CENTRAVIS

ЗБІРНИК НАУКОВИХ ПРАЦЬ

ЕКОНОМІЧНА КІБЕРНЕТИКА: СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В УПРАВЛІННІ

Міністерство освіти і науки України
Український державний університет науки і технологій

ЕКОНОМІЧНА КІБЕРНЕТИКА: СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В УПРАВЛІННІ

Збірник наукових праць
за матеріалами Всеукраїнської науково-практичної
інтернет-конференції
3-4 березня 2026 р.

Дніпро
2026

УДК 330.46

Організатори конференції:
кафедра економічної інформатики
Українського державного університету науки і технологій;
Національний університет «Запорізька політехніка».
Склад редакційної групи:
Бандоріна Л.М., Удачина К.О., Підгорна К.Д.

Економічна кібернетика : сучасні інформаційні технології в управлінні : збірник наукових праць за матеріалами Всеукраїнської науково-практичної інтернет-конференції, м. Дніпро, 3-4 березня 2026 р. Дніпро : УДУНТ, 2026. 260 с.

Збірник наукових статей за матеріалами Всеукраїнської інтернет-конференції, присвяченої актуальним проблемам розвитку та впровадження сучасних інформаційних технологій у сфері управління, виробництва, логістики, фінансів, освіти та державного управління. Розглянуто теоретичні й прикладні аспекти побудови систем аналізу та підтримки прийняття обґрунтованих управлінських рішень, а також інструменти й методи оптимізації виробничих, логістичних і фінансових процесів. Окрему увагу приділено питанням цифрової трансформації в освіті, науці, промисловості та публічному управлінні, зокрема застосуванню цифрових платформ, аналітичних систем, технологій оброблення даних і моделювання складних соціально-економічних процесів.

Збірник призначено для науковців, викладачів, аспірантів, здобувачів вищої освіти, а також фахівців-практиків у галузі інформаційних технологій, економіки, управління та цифрової трансформації.

Матеріали подано в авторській редакції.
Відповідальність за дотримання норм авторського права, за зміст і достовірність матеріалів несуть автори.

ЗМІСТ

СИСТЕМИ АНАЛІЗУ ТА ПРИЙНЯТТЯ ОБҐРУНТОВАНИХ УПРАВЛІНСЬКИХ РІШЕНЬ

ЦИФРОВА ТРАНСФОРМАЦІЯ У СФЕРІ ОСВІТИ, НАУКИ, ВИРОБНИЦТВА І ДЕРЖАВНОГО УПРАВЛІННЯ

ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ ВИКОРИСТАННІ ШІ ДЛЯ ЕКОНОМІЧНОЇ ДІАГНОСТИКИ НА ПІДПРИЄМСТВІ

Савчук Л.М.

кандидат економічних наук, професор,

професор кафедри економічної інформатики,

Бабошкін І.І.

аспірант кафедри економічної інформатики

Український державний університет науки і технологій

м. Дніпро, Україна

Анотація: Виконана систематизація ключових проблем інформаційної безпеки, що виникають при використанні технологій ШІ в процесах економічної діагностики підприємств, а також надані рекомендацій щодо їх мінімізації з урахуванням специфіки українського бізнес-середовища. У роботі розглянуто теоретичні основи застосування ШІ в економічному аналізі, класифіковано основні кіберризики, проаналізовано реальні приклади загроз та оцінено їх потенційні наслідки. На основі проведеного аналізу запропоновано комплекс заходів захисту, що мають практичну цінність для менеджменту підприємств, які планують або вже застосовують ШІ-інструменти в економічній діагностиці.

Ключові слова: штучний інтелект, економічна діагностика підприємства, інформаційна безпека, кіберризики ШІ, витік конфіденційних даних, атаки на моделі штучного інтелекту, економічна безпека бізнесу, GDPR.

