

С. О. Дегтярьов,
аспірант кафедри фінансів, банківської справи та страхування,
Державний біотехнологічний університет
ORCID ID: <https://orcid.org/0009-0008-5403-3306>

DOI: 10.32702/2306-6814.2025.10.175

СИСТЕМНЕ ОСМИСЛЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ КРІЗЬ ПРИЗМУ АДАПТИВНОГО РИЗИК-МЕНЕДЖМЕНТУ

S. Degtyarev,
Postgraduate student of the Department of Finance, Banking and Insurance,
State Biotechnological University

SYSTEMATIC UNDERSTANDING OF THE ECONOMIC SECURITY OF THE STATE THROUGH THE PRISM OF ADAPTIVE RISK MANAGEMENT

Стаття присвячена системному переосмисленню поняття економічної безпеки держави із позицій адаптивного ризик-менеджменту в умовах цифрової економіки та Індустрії 4.0. Розкрито еволюцію категорії "економічна безпека держави" від зародження у XX столітті до сучасних підходів, що враховують глобалізацію та цифрову трансформацію. Проаналізовано новітні методологічні підходи до оцінювання економічної безпеки, зокрема індикаторні системи, інтегральні показники та ризик-орієнтовані методи. Показано вплив Індустрії 4.0 на зміну структури загроз — зростання кіберризиків, інформаційних атак, цифрової нерівності, технологічної залежності — та на появу нових інструментів забезпечення безпеки (проактивний моніторинг, кібербезпека, адаптивне управління ризиками). Зроблено висновок про необхідність адаптивного підходу до управління економічною безпекою держави, який поєднує класичні принципи стійкості із гнучкістю реагування на динамічні ризики цифрової епохи. Перспективи подальших досліджень включають розробку практичних індикаторів та методів адаптивного ризик-менеджменту для зміцнення економічної безпеки.

The article is devoted to a systemic reconceptualization of the state's economic security through the lens of adaptive risk management in the context of the digital economy and the Fourth Industrial Revolution (Industry 4.0). It elucidates the evolution of the "state economic security" category, tracing its development from initial interpretations in the 20th century — centered around sovereignty and economic independence — to modern frameworks that emphasize resilience, competitiveness, and technological self-sufficiency. The study explores how globalization, digital transformation, and increasing uncertainty have reshaped both the content and operationalization of economic security at the national level.

Modern methodological approaches to the assessment of economic security are analyzed in depth. These include indicator-based systems that monitor threshold values for macroeconomic, financial, and structural variables; integral indices that aggregate multiple dimensions of security into a single score; and risk-oriented models that evaluate the likelihood and impact of potential threats. The relevance of adaptive models is highlighted, particularly those capable of recalibrating criteria in response to rapidly evolving challenges.

The impact of Industry 4.0 on the national security landscape is discussed, with particular emphasis on new forms of systemic vulnerability such as cyberattacks, technological dependence on foreign platforms, loss of control over critical digital infrastructure, and the widening gap in digital competencies. Concurrently, the emergence of innovative tools and frameworks — such as proactive cybersecurity protocols, real-time risk monitoring systems, and scenario-based strategic planning — marks a significant transformation in how states manage economic threats.

The article argues that traditional reactive strategies are no longer sufficient in an era defined by speed, volatility, and interconnectivity. Instead, an adaptive approach is needed — one that combines classical principles of stability with flexibility, predictive analytics, and institutional responsiveness. Such a system enhances the ability of the state to anticipate, absorb, and recover from shocks while ensuring long-term development goals are not compromised.

Prospects for further research include the development of practical adaptive toolkits, early warning indicators, and integrated national frameworks for managing economic risks. These advancements can strengthen the resilience of national economies and contribute to the modernization of public governance in conditions of permanent transformation.

Ключові слова: економічна безпека, адаптивний ризик-менеджмент, Індустрія 4.0, цифрова трансформація, національна безпека.

Key words: economic security, adaptive risk management, Industry 4.0, digital transformation, national security.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

У сучасних умовах глобальної турбулентності, якій притаманне накладання численних кризових явищ та швидкий технологічний поступ, забезпечення економічної безпеки держави набуло особливої актуальності. Цифровізація економіки, з одного боку, відкриває нові можливості для зростання, а з іншого — породжує нові ризики і вразливості. Сфера економіки тісно переплітається з національною безпекою: нині економіка і безпека вже не існують окремо, а політики дедалі більше інтегрують їх задля захисту національних інтересів. В цих обставинах постає наукова і практична проблема — яким чином осмислити економічну безпеку держави як цілісну систему, здатну адаптуватися до динамічних змін, ризиків та загроз.

