АКТУАЛЬНІ ПИТАННЯ ЕКОНОМІЧНИХ НАУК

Облік і оподаткування

УДК 657:330

DOI https://doi.org/10.5281/zenodo.18279046

Інноваційні підходи до запобігання шахрайству в аудиті на основі інтеграції штучного інтелекту у бізнес-процеси підприємства

Пашкевич Марина Сергіївна

доктор економічних наук, професор, завідувач кафедри міжнародних відносин і аудиту Національного технічного університету «Дніпровська політехніка», просп. Д. Яворницького 19, Дніпро, 49005, Україна,

Email: pashkevych.m.s@nmu.one,

ORCID ID: https://orcid.org/0000-0003-3012-1690

Усатенко Ольга Вікторівна

доктор економічних наук, професор, завідувач кафедри економічного аналізу і фінансів Національного технічного університету «Дніпровська політехніка», просп. Д. Яворницького 19, Дніпро, 49005, Україна,

Email: Usatenko.Ol.V@nmu.one,

ORCID ID: https://orcid.org/0000-0003-3198-9002

Усатенко Максим Володимирович

аспірант, Національний технічний університет «Дніпровська політехніка», просп. Д. Яворницького 19, Дніпро, 49005, Україна,

Email: Usatenko.Mak.V@nmu.one,

ORCID ID: https://orcid.org/0009-0006-4360-5597

Прийнято: 02.01.2026 | Опубліковано: 17.01.2026

АКТУАЛЬНІ ПИТАННЯ ЕКОНОМІЧНИХ НАУК

Анотація: У сучасних умовах цифрової трансформації облікових та аудиторських систем особливої актуальності набуває проблема шахрайства в аудиті, що негативно впливає на достовірність фінансової інформації та прийняття управлінських рішень. З огляду на це, інтеграція штучного інтелекту у бізнес-процеси підприємства розглядається як інноваційний інструмент підвищення надійності аудиту. Застосування цифрових технологій дозволяє автоматизувати рутинні процедури, знижуючи ризик людського чинника, а також своєчасно виявляти ознаки маніпуляцій чи помилок у фінансовій звітності. **Метою** даної статті є дослідження інноваційних підходів до запобігання шахрайству в аудиті шляхом інтеграції інструментів штучного інтелекту у внутрішні бізнес-процеси підприємств, зокрема в частині обробки облікових даних, аналітики ризиків і верифікації звітності. **Методологічну основу** дослідження становлять системний та ризик-орієнтований підходи, а також порівняльний аналіз сучасних цифрових рішень, що використовуються в облікових і аудиторських практиках в Україні та за кордоном. **Результати.** У статті охарактеризовано механізми виявлення шахрайства на основі алгоритмів штучного інтелекту, зокрема засобів машинного навчання, інтелектуального аналізу даних, нейромережевого аналізу та систем розпізнавання аномалій у транзакційній активності. Продемонстровано, як автоматизоване опрацювання великих обсягів облікових даних дозволяє виявляти приховані закономірності, що можуть свідчити про потенційні шахрайські дії або викривлення у фінансовій звітності. Обґрунтовано економічну доцільність впровадження таких технологій у бізнес-процеси підприємств, зокрема в частині внутрішнього аудиту та контролю, як інструменту підвищення ефективності аудиторських перевірок, зменшення витрат на ручну обробку даних та підвищення точності виявлення ризиків. Проаналізовано ризики та обмеження цифрових рішень. **Зроблено висновок**, що застосування штучного інтелекту в аудиті створює новий рівень протидії шахрайству, забезпечуючи підвищення об’єктивності та достовірності аудиторських висновків.