Постановка проблемию. У сучасних умовах цифрової трансформації економіки штучний інтелект (ШІ) перетворюється на ключовий інструмент підвищення конкурентоспроможності та ефективності управління підприємствами. Застосування технологій ШІ в економічній діагностиці дозволяє автоматизувати аналіз фінансової звітності, прогнозування ризиків

банкрутства, оцінку ліквідності, прибутковості та стійкості бізнесу, забезпечуючи обробку великих обсягів даних у реальному часі та суттєве підвищення точності управлінських рішень [1]. За даними 2026 року, 93 % українських компаній уже використовують ШІ в операційній діяльності, тоді як глобальний показник перевищує 78 % [2]. У фінансовому та аналітичному секторах ШІ застосовується для кредитного скорингу, виявлення шахрайства та стратегічного планування, що скорочує операційні витрати й прискорює прийняття рішень.

Водночас стрімке впровадження ШІ супроводжується суттєвим зростанням загроз інформаційної безпеки. Конфіденційні дані підприємств стають об’єктом атак та витоків через хмарні сервіси [3]. За оцінками, 87 % керівників компаній вважають вразливості ШІ найшвидше зростаючим кіберризиком, а в Україні ця проблема посилюється геополітичними факторами та обмеженими ресурсами на кібербезпеку [4].

Актуальність теми зумовлена поєднанням двох протилежних тенденцій: ШІ стає невід’ємною частиною економічної діагностики, але водночас створює нові вектори кіберзагроз, які традиційні системи захисту не завжди здатні нейтралізувати.

Виклад основного матеріалу. Економічна діагностика підприємства – це комплексна оцінка фінансового стану, ефективності діяльності, ризиків та потенціалу розвитку з метою обґрунтування управлінських рішень [1]. Традиційні методи (коефіцієнтний, трендовий, Z-score) мають обмеження щодо швидкості обробки даних та адаптивності до динамічних змін.

Штучний інтелект у контексті економічної діагностики визначається як сукупність алгоритмів, що імітують когнітивні функції людини для аналізу, прогнозування та прийняття рішень на основі великих даних [5]. До основних технологій відноситься машинне навчання (supervised/unsupervised) та ансамблеві методи (XGBoost, Random Forest), які використовуються для прогнозування банкрутства та класифікації ризиків; глибоке навчання (LSTM, трансформери) для аналізу часових рядів фінансових показників;обробка

природної мови (NLP) та генеративний ШІ для аналізу текстових звітів і формування рекомендацій.

Переваги застосування ШІ порівняно з традиційними методами надані у таблиці 1 і включають обробку великих обсягів структурованих і неструктурованих даних у реальному часі;підвищення точності прогнозів банкрутства до 90–99 % (AUC 0,92–0,99), що на 10–25 % перевищує класичні моделі[6];автоматизація рутинних процесів і скорочення часу аналізу з днів до хвилин; адаптивність моделей через постійне перенавчання; генерація сценаріїв «що-якщо» та рекомендацій щодо управління ліквідністю та капіталом[7].

В Україні застосування ШІ в економічній діагностиці активно зростає: у 2025–2026 рр. 24–42 % компаній використовують його для фінансового аналізу, прогнозування та оптимізації, особливо в банківському секторі, агробізнесі та промисловості [4].

Застосування штучного інтелекту в економічній діагностиці підприємства, попри значні переваги, створює комплекс специфічних загроз інформаційної безпеки, які виникають на всіх етапах життєвого циклу моделей – від підготовки даних до експлуатації. Ці ризики суттєво відрізняються від традиційних кіберзагроз і можуть призводити до спотворення результатів діагностики, витоку конфіденційних даних та серйозних фінансових втрат [3].

Таблиця 1. Порівняння традиційних методів та ШІ-інструментів в економічній діагностиці

Критерій	Традиційні методи	ШІ-інструменти	Перевага ШІ (%)
Точність прогнозування банкрутства	70–85 %	90–99 %	+15–25
Швидкість обробки даних	Дні–тижні	Секунди–хвилини	×100–1000
Обсяг даних	Обмежений (структуровані звіти)	Великі + неструктуровані дані	Значна
Адаптивність до змін	Низька	Висока (перенавчання)	Значна
Вартість впровадження	Низька–середня	Середня–висока (початкова)	Окупність 12–24 міс.

