

УДК 336.226:631.115:330.322

DOI: 10.60022/2(9)-13S

Сіренко Олена Вікторівна

кандидат економічних наук, доцент

доцент кафедри обліку і оподаткування

Полтавський державний аграрний університет, Україна

Sirenko Olena

PhD in Economics, Associate Professor

Associate Professor of the Department of Accounting and Taxation

Poltava State Agrarian University, Ukraine

ORCID: 0000-0003-4875-308X

Яковенко Роман Леонідович

здобувач третього (освітньо-наукового) рівня вищої освіти

Полтавський державний аграрний університет, Україна

Yakovenko Roman

PhD Student

Poltava State Agrarian University, Ukraine

ORCID: 0009-0006-9302-5910

ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ ДІАГНОСТИКИ ЕКОНОМІЧНОЇ БЕЗПЕКИ: ТЕОРЕТИЧНІ МОДЕЛІ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В УПРАВЛІННІ РИЗИКАМИ

Анотація. Актуальність дослідження зумовлена зростаючою складністю економічних загроз, що формуються в умовах цифрової трансформації та високої невизначеності бізнес-середовища. Традиційні методи оцінювання ризиків виявляють обмежену здатність реагувати на динамічні зміни та обробляти великі масиви різнорідних даних, що посилює потребу у впровадженні інтелектуальних рішень нового покоління. Використання алгоритмів штучного інтелекту створює можливості для підвищення точності діагностики, формування систем раннього попередження та забезпечення стійкості підприємств до зовнішніх і внутрішніх загроз. Отримані результати засвідчили, що побудована модель здатна істотно підвищити ефективність діагностики ризиків завдяки поєднанню багатоканальних даних, алгоритмів глибинного аналізу та механізмів формування інтегральних індикаторів ризиковості. Запропонована система забезпечує своєчасне виявлення аномалій, формування прогнозних сценаріїв та підготовку обґрунтованих управлінських рішень у режимі реального часу.

Ключові слова: штучний інтелект, управління ризиками, економічна безпека підприємства, аномалійний аналіз, предиктивна аналітика, цифрова трансформація, індикатори ризиковості.

INTELLIGENT SYSTEMS FOR ECONOMIC SECURITY DIAGNOSTICS: THEORETICAL MODELS OF ARTIFICIAL INTELLIGENCE APPLICATION IN RISK MANAGEMENT

Abstract. The relevance of the study is driven by the growing complexity of economic threats arising in the context of digital transformation and high uncertainty of the business environment. Traditional risk assessment methods demonstrate limited capacity to respond to dynamic changes and to process large volumes of heterogeneous data, which amplifies the need for implementing next-generation intelligent solutions. The use of artificial intelligence algorithms creates opportunities to enhance diagnostic accuracy, develop early warning systems, and strengthen enterprises' resilience to internal and external threats. The purpose of this research is to provide theoretical justification and construct a model of intelligent diagnostics of enterprise economic security that integrates machine learning, predictive analytics, and mechanisms of optimization-based managerial decision support. The methodological framework of the study includes a systems approach, economic modelling methods, machine learning tools, SWOT analysis, as well as comparative-structural and analytical approaches to risk assessment. The comprehensive combination of these methods enabled the examination of the threat structure, identification of functional contours of the model, and evaluation of its

potential for risk management. The results indicate that the proposed model can significantly improve the effectiveness of risk diagnostics through the integration of multichannel data, deep analytical algorithms, and mechanisms for generating integrated risk indicators. The system ensures timely anomaly detection, development of forecast scenarios, and preparation of evidence-based managerial decisions in real time. The SWOT analysis confirmed the high potential of the model while outlining the conditions and limitations affecting its practical implementation.

Keywords: *artificial intelligence, risk management, economic security of the enterprise, anomaly detection, predictive analytics, digital transformation, risk indicators.*

Постановка проблеми. Сучасні підприємства функціонують у середовищі, що характеризується високою динамічністю, цифровою турбулентністю та зростанням інституційних, фінансових і операційних загроз. Традиційні підходи до діагностики ризиків економічної безпеки ґрунтуються переважно на ретроспективному аналізі, експертних оцінках та лінійних моделях, які не здатні адекватно реагувати на швидкоплинні зміни та обробляти великі обсяги різнорідних даних [1, с. 227]. Відсутність можливості своєчасно виявляти приховані патерни, аномальні відхилення та комплексні причинно-наслідкові зв'язки суттєво знижує ефективність управління ризиками та підвищує вразливість підприємств до внутрішніх і зовнішніх загроз. У цих умовах виникає потреба у створенні інтелектуальних систем нового типу, здатних забезпечувати багатовимірний аналіз, формування прогнозів та розроблення рекомендацій в режимі реального часу [2, с. 104].