Поняття економічної безпеки держави еволюціонувало під впливом соціально-економічних і технологічних змін. Вперше термін "економічна безпека" отримав практичне втілення у 1930-х роках, коли президент США Ф.Д. Рузвельт заснував Комітет з економічної безпеки для подолання наслідків Великої депресії. У період холодної війни економічна складова стала невід'ємною частиною стратегії національної безпеки, акцентуючи важливість економічної стійкості для збереження державного суверенітету. Після здобуття незалежності Україна також приділила значну увагу цій проблематиці:

у 1996 р. було створено Раду національної безпеки і оборони (РНБО) для координації політики безпеки, а згодом на законодавчому рівні закріплено поняття економічної безпеки як частини національної безпеки. Отже, проблема економічної безпеки держави тісно пов'язана з вирішенням важливих завдань державної політики — захисту суверенітету, сталого розвитку, добробуту населення.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Проблематика економічної безпеки держави широко представлена у вітчизняній та зарубіжній науковій літературі, де вона розглядається як багатовимірна категорія, що поєднує в собі макроекономічну стабільність, технологічну автономність, інституційну ефективність та стійкість до зовнішніх і внутрішніх ризиків.

Серед фундаментальних праць варто відзначити дослідження А.О. Бойка та А.О. Єпіфанова [1], які розкривають сутність економічної безпеки держави, її функціональне призначення та ключові напрямки формування в умовах трансформаційної економіки. Автори наголошують на необхідності розробки системи граничних показників та індикаторів, що дозволяють об'єктивно оцінювати рівень безпеки. Концептуальну базу категорії "економічна безпека" розширено у підручнику О.М. Бандурки та співавт. [2], де вона розглядається як системна складова національної безпеки, яка охоплює політичні, фінансові, енергетичні, соц-

іальні та інші аспекти, що потребують узгодженого державного регулювання.

Новітній виклик економічній безпеці — цифровізацію — докладно аналізують М.І. Копитко та Д.А. Завєруха [3]. У своїй роботі вони акцентують увагу на ключових аспектах впливу Індустрії 4.0 на економічну безпеку, зокрема на зростанні кіберризиків, цифровій залежності та необхідності трансформації політики безпеки. І. Мігус [4] пропонує міжнародний зріз проблеми, аналізуючи виклики Індустрії 4.0 у глобальному контексті та зосереджуючись на практиках адаптації безпекових стратегій до нових технологічних умов.

Зарубіжні дослідники Н. Farrell та А. Newman [5] вводять поняття "стан економічної безпеки" (economic security state), що характеризується активним втручанням урядів у регулювання стратегічних ланцюгів постачання, технологій та капіталів з метою мінімізації критичних залежностей.

Отже, сучасна наукова думка сходиться на необхідності системного підходу до економічної безпеки, що враховує як традиційні індикатори, так і новітні ризики цифрової епохи, та потребує впровадження адаптивного ризик-менеджменту як ключової управлінської парадигми.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ (ПОСТАНОВКА ЗАВДАННЯ)

Метою статті є системне осмислення економічної безпеки держави крізь призму адаптивного ризик-менеджменту в умовах цифрової трансформації. Для досягнення цієї мети передбачено вирішення наступних завдань: узагальнити еволюцію поняття економічної безпеки держави та визначити його ключові характеристики; проаналізувати сучасні методологічні підходи до оцінювання економічної безпеки (з акцентом на ризик-орієнтованих і адаптивних підходах); дослідити вплив Індустрії 4.0 на трансформацію загроз економічній безпеці та на інструменти їх нейтралізації; обґрунтувати необхідність адаптивного управління ризиками як невід'ємної складової забезпечення економічної безпеки держави. Відповідно до поставленої мети, у статті використано міждисциплінарний підхід, що поєднує теорію національної безпеки, економічну теорію та сучасні концепції менеджменту ризиків.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Змістова трансформація поняття економічної безпеки держави відбувалася синхронно зі змінами у глобальній економіці, політичному устрої та технологічному середовищі. Від первинного акценту на самозабезпечення та економічну автономію у ХХ столітті до сучасного фокусу на цифровій стійкості й адаптивному управлінні ризиками — кожний етап розвитку формували нові акценти в безпековій парадигмі. Умовно цей процес можна представити як поетапну еволюцію підходів, що узагальнено на рис. 1.