Ризики, пов’язані з використанням ШІ для економічної діагностики можна класифікувати за трьома рівнями вразливості: технічні, організаційні ризики пов’язані з інфраструктурою, правові та етичні ризики.

До технічні ризиків відносяться ворожі атаки (adversarial attacks), псування даних (data poisoning), вилучення моделі (model extraction), непрозорість чорної скриньки (black-box opacity) [8].

До організаційних ризиків відносяться витік конфіденційних фінансових даних через хмарні сервіси та інсайдерські загрози (зростання таких інцидентів на 56–80 % у 2025–2026 рр.), концентрація ризиків у постачальників (supply chain risks)[9].

Правові та етичні ризики включають порушення вимог GDPR, Закону України «Про захист персональних даних» та Акту ЄС про ШІ, що загрожує значними штрафами; упередженість (bias) моделей, яка призводить до дискримінаційних висновків діагностики та потенційних судових позовів.

Специфіка економічної діагностики полягає в тому, що спотворення результатів аналізу безпосередньо впливає на стратегічні рішення підприємства, конкурентоспроможність та економічну безпеку бізнесу.

Теоретичні загрози інформаційної безпеки при використанні ШІ в економічній діагностиці набувають реальних форм у практиці підприємств 2025–2026 рр. Атаки на ШІ-системи призводять не лише до технічного компрометації, а й до спотворення результатів аналізу фінансової звітності, прогнозів ліквідності, оцінки ризиків банкрутства та стратегічних рішень [3].

Одним із наймасштабніших прикладів стала атака на ланцюг постачання через компрометацію ШІ-додатка Drift (інтегрованого з Salesforce). Зловмисники викрали OAuth-токени, отримавши доступ до сотень корпоративних середовищ і конфіденційних фінансових даних, що використовуються для навчання моделей прогнозування грошового потоку та оцінки стійкості.

Реальні випадки псування даних фіксуються в системах виявлення шахрайства та фінансового аналізу: навіть 1 % зіпсованих даних призводить до систематичного спотворення прогнозів банкрутства та хибних управлінських рішень [10].

В Україні 2025–2026 рр. CERT-UA зафіксувала 4315 кіберінцидентів (зростання на 70 %), 38 % з яких спрямовані на приватний сектор. Понад 67 % фішингових атак використовували генеративний ШІ та deepfake. Середній час виявлення компрометації становить 197–277 днів, що критично для ШІ-систем, які постійно перенавчаються на корпоративних даних [11]. Яскраві приклади: атака на логістичну компанію (25 працівників) з блокуванням сервера 1С та втратами $12 000; BEC-атака на юридичну фірму з несанкціонованим переказом ₴340 000. Такі інциденти безпосередньо блокують доступ до фінансових даних і унеможливлюють оперативну економічну діагностику. Оцінка наслідків практичних ризиків ШІ в економічній діагностиці надана у таблиці 2.

Порівняльний аналіз показує суттєві відмінності: МСБ (до 250 працівників) становить 43 % глобальних цілей атак через відсутність професійного захисту. 60 % малих компаній закриваються протягом 6 місяців після інциденту. Великий бізнес стає мішенню складніших атак на ланцюги постачань та хмарні ШІ-сервіси, але має кращі можливості відновлення [12].

Таблиця 2. Оцінка наслідків практичних ризиків ШІ в економічній діагностиці

Тип ризику	Наслідки для підприємства	Середні втрати (2025–2026)
Витік/псування даних	Спотворення прогнозів банкрутства, ліквідності	$4,45 млн (глобально); $25–50 тис. (МСБ Україна)
Ворожі атаки	Помилкові управлінські рішення	Втрата контрактів, інвестицій
Вилучення моделі	Втрата конкурентної переваги (алгоритми діагностики)	Репутаційні + юридичні штрафи
ШІ-фішинг / deepfake	Блокування доступу до фінансових даних	₴340 тис. – кілька млн (Україна)

На основі проведеного аналізу пропонується комплексний підхід до мінімізації ризиків використання ШІ в економічній діагностиці підприємства. Рекомендації поділяються на технічні, організаційно-правові та регуляторні заходи з урахуванням специфіки українського бізнесу.