Аналіз останніх досліджень і публікацій. Сучасні дослідження демонструють швидке зростання уваги до застосування штучного інтелекту у сфері діагностики та прогнозування економічних і фінансових ризиків, що зумовлено складністю цифрового середовища та потребою в точніших моделях прийняття рішень. У роботі P. Pal та ін. показано, що використання градієнтного бустингу та глибинних моделей дозволяє формувати високоточні кредитні скорингові системи та оптимізувати фінансові рішення в ланцюгах постачання [3, р. 2]. Дослідження T. Liu та L. Yang підсилює цю тезу, доводячи ефективність поєднання теорії грубих множин із ВР-нейронними мережами для раннього виявлення фінансових ризиків публічних компаній [4]. У систематичному огляді L. Vancsura та колег окреслено ключові технологічні розриви у фінансовому прогнозуванні, зокрема недостатню інтерпретованість моделей та відсутність їх перевірки у реальних торговельних стратегіях [5]. Ці обмеження підтверджуються бібліометричним аналізом A. Valencia-Agias та співавт., які показали стрімке зростання інтересу до ML у ризик-менеджменті та водночас наголосили на потребі міждисциплінарних підходів [6]. Вивчення можливостей машинного навчання для макроекономічних прогнозів у роботі Y. Duan та ін. засвідчило, що методи на кшталт quantile regression forest можуть суттєво підвищувати точність оцінювання монетарних та системних ризиків [7]. Аналогічно у дослідженні J. Muria-Tarazón та ін. доведено, що ризик-оцінювання штучного інтелекту є однією з найдинамічніших сфер, особливо в умовах зростання вимог до етичності, прозорості та регулювання [8]. У сфері неприбуткових організацій H. Huang встановив, що ансамблеві моделі (Random Forest, LightGBM) дають змогу значно підвищувати якість прогнозування дефолтів та посилювати фінансову стійкість [9, с. 104]. Додатково роль генеративних технологій у ризик-прогнозуванні успішно продемонстровано у праці K.-C. Yao та ін., де окреслено потенціал GAN та великих мовних моделей для підвищення точності та інтерпретованості фінансових моделей [10, с. 104]. У галузевому вимірі дослідження O. Самойлова та Г. Дошенка підтвердило, що SCADA-системи є критично важливими джерелами даних для технічного діагностування, а якість даних визначає результативність прогнозних моделей ШІ [11, с. 104]. На макрорівні робота A. Буряка та O. Масля засвідчила стратегічний потенціал генеративного ШІ у мінімізації цифрових ризиків держави та підвищенні кіберстійкості критичної інфраструктури [12, с. 17]. Сукупність проаналізованих джерел демонструє еволюцію сучасної парадигми ризик-менеджменту – від традиційних статистичних моделей до комплексних інтелектуальних систем, здатних обробляти великі гетерогенні масиви даних, забезпечувати інтерпретованість рішень та інтегруватися у багаторівневі системи економічної безпеки.

Попри значний науковий прогрес, низка питань залишається невирішеною, зокрема відсутність уніфікованих підходів до інтеграції моделей ШІ у корпоративні та державні системи моніторингу, проблеми алгоритмічної прозорості та пояснюваності, обмеження, пов'язані з якістю даних, нестійкість моделей у турбулентному середовищі та необхідність комплексної оцінки етичних і регуляторних аспектів. Саме тому наше дослідження спрямоване на подолання цих концептуальних та прикладних прогалин, передусім через побудову цілісної системи інтелектуальної діагностики, здатної

забезпечувати проактивне управління ризиками та адаптацію до зміни зовнішніх умов.

Метою статті є теоретичне обґрунтування та розроблення моделі інтелектуальної діагностики економічної безпеки підприємства, яка інтегрує алгоритми машинного навчання, предиктивну аналітику, технології розпізнавання аномалій та інструменти оптимізаційної підтримки управлінських рішень з метою підвищення точності, оперативності та проактивності ризик-менеджменту.

Виклад основного матеріалу. Поняття економічної безпеки традиційно розглядається як здатність підприємства забезпечувати стабільність функціонування, підтримувати стійкість фінансово-господарських процесів та протидіяти внутрішнім і зовнішнім загрозам. Її сутність проявляється через комплекс ключових компонентів – фінансову стійкість, ресурсну забезпеченість, операційну надійність, інноваційно-технологічний потенціал, кадрову стабільність та стратегічну гнучкість. Саме взаємодія цих складових формує інституційне підґрунтя для підтримання конкурентоспроможності та безперервності бізнес-процесів [13, с. 161].

У теорії та практиці менеджменту ризиків діагностика економічної безпеки ґрунтується на низці класичних підходів. Фінансовий підхід передбачає аналіз ліквідності, рентабельності, автономії та оцінювання імовірності загроз платоспроможності. Ресурсний підхід зосереджується на достатності й структурі матеріальних, трудових та інформаційних ресурсів. Операційний підхід акцентує увагу на стабільності виробничо-логістичних процесів, рівні операційних витрат та параметрах ефективності. Стратегічний підхід орієнтується на довгострокові ризики, пов'язані зі змінами ринку, технологічними трансформаціями, інституційними факторами та конкурентним середовищем [12, с. 20]. У сукупності ці методи забезпечують базову рамку для виявлення, оцінювання та прогнозування загроз.