Ключові слова: аудит, шахрайство, штучний інтелект, бізнес-процеси, внутрішній контроль, цифрова трансформація, автоматизація бізнес-процесів

Innovative Approaches to Audit Fraud Prevention through the Integration of Artificial Intelligence into Enterprise Business Processes

Maryna Pashkevych
Doctor of Economic Sciences, Professor, Head of the Department of International Relations and Auditing, Dnipro University of Technology, 19, D. Yavornytskyi Ave., Dnipro, 49005, Ukraine
Email: pashkevych.m.s@nmu.one,
ORCID ID: https://orcid.org/0000-0003-3012-1690

Olga Usatenko
Doctor of Economic Sciences, Professor, Head of the Department of Economic Analysis and Finance, Dnipro University of Technology, 19, D. Yavornytskyi Ave., Dnipro, 49005, Ukraine
Email: usatenko.ol.v@nmu.one
ORCID ID: https://orcid.org/0000-0003-3198-9002

Maxym Usatenko,
Postgraduate student, Dnipro University of technology, 19, D. Yavornytskyi Ave., Dnipro, 49005, Ukraine
Email: Usatenko.Mak.V@nmu.one,
ORCID ID: https://orcid.org/0009-0006-4360-5597

Abstract: In the context of the ongoing digital transformation of accounting and auditing systems, the issue of audit fraud has become increasingly relevant, as it negatively affects the reliability of financial information and the quality of managerial

decision-making. In this regard, the integration of artificial intelligence into enterprise business processes is viewed as an innovative tool for enhancing audit reliability. The application of digital technologies enables the automation of routine procedures, thereby reducing the impact of human error and facilitating the timely detection of potential manipulations or inaccuracies in financial reporting.

The purpose of this study is to examine innovative approaches to audit fraud prevention through the integration of artificial intelligence tools into internal business processes, particularly in the areas of accounting data processing, risk analytics, and report verification. **The methodological basis of the research** includes a systems-based and risk-oriented approach, as well as a comparative analysis of modern digital solutions applied in accounting and audit practices in Ukraine and internationally.

Results. The article characterizes mechanisms for fraud detection based on artificial intelligence algorithms, including machine learning tools, data mining, neural network analysis, and anomaly detection systems in transactional activity. It demonstrates how the automated processing of large volumes of accounting data reveals hidden patterns that may indicate potential fraudulent activities or distortions in financial reporting. The study substantiates the economic feasibility of implementing such technologies within enterprise business processes – particularly in internal audit and control – as a means of increasing audit efficiency, reducing the costs of manual data processing, and improving the accuracy of risk detection. The paper also analyzes the risks and limitations of digital solutions under current regulatory gaps and professional preparedness challenges. It concludes that the use of artificial intelligence in auditing establishes a new level of fraud prevention, ensuring greater objectivity and reliability in audit conclusions.

Keywords: audit, fraud, artificial intelligence, business processes, internal control, digital transformation, business process automation.

Постановка проблеми у загальному вигляді та її зв'язок з важливими науковими чи практичними завданнями. В умовах цифрової трансформації

економіки, глобалізації фінансових ринків і зростання обсягів даних, що підлягають обліку та аудиту, проблема шахрайства в аудиті набуває особливої актуальності. Підвищена увага суспільства, інвесторів, регуляторних органів до прозорості фінансової звітності та довіри до аудиторських висновків актуалізує необхідність пошуку нових підходів до виявлення та запобігання маніпуляціям у сфері обліку.

Традиційні аудиторські інструменти, орієнтовані на вибірковий аналіз даних та пост-фактум перевірки, дедалі частіше виявляються недостатньо ефективними в умовах складних і швидкозмінних бізнес-процесів. Це створює простір для поширення шахрайських схем, зокрема тих, що базуються на багаторівневих транзакціях, креативному обліку або навмисному приховуванні фінансових показників. У відповідь на ці виклики, провідні компанії починають інтегрувати інструменти штучного інтелекту (ШІ) у внутрішні процеси аудиту та контролю з метою своєчасного виявлення аномалій, моделювання ризиків і верифікації інформації в реальному часі.