Дана схема ілюструє ключові віхи зміни пріоритетів у сфері економічної безпеки, відображаючи перехід від класичної інституційної моделі до адаптивної системи, яка враховує динамічні ризики цифрової доби.



Рис. 1. Еволюція підходів до економічної безпеки держави

Економічна безпека держави традиційно розглядається як здатність національної економіки підтримувати стійкий розвиток, захищати ключові національні інтереси та протидіяти загрозам різного походження. На початкових етапах формування цієї концепції акцент робився на захисті економічного суверенітету: держава повинна мати достатні ресурси і можливості, щоб не залежати критично від зовнішніх сил та гарантувати мінімально необхідний рівень добробуту своїх громадян. Ще античні мислителі (зокрема, Платон) зазначали, що держава, яка володіє достатніми ресурсами, здатна забезпечити безпеку свого існування [3, с. 118—120].

У модерну добу поняття економічної безпеки поступово набувало інституційних форм: Комітет з економічної безпеки у США (1934) заклав основу соціально-економічних гарантій, а план Маршалла (1948) в післявоєнній Європі підкреслив роль економічної стабільності для запобігання політичним загрозам [2]. У другій половині ХХ ст. економічна безпека стала невіддільною від стратегії національної безпеки. В пострадянських країнах, зокрема в Україні, інтерес до цієї теми зріс на рубежі 1990-х-2000-х років у зв'язку з необхідністю трансформації економіки та побудови власної системи національної безпеки. З'явилися перші вітчизняні дослідження (наприклад, Бандурка та ін.), де було закладено теоретичні основи економічної безпеки. У них економічна безпека постає як комплексна категорія, що поєднує елементи стійкості (незалежності, самодостатності) та динаміки (здатності реагувати на зміни середовища). Згодом увага дослідників переключилася на деталізацію цієї категорії — виділення структурних елементів (фінансова, інвестиційна, енергетична, соціальна безпека тощо), визначення індикаторів для їх вимірювання, а також ідентифікацію основних загроз економічній безпеці на різних етапах розвитку держави [1-4].

На основі узагальнення різних трактувань можна виділити декілька ключових характеристик економічної безпеки держави. По-перше, це економічна стійкість — здатність економіки витримувати шоки (кризи, війни, стихійні лиха) без катастрофічних втрат для структури господарства і рівня життя населення [1, с. 68—70]. По-друге, економічна незалежність — це мінімізація критичної залежності від зовнішніх джерел (енергоносіїв, продовольства, імпорту стратегічних товарів, зовнішніх запозичень), що в разі шантажу або глобальних потрясінь може поставити під загрозу суверенітет [2]. По-третє, високий рівень конкурентоспроможності та розвитку — економіка має генерувати достатній обсяг інновацій, підтримувати науково-технологічний потенціал,

щоб не відстати від провідних країн (технологічна безпека) [4, с. 55]. По-четверте, соціальна стабільність — підтримання прийнятного рівня добробуту, зайнятості, соціальної справедливості, оскільки соціальні потрясіння (масове безробіття, бідність) безпосередньо підривають економічну безпеку [3, с. 119—121]. І нарешті, інституційна спроможність — ефективна держава, яка здатна формувати і реалізовувати економічну політику, боротися з корупцією, забезпечувати правопорядок у сфері економіки [2; 3]. Всі ці аспекти разом формують складну систему, рівновага якої і становить економічну безпеку держави.

Для вимірювання і моніторингу економічної безпеки держави розроблено низку методик, що відображають різні наукові підходи. Один з найпоширеніших — індикаторний підхід, суть якого полягає у встановленні системи ключових показників (макроекономічних, фінансових, соціальних, зовнішньоекономічних тощо) та порогових значень для них [2]. Перевищення або погіршення показника за межі порогу сигналізує про потенційну загрозу. В Україні прикладом є методика Міністерства економіки з оцінки рівня економічної безпеки, що оперує десятками індикаторів (темпи зростання ВВП, рівень інфляції, співвідношення держборгу до ВВП, дефіцит бюджету, рівень тіньової економіки, імпортозалежність за критичними позиціями тощо). Індикаторний підхід надає зручний інструментарій для державного моніторингу і внесений навіть у Стратегію економічної безпеки України (2021) як основа оцінки стану безпеки [6]. Втім, його обмеження полягають у тому, що він фіксує вже наявні проблеми і не завжди встигає за швидкими змінами ризиків.

