al-Hiari M. (2024). Mathematical model and structure of a neural network for detection of cyber attacks on information and communication systems. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska, 3*(14), 49–55. https://doi.org/10.35784/iapgos.6155

zakon.rada.gov.ua. (2018, June 21). Zakon Ukrainy «Pro natsionalnu bezpeku Ukrainy» vid 21.06.2018 r. № 2469-VIII (zi zminamy ta dopovnenniamy) [Law of Ukraine "On national security of Ukraine" dated 21.06.2018 No. 2469-VIII (with amendments and supplements)]. https://zakon.rada.gov.ua/laws/show/2469-19#Text

Zhalil Ya. (2025). *Ekonomichna bezpeka Ukrainy v umovakh vysokykh voiennykh ryzykiv ta hlobalnoi nestabilnosti*: eksp.-analit. dop. [Economic security of Ukraine in the conditions of high military risks and global instability: exp.-analyt. rep.]. Kyiv: NISD. https://doi.org/10.53679/NISS-analytrep.2025.03

Zubko T. (2019). The diagnosis of economic security of the enterprise. *Herald of Herald of Kyiv National University of Trade and Economics, 6*, 85–92. https://doi.org/10.31617/visnik.knute.2019(128)08

Стаття надійшла до редакції / Received: 11.05.2026
Статтю прийнято до публікації / Accepted: 24.05.2026
Оприлюднено / Published: 24.06.2026