Однак, попри зростаючий інтерес до впровадження цифрових технологій у сфері аудиту, залишається недостатньо дослідженим механізм впливу ШІ на зниження ризиків шахрайства, а також економічна доцільність і практична ефективність таких рішень в умовах реального функціонування підприємств. Не менш важливим є питання правової та професійної готовності до роботи з ШІ в аудиті, зокрема з урахуванням конфіденційності даних, відповідальності за висновки, сформовані алгоритмами, та рівня довіри до цифрових рішень.

Таким чином, постає комплексна науково-практична проблема, що поєднує аспекти протидії шахрайству, цифрової трансформації обліку та аудиту, економічної ефективності інноваційних рішень і професійної відповідальності в умовах автоматизації бізнес-процесів. Її вирішення має важливе значення для підвищення якості аудиторських послуг, прозорості фінансової звітності та зміцнення довіри до аудиту як суспільного інституту.

Аналіз останніх досліджень і публікацій. Інтерес до застосування штучного інтелекту у сфері аудиту та виявлення шахрайства неухильно зростає, що знаходить відображення у численних наукових публікаціях останніх років. Наукова спільнота дедалі частіше звертається до міждисциплінарного підходу, поєднуючи технологічні інновації з економічною, управлінською та аудиторською проблематикою.

У роботі Ramos S., Perez-Lopez J. A., Abreu R. [1, с. 330–342] проведено бібліометричний аналіз тенденцій застосування ШІ в аудиті та виявленні шахрайства. Дослідники виокремили ключові напрями розвитку цієї сфери, зокрема аналітику ризиків, автоматизацію перевірок і впровадження XAI (explainable AI). Подібний вектор дослідження підтримали Yaseen H. та Al-Amarneh A. [2, с. 217], які наголошують на важливості таких нематеріальних чинників, як довіра, прозорість та сприйняття справедливості при впровадженні ШІ -систем у фінансові інститути. Вони підкреслюють, що успішність інтеграції технологій значною мірою залежить від рівня прийняття інновацій з боку користувачів.

Bou Reslan F. та Jabbour Al Maalouf N. [3, с. 577] зосереджуються на трансформаційному впливі ШІ на ефективність, виявлення шахрайства та динаміку навичок у бухгалтерській практиці. Їхнє дослідження показує, що впровадження ШІ не лише змінює технологічний ландшафт, а й вимагає переосмислення компетентностей персоналу. У свою чергу, Nguyen T. C. та співавт. [4, с. 1–18] запропонували модель прогнозування шахрайства у фінансовій звітності на основі методів машинного навчання, що підтверджує зростання ефективності алгоритмів у порівнянні з традиційними методами аудиту. Комплексний літературний огляд із фокусом на машинне навчання для виявлення фінансового шахрайства представлено в роботі Hernandez Aros L. та ін. [5], яка окреслює сучасні методологічні підходи до побудови детекторів аномалій. Систематизацію методів машинного навчання, з акцентом на технічну реалізацію, надають Compagnino A. A. та співавт. [6], пропонуючи структуру для

класифікації алгоритмів за їх придатністю до виявлення шахрайських дій. У свою чергу, Tümmler M. і Quick R. [7, с. 115–132] проводять систематичний огляд експериментальних досліджень з виявлення шахрайства в аудиті, що дозволяє оцінити валідність різних підходів у практиці.

Цінний приклад емпіричного дослідження представили Kokina J. та ін. [8], які вивчили виклики і можливості впровадження ШІ у польових аудиторських умовах. Їхня робота розкриває бар'єри, пов'язані з довірою до технологій, складністю інтерпретації результатів і професійною етикою. Водночас Sanz Martín L. та ін. [9, с. 1–42] здійснили бібліометричний та систематичний огляд еволюції ШІ і суміжних технологій у сфері обліку й фінансів, що демонструє стрімке зростання дослідницького інтересу до тематики.