Технічні заходи включають впровадження навчання на державному рівні (federated learning) та диференціальної конфіденційності(differential privacy), коли дані залишаються локально, а навчання відбувається на агрегованих градієнтах з додаванням контрольованого шуму, що суттєво знижує ризик витоку та псування даних[10]; перехід на зрозумілий ШІ (Explainable AI, XAI) (SHAP, LIME) для забезпечення прозорості рішень і виявлення упереджень чи атак; регулярна атака «червоної команди» (red-teaming) та аудит моделей за OWASP LLM Top 10 і NIST Adversarial ML Taxonomy; шифрування даних, шлюзи ШІ та безпечні багатосторонні обчислення (secure multi-party computation) для захисту в процесі навчання та експлуатації [13].

До організаційно-правових заходів відносяться розробка внутрішньої політики використання ШІ з чіткими правилами роботи з конфіденційними даними та обов'язковим маркуванням ШІ-генерованих звітів; інтеграція ISO/IEC 42001 у систему управління інформаційною безпекою (ISO 27001) з обов'язковою оцінкою ризиків ШІ; щорічне навчання персоналу та впровадження кіберстрахування з покриттям ШІ-специфічних інцидентів [14].

Пропозиції для національного рівня в Україні включають адаптацію Акту ЄС щодо ШІ з визнанням економічної діагностики ШІ як високоризикової категорії; створення регуляторних «пісочниць» для тестування ШІ-інструментів; розробку державних рекомендацій з кібербезпеки ШІ Адміністрацією Держспецзв'язку.

Запропоновані рекомендації забезпечують баланс між інноваціями та безпекою, дозволяючи підприємствам використовувати ШІ для економічної діагностики без критичних ризиків. Їх впровадження вимагає поетапного

підходу: спочатку – аудит та політика, потім – технічні контролі, з постійним моніторингом ефективності.

Матриця ключових заходів мінімізації ризиків наведена у таблиці 3.

Таблиця 3. Матриця ключових заходів мінімізації ризиків

Ризик	Заходи захисту	Очікуваний ефект	Рівень впровадження (МСБ / Великий бізнес)
Псування даних	Федерат. навч. + Диф. конф. + очищ. даних	Зниження впливу на 70–90 %	Середній / Високий
Ворожі атаки	Adversarial training + атака «черв. команди»	Підвищення robustness на 40–60 %	Високий / Високий
Витік даних	Диф. конф.+ шифрування + шлюзи ШІ	Контроль витоку < 1 %	Середній / Високий
Непрозорість чорної скриньки	XAI (SHAP/LIME) + аудит	Повна пояснюваність рішень	Високий / Високий
Концентрація ризиків у постачальниках	Оцінка постачальника + ISO 42001	Зниження системних вразливостей	Низький / Високий

Джерело: узагальнено за [10]; [14].

Висновки. Проведене дослідження доводить, що штучний інтелект став потужним інструментом підвищення ефективності економічної діагностики підприємств. В Україні частка компаній, що застосовують ШІ в аналітиці та фінансовому плануванні, зросла до 24–42 % у 2025–2026 рр., відображаючи глобальну тенденцію цифрової трансформації.

Водночас впровадження ШІ супроводжується суттєвим зростанням загроз інформаційної безпеки. За даними оглядів, 87 % керівників компаній вважають вразливості ШІ найактуальнішим ризиком. В Україні ця проблема посилюється геополітичними факторами, обмеженими ресурсами МСБ та зростанням ШІ-фішингу на 70 %.

Практичні кейси 2025–2026 рр. підтверджують, що спотворення результатів діагностики призводить до помилкових рішень, фінансових втрат від десятків тисяч до мільйонів доларів та навіть припинення діяльності підприємств, особливо МСБ.