Альтернативою є комплексні індекси та рейтинги, що узагальнюють показники в одному числовому індексі. Прикладом міжнародного індексу є Global Security Index, або національні інтегральні індекси, які обчислюються науковцями для зіставлення динаміки безпеки за роки. Такі індекси зручні для макроаналізу, але інколи критикуються за суб'єктивність вибору ваг та показників [8].

Все більшої популярності набуває ризик-орієнтований підхід у оцінюванні економічної безпеки. Він базується на ідентифікації ключових ризиків для економічної системи та оцінці ймовірності і потенційного збитку від їх реалізації. Цей підхід запозичений із сфери корпоративного управління ризиками (ERM — Enterprise Risk Management) та адаптований до державного рівня [7]. Наприклад, ризик-орієнтована модель може оцінювати, які загрози найбільш небезпечні для країни у коротко— та довгостроковій перспективі: фінансові кризи, різкі коливання цін на експортно-імпортні товари, відтік капіталу, енергетичні шоки, кібератаки на критичну інфраструктуру, пандемії тощо. Кожному ризику присвоюється рейтинг (за рівнем небезпеки), і на основі цього формується профіль ризиків держави [5, с. 126—129]. Подібний підхід потребує наявності розвинутої аналітичної бази, сценарного моделювання та прогнозування. Його перевага — проактивність, тобто можливість завчасно виявляти уразливі місця і готувати превентивні заходи, а не лише реагувати постфактум. Саме розвиток інформаційних технологій (Big Data, аналітичні платформи) дозволив дер-

жавам більш широко застосовувати ризик-орієнтовані методи. Так, сучасні програмні комплекси можуть моніторити в режимі реального часу фінансові потоки, зовнішні ринки, соціальні мережі, щоб виявляти аномалії чи ознаки наближення кризи. Скажімо, аналіз великих даних і машинне навчання використовуються для прогнозування ймовірності дефолтів, банківських криз або пікових навантажень на енергосистему, що дає змогу завчасно вжити заходів.

Окремо варто відзначити адаптивні підходи до оцінки безпеки, що лише формуються. Їх суть — перегляд критеріїв та моделей оцінювання по мірі зміни самого середовища. Якщо традиційні методики є досить статичними (набір індикаторів та їхні пороги рідко змінюються), то адаптивний підхід передбачає регулярний перегляд параметрів безпеки відповідно до актуальних трендів [4; 9]. Приміром, у 2010-х роках ще мало уваги приділялося таким показникам, як рівень кібератак чи захищеність персональних даних, а сьогодні ці критерії виходять на перший план. Адаптивні моделі інтегрують зворотний зв'язок: результати оцінки та виникнення нових типів загроз приводять до коригування самих моделей оцінювання. Таким чином, система "навчається" і удосконалюється з часом. Хоча адаптивні методи перебувають на ранніх стадіях впровадження, їх поява — закономірна відповідь на виклики швидкоплинного світу.

На порозі четвертої промислової революції держави стикаються з якісно новим середовищем безпеки. Індустрія 4.0 характеризується тотальною цифровізацією виробництва, бізнесу, державних послуг; впровадженням кіберфізичних систем, Інтернету речей, штучного інтелекту, хмарних технологій у всі сфери економіки. Ці зміни несуть не лише економічний ефект, а й нові виклики для безпеки. Природа загроз суттєво змінилася: замість переважно економічних і політичних факторів ризику (кризи, санкції, торговельні війни) на передній план виходять технологічні та інформаційні загрози. Серед них: кіберризик (злочинні атаки на банківську систему, енергомережі, урядові бази даних), інформаційні війни та маніпуляції (що можуть дестабілізувати фінансові ринки чи спровокувати паніку), вразливості ланцюгів постачання внаслідок тотальної автоматизації, цифрова нерівність (розрив між тими, хто володіє сучасними технологіями, і тими, хто відстає, що створює соціальну напругу), втрата робочих місць через автоматизацію (що може спричинити зростання безробіття у традиційних галузях і вимагатиме переорієнтації працівників). До традиційних загроз (наприклад, надмірної залежності від імпорту енергоносіїв чи зовнішнього боргу) додаються нові — залежність від імпорту технологій та програмного забезпечення, ризик "технологічної колонізації" (коли критична інфраструктура працює на іноземних платформах, що може стати об'єктом тиску). З'являється навіть термін "технологічний суверенітет", який стає складовою економічної безпеки: здатність держави самостійно підтримувати ключові технології та інтернет-інфраструктуру, аби не стати заручником монополій чи геополітичних опонентів [4, с. 54—58].