Водночас сучасні умови високої невизначеності, зумовлені цифровою турбулентністю, геополітичними шоками та зростанням швидкості обміну даними, суттєво обмежують ефективність традиційних підходів. Їхні недоліки проявляються у слабкій здатності обробляти великі масиви даних, низькій оперативності реагування, недостатній гнучкості щодо виявлення нестандартних патернів та високій залежності від суб'єктивних суджень аналітиків. За цих умов стає очевидною потреба у застосуванні інтелектуальних систем, здатних забезпечити багатовимірну, адаптивну та предиктивну діагностику ризиків економічної безпеки.

Сутність інтелектуальних систем у сфері менеджменту та економічної безпеки полягає у здатності цих технологій виконувати складні аналітичні, прогностичні та когнітивні функції, які раніше вимагали значної участі людини. Інтелектуальні системи інтегрують алгоритми штучного інтелекту, методи машинного навчання та експертні правила, формуючи адаптивні інструменти підтримки управлінських рішень. У контексті безпеки вони забезпечують багатовимірну діагностику ризикових зон, моделювання сценаріїв впливу загроз та автоматизоване реагування на нетипові зміни у внутрішньому чи зовнішньому середовищі підприємства [2; 14].

Ключові можливості III у системах діагностики економічної безпеки охоплюють кілька груп технологій – табл. 1. Машинне навчання дозволяє розпізнавати закономірності у великих масивах даних, будувати прогностичні моделі та точніше оцінювати ймовірність виникнення ризиків. Предиктивна аналітика підсилює цей процес завдяки сценарному прогнозуванню та оцінюванню потенційних наслідків управлінських рішень [15, с. 48]. Технології розпізнавання аномалій автоматично виявляють нетипові відхилення у фінансових, операційних чи поведінкових параметрах, що часто сигналізують про приховані загрози або шахрайські дії. Інструменти оптимізації рішень, засновані на генетичних алгоритмах, нейромережових моделях чи методах багатоцільової оптимізації, забезпечують пошук найкращих управлінських альтернатив у режимі реального часу.

Таблиця 1

Ключові можливості III у діагностиці економічної безпеки підприємства

Група технологій III	Сутність	Роль у діагностиці економічної безпеки
Машинне навчання (ML)	Автоматичне виявлення закономірностей у великих масивах даних; класифікація та кластеризація	- формування моделей ризиковості; - прогнозування фінансових та операційних загроз; - визначення прихованих факторів впливу
Предиктивна аналітика	Поєднання ML, статистики та імітаційного моделювання для створення прогнозів.	- моделювання сценаріїв розвитку ризиків; - оцінювання наслідків управлінських рішень; - підвищення точності прогнозів безпеки
Розпізнавання аномалій	Виявлення нетипових відхилень у даних за допомогою нейронних мереж, автоенкодерів та кластеризації	- виявлення шахрайства, помилок, внутрішніх загроз; - контроль операційної стабільності; - рання індикація небажаних тенденцій

Продовження таблиці 1

Оптимізація рішень (AI Optimization)	Генетичні алгоритми, нейромережі, методи динамічного програмування для пошуку найкращих рішень	- підбір оптимальної стратегії управління ризиками; - оптимізація ресурсного забезпечення; - пропозиція найефективніших дій у режимі реального часу
NLP та когнітивна аналітика	Обробка текстів, звітів, документів, новин, політичних і ринкових сигналів	- виявлення зовнішніх загроз у медійному та нормативному середовищі; - автоматизація моніторингу документації; - інтеграція слабоструктурованої інформації в систему безпеки

Джерело: складено авторами за [2; 14; 15]

Функціонування інтелектуальних систем є нерозривно пов'язаним із якістю, повнотою та релевантністю даних, адже саме дані формують основу алгоритмічного навчання та точність діагностики. Цифрові платформи – ERP/CRM-системи, аналітичні хмарні сервіси, кіберфізичні платформи, датчики IoT – забезпечують безперервний збір, інтеграцію й візуалізацію інформації, створюючи єдиний інформаційний простір для моніторингу ризиків. Їх використання дозволяє трансформувати фрагментарні дані на операційному, фінансовому та стратегічному рівнях у цілісну систему раннього попередження, що підвищує ефективність управління економічною безпекою та зменшує часові лаги у прийнятті рішень [16, с. 70].

Узагальнюючи наведені можливості, варто підкреслити, що застосування інтелектуальних систем суттєво розширює аналітичний потенціал підприємства, забезпечуючи багатоканальний моніторинг ризиків та автоматизовану обробку великих масивів даних. Завдяки інтеграції машинного навчання, предиктивної аналітики, аномалійного детектування та оптимізаційних алгоритмів, фрагментарні дані операційного, фінансового і стратегічного рівнів трансформуються в цілісну систему раннього попередження. Це дозволяє не лише підвищити точність і швидкість діагностики економічної безпеки, а й мінімізувати часові лаги у прийнятті управлінських рішень, забезпечуючи проактивну реакцію на потенційні загрози.