Запропонований комплекс заходів дозволяє суттєво знизити вразливість без блокування інновацій. На національному рівні необхідна адаптація Акту ЄС щодо ШІ, створення регуляторних «пісочниць» та державних стандартів для ШІ високого ризику в економічній діагностиці.

Результати дослідження мають практичну цінність для менеджменту українських підприємств, сприяючи балансу між конкурентоспроможністю та інформаційною безпекою. Перспективи подальших досліджень: емпіричне тестування запропонованих заходів на реальних даних українських компаній та розробка стійких до кіберзагроз моделей ШІ в умовах воєнного та післявоєнного відновлення економіки.

Перелік посилань:

1. Поповиченко І.В., Спірідонова К.О., Андрійчук А.С. Застосування штучного інтелекту в фінансово-економічному аналізі діяльності підприємства. *Економічний простір,* т. 189. 2024. pp. 81-84.

2. Джугалик Д. 93% українських компаній вже використовують ШІ – дослідження. URL: https://mezha.ua/news/ai-amongst-ukrainian-business-307586/.

3. Global Cybersecurity Outlook 2026.World Economic Forum, 2026. URL: https://www.weforum.org/publications/global-cybersecurity-outlook-2026/

4. Галузеві тренди. Штучний інтелект в Україні: як розвивається галузь. URL: https://hub.kyivstar.ua/articles/galuzevi-trendi-shtuchnij-intelekt-v-ukrayini-yak-rozvivayetsya-galuz.

5. Клюс Ю. І. Можливості ШІ в економічній аналітиці бізнесу та держави [Електронний ресурс] / Клюс Ю. І., Гуменюк В. В. // Економічна аналітика: сучасні реалії та прогностичні можливості : матеріали тез II Міжнар. наук.-практ. конф.; 24 січ. 2025 р. / М-во освіти і науки України, Київ. нац. екон. ун-т ім. В. Гетьмана [та ін.] ; [редкол.: О. Ткаченко, І. Кулага, Л. Козловська]. – Електрон. текст. дані. – Київ : КНЕУ, 2025. – С. 258–260.

6. Qi R. Enterprise Financial Distress Prediction Based on Machine Learning and SHAP Interpretability Analysis. AIDF '25: Proceedings of the 2025 International

Conference on Artificial Intelligence and Digital Finance. New York, NY, USA, 2025. Pages 76-79. DOI: https://doi.org/10.1145/3764727.3764740

7. Belelieu A., Propson D., Parker D. Artificial Intelligence in Financial Services. World Economic Forum, 2025.

8. Firch J. The Top AI Security Risks. URL: https://purplesec.us/learn/ai-security-risks/.

9. Artificial Intelligence Index Report 2025. Stanford University, 2025.

10. Vassilev A., Oprea A., Fordyce A., Anderson H., Davies X., Hamin M. Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations, Gaithersburg: National Institute of Standards and Technology, 2025. DOI: https://doi.org/10.6028/NIST.AI.100-2e2025

11. Статистика кібератак на український бізнес у 2026 році: цифри, тренди та захист. URL: https://it-premium.com.ua/blog/statystyka-kiberatak-ukrainskyj-biznes-2026/.

12. Bruemmer M., Steven J. 2026 Data Breach Industry Forecast. Experian, 2025.

13. Тренди кібербезпеки: до чого готуватись у 2026 році? URL: https://bakotech.com/articles/trendy-kiberbezpeky-do-chogo-gotuvatys-u-2026-roczi/.

14. Пауддар С. Безпека ШІ: Ризики, Регулювання та ISO 42001. URL: https://www.dqsglobal.com/uk/doslidzhujte/blog/bezpeka-shi-riziki,-regulyuvannya-ta-iso-42001.

НАУКОВЕ ВИДАННЯ

ЕКОНОМІЧНА КІБЕРНЕТИКА: СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В УПРАВЛІННІ

Збірник наукових праць
за матеріалами Всеукраїнської науково-практичної
інтернет-конференції
3-4 березня 2026 р.

Відповідальний редактор Л.М. Бандоріна
Комп'ютерна верстка К.Д. Підгорна

Український державний університет науки і технологій
2026