Окрім загроз, Індустрія 4.0 трансформує й інструменти забезпечення безпеки. Традиційні методи — дер-

Таблиця 1. Порівняльна таблиця традиційної та адаптивної моделі безпеки

Критерій	Традиційна модель	Адаптивна модель
Підхід до загроз	Реактивний	Превентивно-прогнозний
Джерело інформації	Офіційна статистика	Big Data, моніторинг в реальному часі
Частота коригувань	Планова (раз на рік і більше)	Динамічна, залежно від ризику
Тип рішень	Нормативно-адміністративні	Гнучкі, мультивекторні
Інструменти	Індикатори, контроль	Сценарії, аналітика, штучний інтелект

Джерело: узагальнено автором на основі [1—6].

жавне регулювання, протекціонізм, контроль над стратегічними галузями — доповнюються новими механізмами. Насамперед це кібербезпека: створення національних центрів кіберзахисту, команд швидкого реагування на кібератаки, систем кібермоніторингу критичної інфраструктури. Фокус безпеки зміщується на захист даних та мереж: впровадження стандартів інформаційної безпеки, шифрування, аудит програмних продуктів, імпортозаміщення програмного забезпечення. Держава все більше інвестує в освіту і науку для підготовки фахівців з високотехнологічних сфер, адже кадровий потенціал стає чинником безпеки (брак ІТ-спеціалістів може послабити здатність країни до цифрового захисту). З'являються нові форми міжнародної співпраці: спільні ініціативи проти кіберзлочинності, угоди про спільні дії у разі нападів на критичну цифрову інфраструктуру, обмін даними про кіберзагрози. Ще один напрям — адаптивне регулювання економіки. Швидкі технологічні зміни вимагають гнучкої нормативної бази, що може оперативно реагувати на появу нових бізнес-моделей (фінтех, криптовалюти, електронна комерція). Закони і стандарти доводиться переглядати частіше, залучаючи експертів та бізнес до процесу (регуляторні "пісочниці", тестові правові режими для інноваційних сфер). Це теж частина економічної безпеки — інституційна спроможність адекватно реагувати на технологічні виклики [1—5].

В епоху Індустрії 4.0 помітна зміна підходів: від реактивних дій до проактивних та прогнозних. Якщо раніше заходи безпеки часто вживалися постфактум — після настання кризи чи інциденту — то нині акцент зміщено на попередження. Використовуються інструменти раннього попередження: системи моніторингу соціальних настроїв (щоб завчасно помітити можливі протестні хвилі через економічні проблеми), економічні симуляції та стресс-тести (моделювання наслідків потенційних шоків), розвідка в кіберпросторі (cyber intelligence) для виявлення планів нападів. Застосування штучного інтелекту дозволяє прогнозувати ризики з вищою точністю — наприклад, прогноз ймовірності виникнення продовольчої кризи на основі кліматичних і ринкових даних, чи оцінка фінансових "бульбашок" на ринку активів, що загрожують економічній стабільності. Таким чином, відбувається перехід від реактивної парадигми безпеки до адаптивно-превентивної. Державна політика має бути достатньо гнучкою, щоб перегрупувати ресурси і засоби на пріоритетні напрями, як тільки з'являються нові загрози.

Це можливо лише за наявності системи адаптивного ризик-менеджменту на національному рівні, що спирається на безперервний моніторинг, аналіз даних і швидке ухвалення рішень.