Ефективність і масштабованість інтелектуальних систем значною мірою визначається інституційними, технічними та етичними умовами їх впровадження, що робить цей аспект одним із центральних у формуванні сучасних підходів до управління економічною безпекою. Однією з ключових проблем залишається доступність якісних, репрезентативних і захищених даних, адже саме вони є фундаментом для алгоритмічного навчання, коректної калібрації моделей та формування надійних прогнозів. У багатьох підприємств зберігається фрагментованість інформаційної інфраструктури, відсутність єдиних стандартів збору даних, наявні розриви між корпоративними базами та зовнішніми джерелами, що призводить до неповноти вибірок, значної кількості пропусків та низької інтероперабельності. За таких умов навіть найефективніші алгоритми машинного чи глибинного навчання демонструють обмежену результативність через викривлення, нестійкість або неможливість узагальнення патернів.

Важливим викликом є також забезпечення прозорості роботи алгоритмічних моделей і мінімізація ризику алгоритмічного упередження. Інтелектуальні системи, що працюють із великими та гетерогенними масивами даних, часто формують рішення у форматі так званої «чорної скриньки», коли логіка прийняття рішень залишається недоступною для користувача. Непрозорість моделей ускладнює аудит ризиків, знижує довіру до результатів і може призводити до ненавмисного відтворення структурних нерівностей у даних. Проблема упередженості особливо актуальна для систем, що приймають управлінські рішення з фінансовими, стратегічними або кадровими наслідками, оскільки помилки чи викривлення можуть спричинити значні негативні ефекти для підприємства. У цьому контексті важливого значення набувають технології explainable AI (XAI), методи інтерпретованості та аудит трасування даних.

Окрему складність становлять питання кібербезпеки, адже зростання обсягів корпоративних даних і використання хмарних рішень підвищує ризики витоків, маніпулювання інформацією, атак на моделі чи підміни даних для навчання. Уразливості на рівні API, недостатній контроль доступу або відсутність системного моніторингу можуть стати джерелом нових загроз економічній безпеці. Додаткові ризики виникають у процесі інтеграції інтелектуальних систем із корпоративними ERP-, CRM-, SCM- та бухгалтерськими платформами, де будь-яке порушення цілісності даних може призвести до помилкових управлінських рішень.

Значну роль відіграють і нормативно-правові обмеження. Інтелектуальні системи мають відповідати вимогам законодавства у сферах захисту персональних даних, кіберзахисту, регулювання цифрової інфраструктури та фінансового комплаєнсу. Для України особливо актуальними є проблеми гармонізації локального законодавства з європейськими стандартами штучного інтелекту (EU AI Act), адаптації до вимог кіберстійкості NIS2, регуляції обробки критичних даних, а також забезпечення аудитованості моделей. Недостатня правова визначеність або суперечності у регулюванні можуть затримувати впровадження інтелектуальних рішень у сфері економічної безпеки, а також створювати правові ризики для підприємств.

Ще одним обмеженням є кадрова та інституційна готовність організацій. Інтелектуальні системи вимагають високого рівня компетентностей у сферах аналітики даних, кібербезпеки, цифрового менеджменту та експлуатації складних моделей машинного навчання. Брак спеціалістів або відсутність відповідних внутрішніх процедур знижує ефективність систем і створює залежність від зовнішніх інтеграторів, що може підвищувати ризики витоку та втрати контролю над аналітичними процесами.

Таким чином, сукупність зазначених аспектів зумовлює потребу у формуванні збалансованої рамки впровадження ШІ, яка поєднує технологічні можливості з інституційними гарантіями безпеки, прозорості та довіри. Підприємства мають орієнтуватися на комплексний підхід, де поєднуються стандарти якості даних, регуляторні вимоги, етичні принципи, кіберзахисні процедури та культура відповідального використання штучного інтелекту. Саме в межах такої рамки може ефективно функціонувати запропонована модель, побудована на інтеграції алгоритмів штучного інтелекту, потоків корпоративних даних та механізмів аналітичної логіки управління ризиками, що забезпечує проактивне й обґрунтоване прийняття управлінських рішень – рис. 1.