Reyes Lazo M. D. та ін. [10, с. 523] розглядають фінансовий аудит як дієвий інструмент виявлення шахрайства, підкреслюючи його роль у системі внутрішнього контролю. Зміщення акценту з технології на інформаційні системи спостерігається в роботі Qatawneh A. M. [11, с. 1391–1409], яка демонструє, як NLP (Natural Language Processing) може модифікувати підходи до аналізу текстових даних у бухгалтерії. Bhattacharya I. та Mickovic A. [12] підтримують цю ідею, застосовуючи контекстне навчання мови для виявлення обману у фінансовій звітності.

Georgiou I. та співавт. [13, с. 276] зосереджуються на системному огляді використання блокчейн-технологій у бухгалтерії та аудиті, зокрема при роботі з криптовалютами, що відкриває нові горизонти боротьби з шахрайством. Тим часом Hafez I. Y. та ін. [14, с. 6] аналізують ШІ -підходи до виявлення шахрайства з кредитними картками, акцентуючи на гнучкості моделей у виявленні динамічних шахрайських шаблонів.

Останні публікації також розкривають інтегровані техніко-аналітичні підходи. Sodnomdavaa T. та Lkhagvadorj G. [15, с. 13] пропонують поєднання машинного навчання з XAI (пояснювальний ШІ) для підвищення прозорості процесу виявлення шахрайства. Leocádio D. та ін. [16, с. 238] формують

концептуальну основу для інтеграції ШІ в аудиторські практики, акцентуючи на управлінських та нормативних викликах.

Значущу етичну проблематику застосування ШІ в аудиті порушують Murikah W. та співавт. [17], підкреслюючи потенціал упередженості алгоритмів і потребу в етичному регулюванні. Ця тема перегукується з дослідженням Murphy B. та ін. [18], де за допомогою тематичного моделювання було досліджено, як ШІ трансформує концепцію бухгалтерського обліку. Огляд сучасних цифрових методів наведено у роботі Odeyemi O. та ін. [19, с. 202–214], де підкреслено важливість адаптації традиційних методів до цифрової епохи.

Таким чином, сучасні дослідження підтверджують зростаючу роль штучного інтелекту як інструменту виявлення фінансового шахрайства та трансформації аудиторських практик.

Виділення невирішених раніше частин загальної проблеми. Попри значну кількість досліджень, присвячених впровадженню ШІ в аудит [1–9, 11, 13–17], а також зростаючому масиву праць, що аналізують ефективність технологій виявлення помилок та шахрайства [4–7, 10, 12, 15], недостатньо вивченими залишаються аспекти цілісної інтеграції таких рішень у бізнес-процеси підприємства з урахуванням економічної доцільності, етичних ризиків і практичної готовності аудиторських служб до їх використання. Більшість наукових публікацій фокусується на технічних характеристиках моделей або на описі переваг впровадження, уникаючи критичного аналізу бар'єрів, пов'язаних із нормативною невизначеністю, обмеженістю емпіричних даних та складністю адаптації ШІ до контексту професійної відповідальності.

Водночас саме ці невирішені питання є визначальними для ефективного запобігання шахрайству в умовах цифрової трансформації. Необхідність системного дослідження комплексного впливу ШІ -технологій на аудит обумовлена зростанням ризиків алгоритмічної упередженості, нерівномірним рівнем цифрової компетентності фахівців та відсутністю чітких стандартів, що регулюють використання інтелектуальних систем у перевірках фінансової

звітності. У межах цієї роботи доцільним є проаналізувати, яким чином впровадження ШІ змінює логіку аудиторських процедур у контексті боротьби з шахрайством, і запропонувати практичні підходи до подолання викликів, пов'язаних із професійною, етичною та організаційною адаптацією технологій.

Формулювання цілей статті (постановка завдання). Метою дослідження є обґрунтування інноваційних підходів до запобігання шахрайству в аудиті шляхом інтеграції інструментів ШІ у бізнес-процеси підприємства, з урахуванням економічної доцільності, аналітичних можливостей та ризиків цифрової трансформації.