Виходячи з викладеного, логічним є висновок, що для ефективного забезпечення економічної безпеки держави в сучасних умовах необхідно впроваджувати адаптивний підхід до управління ризиками. Адаптивний ризик-менеджмент означає, що держава постійно вчиться на основі минулих подій і поточних індикаторів, та коригує свою політику безпеки. Це аналогія до живого організму, який підтримує гомеостаз, але водночас реагує на подразники зовнішнього середовища. Наприклад, якщо виявлено тренд зростання кібератак на банківський сектор, адаптивна система одразу посилює кібербезпеку фінансової сфери, запускає резервні протоколи, інформує бізнес про ризики. Якщо ж, навпаки, певні загрози втратили актуальність, ресурси можуть бути перекинуті на інші напрямки.

З урахуванням виокремлених категорій сучасних загроз постає об'єктивна необхідність зміни парадигми забезпечення економічної безпеки держави. Традиційні підходи, орієнтовані на стабільність, контроль і нормативне реагування, дедалі менше відповідають динамічному характеру ризиків цифрової доби. Водночас адаптивна модель безпеки передбачає гнучке управління на основі моніторингу, прогнозування та зворотного зв'язку. У зв'язку з цим доцільно здійснити порівняльний аналіз основних відмінностей між традиційною та адаптивною моделями системи економічної безпеки, що подано в таблиці 1.

Порівняльний аналіз свідчить про суттєву трансформацію підходів до забезпечення економічної безпеки в умовах цифрової економіки. Традиційна модель, зосереджена переважно на стабільності, індикаторному оцінюванні та адміністративному регулюванні, виявляється недостатньо ефективною в ситуаціях високої динаміки та комплексності загроз. Натомість адаптивна модель демонструє більшу гнучкість, передбачає постійний моніторинг, прогнозування та управління ризиками в режимі реального часу. Її ключовими характеристиками є перевага аналітичних інструментів над формальними, ширше використання цифрових технологій (зокрема штучного інтелекту, big data), мультиакторна взаємодія та здатність до швидкого коригування стратегій. Таким чином, перехід до адаптивної моделі є критично

важливим для підвищення стійкості та конкурентоспроможності економіки в умовах Індустрії 4.0.

Зіставлення ключових характеристик традиційної та адаптивної моделей економічної безпеки підтверджує необхідність впровадження нових організаційно-інституційних рішень, здатних забезпечити реалізацію принципів гнучкості, випереджувального реагування та багаторівневого моніторингу. Формування такої моделі безпеки вимагає не лише концептуальних змін, а й відповідної інфраструктури для збору, аналізу та використання ризик-інформації в режимі реального часу. Саме тому для реалізації адаптивного ризик-менеджменту потрібні відповідні інституційні механізми. Зокрема, постійно діючі ситуаційні центри при органах влади, що відслідковують ризики в економіці та готують аналітичні рішення (в Україні елементом такої системи є НБУ, що моніторить фінансову стабільність, або РНБО з її Центром кібербезпеки). Необхідна правова база для гнучкого управління в кризових ситуаціях (якщо виникає надзвичайна загроза економічній безпеці — механізми надзвичайного стану чи антикризового управління економікою). Важливим є налагодження партнерства держави і бізнесу у сфері безпеки: держава повинна отримувати інформацію від приватного сектора про ризики (наприклад, банки повідомляють про підозрілі транзакції, енергокомпанії — про кіберінциденти), а бізнес — підтримку та рекомендації від держави. Це концепція "цілісного підходу" (whole-of-society approach) до національної безпеки, де економічна безпека розглядається як спільна справа уряду, бізнесу та громадян.

Окремо слід підкреслити роль стратегічного прогнозування та сценарного планування. Адаптивність не можлива без бачення майбутнього розвитку. Тому держава розробляє сценарії: оптимістичні, базові, песимістичні — щодо динаміки економіки та зовнішнього середовища, і для кожного сценарію передбачають пакет заходів. Наприклад, сценарій нової глобальної фінансової кризи — держава готує антикризовий план підтримки економіки; сценарій технологічного прориву — інвестує в освіту та інфраструктуру, щоб використати можливості. У Стратегії економічної безпеки України до 2025 року прямо зазначено необхідність прогнозування і підвищення здатності економіки до адаптації перед зовнішніми і внутрішніми викликами [6].

Насамкінець, варто відмітити, що адаптивний ризик-менеджмент спирається на у суспільстві та владних структурах. Якщо керівництво держави, бізнес-еліта і громадськість усвідомлюють значущість економічної безпеки та готові інвестувати в неї (час, ресурси, зусилля), тоді запровадження нових підходів проходить успішніше. Формування такої культури — завдання не лише освітнє, а й практичне (тренування, навчання управлінців, обмін досвідом із партнерами).