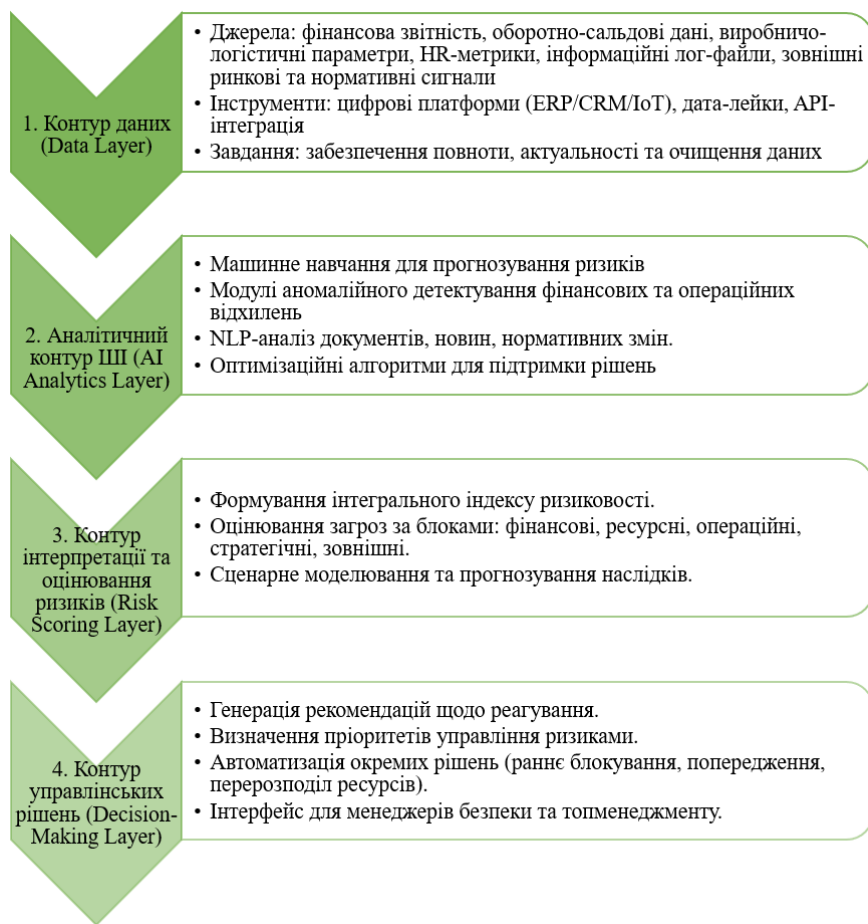


Рис. 1. Модель інтелектуальної діагностики економічної безпеки підприємства
Джерело: сформовано авторами

Розроблена модель інтелектуальної діагностики економічної безпеки ґрунтується на взаємодії чотирьох стратегічних контурів, кожен із яких виконує специфічну функцію у формуванні цілісної

системи управління ризиками.

Перший контур – даних – забезпечує багатоканальний збір, інтеграцію та структурування інформації з фінансових, операційних, кадрових, логістичних та зовнішніх джерел. Він формує основу аналітичної екосистеми, визначаючи якість і повноту подальших управлінських рішень.

Другий контур – аналітики ІІІ – трансформує отримані дані в інтелектуальні сигнали шляхом застосування машинного навчання, методів розпізнавання аномалій, когнітивної аналітики та оптимізаційних алгоритмів. Саме на цьому етапі відбувається виявлення закономірностей, прогнозування ризиків і моделювання потенційних сценаріїв розвитку подій.

Третій контур – інтерпретації та оцінювання ризиковості – виконує роль концептуального "перекладача" між машинними результатами й управлінським контекстом. Він узагальнює вихідні сигнали ІІІ в інтегральні індекси ризиковості, визначає критичні зони, формує курси альтернативних сценаріїв і дозволяє оцінювати силу та напрям впливу різних загроз.

Четвертий контур – управлінських рішень – перетворює аналітичні висновки на практичні дії: рекомендації, сценарні пропозиції, автоматизовані тригери реагування та рішення щодо перерозподілу ресурсів. Цей контур забезпечує замкнутість циклу управління, оскільки результати реалізованих заходів повертаються у систему для подальшого навчання й оптимізації моделей.

Узгоджена взаємодія всіх контурів формує динамічну, самооновлювану систему діагностики економічної безпеки, здатну адаптуватися до високої мінливості середовища, обробляти великі масиви даних та забезпечувати проактивне управління ризиками.

Водночас, незважаючи на значний потенціал, така модель має як структурні переваги, так і обмеження, що проявляються на рівні технологій, даних та інституційного середовища. Це зумовлює необхідність системної оцінки її функціональної стійкості, адаптивності та здатності до масштабування в умовах реальних управлінських процесів. Для комплексного розуміння її можливостей доцільно провести SWOT-аналіз моделі – табл. 2, який дозволяє оцінити її сильні сторони, внутрішні слабкості, а також зовнішні можливості і загрози її подальшого застосування.

Таблиця 2

SWOT-аналіз моделі інтелектуальної діагностики економічної безпеки підприємства

S – Strengths (Сильні сторони)	W – Weaknesses (Слабкі сторони)
Висока точність прогнозування завдяки машинному навчанню та багатовимірним моделям.	Залежність від доступності якісних, стандартизованих та репрезентативних даних.
Виявлення прихованих загроз, слабкоструктурованих патернів і аномалій, недоступних традиційним методам.	Складність інтеграції з різномірними корпоративними інформаційними системами.
Швидка обробка великих масивів даних і мінімізація людського фактору.	Високі вимоги до захисту даних, кібербезпеки та контролю доступу.
Формування системи раннього попередження у реальному часі.	Потреба у висококваліфікованих ІТ-фахівцях і аналітиках для налаштування моделі.
Самонавчання моделі та зростання її ефективності під впливом нових даних.	Ризик «чорної скриньки» – непрозорість роботи окремих алгоритмів та складність інтерпретації результатів.
O – Opportunities (Можливості)	T – Threats (Загрози)
Розвиток хмарних платформ, IoT та кіберфізичних систем, що розширюють аналітичну інфраструктуру.	Кіберризики та атаки, спрямовані на спотворення даних або втручання в моделі.
Інтеграція з ESG-аналітикою, кіберзахистом та стратегічним плануванням.	Нормативні обмеження щодо персональних даних, алгоритмічної прозорості та етики ІІІ.
Можливість застосування у державному контролі, аудиті, фінансовому моніторингу та галузевих системах.	Алгоритмічне упередження, що може впливати на якість оцінювання ризиків.
Перехід підприємств до проактивного ризик-менеджменту.	Надмірна автоматизація може знижувати управлінську критичність та якість прийняття рішень.
Масштабування моделі на всі бізнес-процеси підприємства.	Висока турбулентність зовнішнього середовища, що зменшує стабільність і точність моделей.