Таким чином, адаптивне управління ризиками є логічною відповіддю на сучасні виклики економічній безпеці. Воно дозволяє об'єднати системне бачення (цілісність, врахування всіх складових безпеки) із гнучкістю (швидкою реакцією та трансформацією підходів). У результаті держава отримує більш стійку та живучу економічну систему, менш вразливу до шоків і більш спроможну використати нові можливості.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Економічна безпека держави в сучасному світі постає як динамічна системна категорія, зміст якої змінюється під впливом глобалізації та четвертої промислової революції. Проведене дослідження показало, що традиційні уявлення про економічну безпеку (як про захищеність від окремих статичних загроз) більше не є достатніми. Сьогодні економічна безпека — це стан рівноваги і стійкості національної економіки, що підтримується завдяки здатності адаптуватися до нових ризиків і викликів. Нині відбувається конвергенція методів забезпечення безпеки з практиками ризик-менеджменту, виробленими в корпоративному секторі та сфері управління проектами. Індустрія 4.0, цифрова економіка та глобальні непередбачувані фактори (пандемії, геополітичні конфлікти, кліматичні кризи) вимагають від держав впровадження проактивних і адаптивних стратегій захисту національних економічних інтересів.

В рамках дослідження узагальнено еволюцію поняття економічної безпеки: від акценту на незалежності та захищеності в XX столітті — до багатовимірного підходу, що включає технологічну, інноваційну, соціальну складові в XXI столітті. Проаналізовано сучасні методології оцінки рівня безпеки, серед яких індикаторні та індексні методи залишаються важливими інструментами, але все більшого значення набувають ризик-орієнтовані підходи. Показано, що Індустрія 4.0 призводить до якісного оновлення спектру загроз: поряд із традиційними економічними ризиками з'явилися кіберзагрози, інформаційні маніпуляції, технологічні залежності, які потребують нових підходів у політиці безпеки.

У таких умовах держава вимушена адаптувати свої інститути та механізми: розвивати кібербезпеку, нормативно реагувати на цифрові виклики, посилювати аналітичну спроможність для прогнозування криз. Отже, постає гостра необхідність переходу до адаптивного ризик-менеджменту для забезпечення економічної безпеки держави. Такий підхід дозволить створити гнучку систему захисту, що вчасно виявляє нові загрози і адекватно на них відповідає, мінімізуючи можливі збитки для економіки та суспільства. Він поєднує превентивні заходи, постійний моніторинг та готовність змінювати стратегію залежно від розвитку ситуації. Адаптивна модель зміцнює національну економіку, підвищує довіру до державних інститутів і забезпечує стабільність розвитку навіть у турбулентні часи.

Перспективи подальших досліджень полягатимуть у деталізації практичних аспектів впровадження адаптивного ризик-менеджменту на державному рівні та розробці конкретних методичних рекомендацій для органів влади щодо створення систем моніторингу та реагування на економічні ризики, а також критерії ефективності такої системи. Цікавим напрямом є визначення оптимального набору індикаторів "цифрової" економічної безпеки (наприклад, показників кіберстійкості, рівня технологічної автономії тощо) та інтегрування їх у існуючі оцінки. Також варто дослідити механізми фінансового забезпечення економічної безпеки — формування резервів, страхових інстру-

ментів, фондів стабілізації — у логіці адаптивного управління ризиками. Окрім того, перспективним є порівняльний аналіз досвіду різних країн у побудові систем економічної безпеки в умовах Індустрії 4.0: виявлення найкращих практик, які могли б бути імплементовані в Україні. У цілому, подальші розвідки повинні сприяти формуванню цілісної науково обгрунтованої системи економічної безпеки, що відповідає викликам цифрової ери та забезпечує стійкий розвиток держави.

Література:

1. Бойко А. О., Єпіфанов А. О. Економічна безпека держави: сутність та напрями формування. Вісник СумДУ. Серія "Економіка". 2018. № 3. С. 65—75. URL: visnyk.fem.sumdu.edu.ua
2. Бандурка О. М., Духов В. Є., Петрова К. Я., Черняков М. (2003). Основи економічної безпеки: підручник. Харків: Вид-во Нац. ун-ту внутр. справ. 2003.
3. Копитко М. І., Заверуха Д. А. Ключові аспекти впливу Індустрії 4.0 на економічну безпеку держави. Соціально-правові студії. 2021. № 4 (14). С. 117—122. URL: sls-journal.com.ua
4. Мігус І. Основні тенденції розвитку Індустрії 4.0 та її вплив на економічну безпеку держави: міжнародний аспект. Вчені записки Університету "КРОК". 2023. № 1 (69). С. 52—59. DOI: <https://doi.org/10.31732/2663-2209-2022-69-52-59>
5. Farrell H., Newman A. The New Economic Security State. Foreign Affairs, 2023. № 102 (5). С. 124-137. URL: foreignaffairs.com
6. Про Стратегію економічної безпеки України на період до 2025 року. Указ Президента України № 347 / 2021 від 11.08.2021. Офіційний інтернет-портал Верховної Ради України. URL: zakon.rada.gov.ua
7. U.S. Department of Homeland Security (DHS). Risk Management Fundamentals: Homeland Security Risk Management Doctrine. 2011. Washington, D.C.: DHS. URL: dhs.gov
8. World Economic Forum (WEF). The Global Risks Report 2023 (18th Edition). Geneva: WEF.
9. OECD. Fostering Economic Resilience in a World of Open and Integrated Markets. OECD Publishing. 2022. DOI: <https://doi.org/10.1787/3c796721-en>.

References:

1. Bojko, A.O. and Yepifanov, A.O. (2018), "Economic security of the state: essence and directions of formation", Visnyk SumDU. Seriiia "Ekonomika", vol. 3, pp. 65—75.
2. Bandurka, O.M. Dukhov, V.Ye. Petrova, K.Ya. and Cherniakov, M. (2003), Osnovy ekonomichnoi bezpeky [Fundamentals of economic security], Vyd-vo Nats. un-tu vnutr. sprav, Kharkiv, Ukraine.
3. Kopytko, M.I. and Zaverukha, D.A. (2021), "Key aspects of the impact of Industry 4.0 on the economic security of the state", Sotsial'no-pravovi studii, vol. 4 (14), pp. 117—122.
4. Mihus, I. (2023), "Main trends in the development of Industry 4.0 and its impact on the economic security of the state: an international aspect", Vcheni zapysky Universytetu "KROK", vol. 1 (69), pp. 52—59. DOI: <https://doi.org/10.31732/2663-2209-2022-69-52-59>

5. Farrell, H. and Newman, A. (2023), "The New Economic Security State", Foreign Affairs, vol. 102 (5), pp. 124—137.

6. President of Ukraine (2021), Decree "On the Strategy of Economic Security of Ukraine for the period until 2025", available at: zakon.rada.gov.ua (Accessed 25 Apr 2025).

7. U.S. Department of Homeland Security (DHS) (2011), Risk Management Fundamentals: Homeland Security Risk Management Doctrine, DHS, Washington, D.C., USA.

8. World Economic Forum (WEF) (2023), The Global Risks Report, 18th Edition, WEF, Geneva.

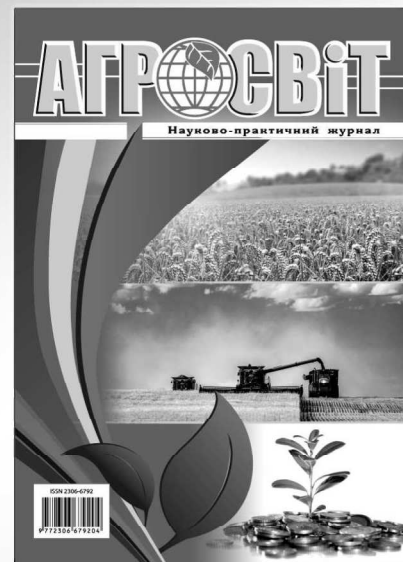
9. OECD (2022), Fostering Economic Resilience in a World of Open and Integrated Markets, OECD Publishing. DOI: <https://doi.org/10.1787/3c796721-en>.

Стаття надійшла до редакції 06.05.2025 р.

АГРОСВІТ

<https://nauka.com.ua>

Передплатний індекс: 23847



Виходить 24 рази на рік

**Журнал включено до переліку
наукових фахових видань України
з ЕКОНОМІЧНИХ НАУК (Категорія «Б»)**

Спеціальності – 051, 071, 072, 073, 075, 076, 292