Джерело: складено авторами

Узагальнюючи результати SWOT-аналізу, можна стверджувати, що запропонована модель інтелектуальної діагностики економічної безпеки поєднує значний технологічний потенціал із високим рівнем адаптивності до динамічних умов функціонування підприємства. Її сильні сторони формують основу для підвищення точності, оперативності й комплексності ризик-менеджменту, тоді як наявні

слабкі місця здебільшого пов'язані з необхідністю якісної цифрової інфраструктури та відповідних компетенцій персоналу. Виявлені можливості підтверджують перспективність масштабування моделі в рамках цифрової трансформації підприємств і галузевих систем безпеки, тоді як зовнішні загрози акцентують потребу у посиленні кіберзахисту, алгоритмічної прозорості та нормативної узгодженості. Це формує базу для подальшого теоретичного розвитку та практичного вдосконалення моделі, зокрема в напрямі створення гібридних систем управління ризиками, здатних забезпечувати стійкість бізнесу в умовах зростаючої невизначеності.

Висновки. Проведене дослідження дозволило встановити теоретичні та прикладні засади формування інтелектуальної моделі діагностики економічної безпеки підприємства, орієнтованої на використання технологій штучного інтелекту. Доведено, що поєднання алгоритмів машинного навчання, предиктивної аналітики, методів розпізнавання аномалій та оптимізаційних рішень істотно підвищує здатність підприємства своєчасно ідентифікувати загрози, оцінювати сценарні наслідки та формувати проактивні управлінські дії. Сформовані контури моделі забезпечують логічну завершеність її архітектури – від збору даних і когнітивного аналізу ризиків до формування інтегральних індикаторів та автоматизованих рекомендацій для прийняття рішень.

SWOT-аналіз моделі підтвердив її потенціал як ефективного інструменту підвищення стійкості бізнес-процесів, одночасно окресливши низку внутрішніх та зовнішніх обмежень, що потребують урахування під час впровадження. Зокрема, забезпечення високої якості даних, розвиток цифрової інфраструктури, посилення кіберзахисту та підвищення кваліфікації персоналу є критично важливими передумовами ефективного функціонування моделі в реальних умовах. У цілому результати дослідження засвідчують, що інтелектуальні системи здатні трансформувати підходи до управління ризиками, посилюючи можливості підприємств протидіяти невизначеності та комплексним загрозам.

Перспективами подальших наукових розробок є розширення моделі за рахунок гібридних AI-рішень, інтеграція з ESG-та кібербезпековими показниками, а також створення адаптивних інституційно-технологічних механізмів, що забезпечать її масштабованість у межах цифрової економіки.

Література

1. Гончар О., Долобанько А. Інноваційні технології управління у забезпеченні економічної безпеки підприємств та розвитку їх потенціалу. *Development Service Industry Management*. 2025. № 1. С. 272–277. DOI: [https://doi.org/10.31891/dsim-2025-9\(37\)](https://doi.org/10.31891/dsim-2025-9(37))
2. Лега О. В., Макачук А. В. Підвищення точності оцінювання показника функціональної стійкості інформаційних систем у цифровій економіці за допомогою ансамблевих моделей машинного навчання. *Наукові записки Львівського університету бізнесу та права*. 2025. № 47. С. 104–112. URL: <https://nzlubp.org.ua/index.php/journal/article/view/1833> (дата звернення: 25.11.2025).
3. Pal P., Wang Z., Zhu X., Chew J., Prus K., Wei X. AI-Based Credit Risk Assessment and Intelligent Matching Mechanism in Supply Chain Finance. *Journal of Theory and Practice in Economics and Management*. 2025. Т. 2. № 3. С. 1–9. DOI: <https://doi.org/10.5281/zenodo.1536>
4. Liu T., Yang L. Financial Risk Early Warning Model for Listed Companies Using BP Neural Network and Rough Set Theory. *IEEE Access*. 2024. Vol. 12. P. 27456–27464. DOI: <https://doi.org/10.1109/ACCESS.2024.3367228>
5. Vancsura L., Tatay T., Bareith T. Navigating AI-Driven Financial Forecasting: A Systematic Review of Current Status and Critical Research Gaps. *Forecasting*. 2025. Vol. 7. № 3. P. 36. DOI: <https://doi.org/10.3390/forecast7030036>
6. Valencia-Arias A., Jimenez Garcia J. A., Agudelo-Ceballos E., Oré León A. J. A., Martínez Rojas E., Leyrer Henríquez J., Ramírez-Ramírez D. M. Machine learning applications in risk management: Trends and research agenda. *F1000Research*. 2025. Vol. 14. P. 233. DOI: <https://doi.org/10.12688/f1000research.161993.2>
7. Duan Y., Goodell J. W., Li H., Li X. Assessing machine learning for forecasting economic risk: Evidence from an expanded Chinese financial information set. *Finance Research Letters*. 2022. Vol. 46 (PA). DOI: <https://doi.org/10.1016/j.frl.2021.102273>
8. Muria-Tarazón J. C., Oltra-Gutiérrez J. V., Oltra-Badenec R., Escobar-Román S. Uncovering Research Trends on Artificial Intelligence Risk Assessment in Businesses: A State-of-the-Art Perspective Using Bibliometric Analysis. *Applied Sciences*. 2025. Vol. 15. № 3. P. 1412. DOI: <https://doi.org/10.3390/app15031412>
9. Huang H. Technology-Driven Financial Risk Management: Exploring the Benefits of Machine Learning for Non-Profit Organizations. *Systems*. 2024. Vol. 12. № 10. P. 416. DOI: <https://doi.org/10.3390/>

systems12100416

10. Yao K.-C., Hung H.-C., Wang C.-H., Huang W.-L., Liang H.-T., Chu T.-H., Chen B.-S., Ho W.-S. Application of Generative AI in Financial Risk Prediction: Enhancing Model Accuracy and Interpretability. *Information*. 2025. Vol. 16. № 10. P. 857. DOI: <https://doi.org/10.3390/info16100857>

11. Самойлов О. О., Дощенко Г. Г. Потреба у великих і якісних обсягах даних для навчання штучного інтелекту: огляд SCADA як головне джерело даних для прогнозування технічного огляду судна. *Прикладні питання математичного моделювання*. 2025. Т. 8. № 1. DOI: <https://doi.org/10.32782/mathematical-modelling/2025-8-1-19>

12. Буряк А. А., Маслій О. А. Мінімізація цифрових ризиків і загроз економічній безпеці держави із використанням генеративного штучного інтелекту. *Eastern-European Journal of Enterprise Technologies*. 2025. Т. 4. № 13(136). С. 17–25. DOI: <https://doi.org/10.15587/1729-4061.2025.336640>

13. Мірзоева Т. В., Гарбут М. А., Гуцул Т. А. Штучний інтелект як інноваційний інструмент управління ризиками агробізнесу. *Modern Economics*. 2025. № 49. С. 161–169. DOI: [https://doi.org/10.31521/modecon.V49\(2025\)-22](https://doi.org/10.31521/modecon.V49(2025)-22)

14. Тетер Н., Лега О. Прогнозна аналітика на основі штучного інтелекту як інструмент передбачення КРІ та підвищення ефективності стратегічного планування. *Цифрова економіка та економічна безпека*. 2025. № 4(19). С. 454–460. DOI: <https://doi.org/10.32782/dees.19-65>

15. Єршова О. О. Використання штучного інтелекту для оптимізації бізнес-процесів підприємства в контексті сталого розвитку. *Журнал стратегічних економічних досліджень*. 2025. № 2. С. 47–61. DOI: <https://doi.org/10.30857/2786-5398.2025.2.6>

16. Рогоза М., Перебийніс В., Кононенко Ж., Карнаухова Г., Зінченко О. Методологічні аспекти прогнозування економічної безпеки: ризики та інтернет-технології в проєктах розвитку. *Науковий вісник Полтавського університету економіки і торгівлі. Серія «Економічні науки»*. 2025. № 3(117). С. 69–76. DOI: <https://doi.org/10.37734/2409-6873-2025-3-9>

References

1. Honchar, O., & Dolobanko, A. (2025). Innovatsiini tekhnolohii upravlinnia u zabezpechenni ekonomichnoi bezpeky pidpriemstv ta rozvytku yikh potentsialu [Innovative management technologies in ensuring economic security of enterprises and developing their potential]. *Development Service Industry Management*, (1), 272–277. [https://doi.org/10.31891/dsim-2025-9\(37\)](https://doi.org/10.31891/dsim-2025-9(37)) [in Ukrainian]

2. Leha, O. V., & Makarchuk, A. V. (2025). Pidvyshchennia tochnosti otsiniuvannia pokaznyka funktsionalnoi stiikosti informatsiinykh system u tsyfrovii ekonomitsi za dopomohoiu ansamblevykh modelei mashynnoho navchannia [Improving the accuracy of assessing functional stability indicators of information systems in the digital economy using ensemble machine learning models]. *Naukovi zapysky Lvivskoho universytetu biznesu ta prava*, (47), 104–112. Retrieved from <https://nzlubp.org.ua/index.php/journal/article/view/1833> [in Ukrainian]

3. Pal, P., Wang, Z., Zhu, X., Chew, J., Prus, K., & Wei, X. (2025). AI-Based Credit Risk Assessment and Intelligent Matching Mechanism in Supply Chain Finance. *Journal of Theory and Practice in Economics and Management*, 2(3), 1–9. <https://doi.org/10.5281/zenodo.1536>

4. Liu, T., & Yang, L. (2024). Financial Risk Early Warning Model for Listed Companies Using BP Neural Network and Rough Set Theory. *IEEE Access*, 12, 27456–27464. <https://doi.org/10.1109/ACCESS.2024.3367228>

5. Vancsura, L., Tatay, T., & Bareith, T. (2025). Navigating AI-Driven Financial Forecasting: A Systematic Review of Current Status and Critical Research Gaps. *Forecasting*, 7(3), 36. <https://doi.org/10.3390/forecast7030036>

6. Valencia-Arias, A., Jimenez Garcia, J. A., Agudelo-Ceballos, E., Ore León, A. J. A., Martínez Rojas, E., Leyrer Henríquez, J., & Ramírez-Ramírez, D. M. (2025). Machine learning applications in risk management: Trends and research agenda. *F1000Research*, 14, 233. <https://doi.org/10.12688/f1000research.161993.2>

7. Duan, Y., Goodell, J. W., Li, H., & Li, X. (2022). Assessing machine learning for forecasting economic risk: Evidence from an expanded Chinese financial information set. *Finance Research Letters*, 46(PA). <https://doi.org/10.1016/j.frl.2021.102273>

8. Muria-Tarazón, J. C., Oltra-Gutiérrez, J. V., Oltra-Badenes, R., & Escobar-Román, S. (2025). Uncovering Research Trends on Artificial Intelligence Risk Assessment in Businesses. *Applied Sciences*, 15(3), 1412. <https://doi.org/10.3390/app15031412>

9. Huang, H. (2024). Technology-Driven Financial Risk Management: Exploring the Benefits of Machine

Learning for Non-Profit Organizations. *Systems*, 12(10), 416. <https://doi.org/10.3390/systems12100416>

10. Yao, K.-C., Hung, H.-C., Wang, C.-H., Huang, W.-L., Liang, H.-T., Chu, T.-H., Chen, B.-S., & Ho, W.-S. (2025). Application of Generative AI in Financial Risk Prediction: Enhancing Model Accuracy and Interpretability. *Information*, 16(10), 857. <https://doi.org/10.3390/info16100857>

11. Samoilov, O. O., & Doshchenko, H. H. (2025). Potreba u velykykh i yakisnykh obsiahakh danykh dlia navchannia shtuchnoho intelektu: ohliad SCADA yak holovne dzherelo danykh dlia prohnozuvannia tekhnichnoho ohliadu sudna [The need for large and high-quality datasets for artificial intelligence training: SCADA as the main data source for ship maintenance forecasting]. *Prykladni pytannia matematychnoho modeliuvannia*, 8(1). <https://doi.org/10.32782/mathematical-modelling/2025-8-1-19> [in Ukrainian]

12. Buriak, A. A., & Maslii, O. A. (2025). Minimizatsiia tsyfrovyykh ryzykiv i zahroz ekonomichnii bezpetsi derzhavy iz vykorystanniam heneratyvnogo shtuchnoho intelektu [Minimizing digital risks and threats to state economic security using generative AI]. *Eastern-European Journal of Enterprise Technologies*, 4(13(136)), 17–25. <https://doi.org/10.15587/1729-4061.2025.336640> [in Ukrainian]

13. Mirzoieva, T. V., Harbut, M. A., & Hutsul, T. A. (2025). Shtuchnyi intelekt yak innovatsiinyi instrument upravlinnia ryzykamy ahrobiznesu [Artificial intelligence as an innovative tool for agribusiness risk management]. *Modern Economics*, 49, 161–169. [https://doi.org/10.31521/modecon.V49\(2025\)-22](https://doi.org/10.31521/modecon.V49(2025)-22) [in Ukrainian]

14. Teter, N., & Leha, O. (2025). Prohnozna analityka na osnovi shtuchnoho intelektu yak instrument peredbachennia KPI ta pidvyshchennia efektyvnosti stratehichnoho planuvannia [AI-based predictive analytics as a tool for forecasting KPIs and improving strategic planning]. *Tsyfrova ekonomika ta ekonomichna bezpeka*, 4(19), 454–460. <https://doi.org/10.32782/dees.19-65> [in Ukrainian]

15. Yershova, O. O. (2025). Vykorystannia shtuchnoho intelektu dlia optymizatsii biznes-protsesiv pidpriemstva v konteksti staloho rozvytku [Use of artificial intelligence for optimizing business processes in the context of sustainable development]. *Zhurnal stratehichnykh ekonomichnykh doslidzhen*, 2, 47–61. <https://doi.org/10.30857/2786-5398.2025.2.6> [in Ukrainian]

16. Rohoza, M., Perebyinis, V., Kononenko, Zh., Karnaukhova, H., & Zinchenko, O. (2025). Metodolohichni aspekty prohnozuvannia ekonomichnoi bezpeky: ryzyky ta internet-tekhnologii v proektakh rozvytku [Methodological aspects of economic security forecasting: risks and Internet technologies in development projects]. *Naukovyi visnyk Poltavskoho universytetu ekonomiky i torhivli. Serii: Ekonomichni nauky*, 3(117), 69–76. <https://doi.org/10.37734/2409-6873-2025-3-9> [in Ukrainian]