Для досягнення поставленої мети у роботі передбачено вирішення таких завдань: охарактеризувати механізми виявлення шахрайства на основі алгоритмів ШІ, зокрема машинного навчання, інтелектуального аналізу даних, нейромережевого моделювання та систем виявлення аномалій; обґрунтувати економічну доцільність впровадження технологій ШІ у внутрішні бізнес-процеси підприємств, насамперед у сфері аудиту та контролю; проаналізувати ризики та обмеження цифрових рішень в аудиті, пов'язані з недостатньою регламентацією, професійною неготовністю, а також з потенційною етичною вразливістю ШІ-систем.

Виклад основного матеріалу дослідження. Сучасні фінансово-економічні системи функціонують у середовищі високої цифровізації, що супроводжується зростанням обсягів даних, швидкості транзакцій та складності фінансових взаємодій. У таких умовах шахрайство набуває дедалі більш прихованих і адаптивних форм, що ускладнює його виявлення традиційними контрольними та аудиторськими інструментами. Це зумовлює підвищений інтерес до використання алгоритмів ШІ, зокрема машинного навчання, інтелектуального аналізу даних, нейромережевого моделювання та систем виявлення аномалій.

Ключовою особливістю машинного навчання у сфері виявлення шахрайства є його здатність працювати з великими масивами структурованих і

неструктурованих даних та виявляти закономірності, які не завжди є очевидними для людини або класичних статистичних методів. Алгоритми навчання дозволяють формувати моделі класифікації на основі історичних даних, де транзакції вже позначені як шахрайські або легітимні. Такий підхід забезпечує високу точність за умови якісної навчальної вибірки, проте водночас залежить від повноти та достовірності попередніх рішень. Проблема дисбалансу класів, характерна для помилкових даних, суттєво впливає на результати навчання, оскільки частка шахрайських операцій зазвичай є незначною порівняно із загальним масивом транзакцій.

Попри значний потенціал, машинне навчання у виявленні шахрайства має певні функціональні обмеження, зокрема пов'язані з його залежністю від якісно структурованих і розмічених навчальних вибірок. Алгоритми навчання ефективно виявляють закономірності, що вже були зафіксовані в історичних даних, однак демонструють обмежену гнучкість щодо виявлення нових, нетипових шахрайських сценаріїв. До того ж такі моделі схильні до перенавчання на повторюваних шаблонах і часто втрачають чутливість до рідкісних або поодиноких випадків шахрайства. У цьому контексті інтелектуальний аналіз даних розширює рамки виявлення, дозволяючи досліджувати не лише класифіковані приклади, а й взаємозв'язки між ознаками, тенденції змін у поведінці користувачів, асоціативні структури, які можуть слугувати непрямими індикаторами помилок. На відміну від машинного навчання, яке орієнтоване на прогнозування, інтелектуальний аналіз часто використовується як інструмент гіпотезоутворення, що дозволяє поєднувати автоматизовану обробку з експертною інтерпретацією.

Інтелектуальний аналіз даних у контексті виявлення шахрайства розширює можливості машинного навчання за рахунок поєднання статистичних методів, алгоритмів кластеризації та пошуку асоціативних правил. Його перевага полягає у можливості комплексного дослідження даних без жорсткої прив'язки до наперед визначених класів. Це дозволяє формувати профілі типових

користувачів, операцій або поведінкових моделей та зіставляти з ними поточні транзакції. Разом з тим інтелектуальний аналіз даних часто потребує значної експертної участі на етапі інтерпретації результатів, оскільки виявлені закономірності не завжди свідчать про шахрайство.

Хоча інтелектуальний аналіз даних демонструє переваги у дослідженні латентних структур і кластерів, він також має свої обмеження, пов'язані з низькою ефективністю у високодинамічних або надзвичайно складних середовищах, де взаємозв'язки між змінними не мають чіткої логічної структури. У таких випадках на перший план виходить нейромережеве моделювання, зокрема застосування глибоких нейронних мереж, здатних автоматично виявляти складні, нелінійні залежності в багатовимірних даних. Нейромережі ефективно справляються з задачами, які вимагають багаторівневої обробки сигналів або врахування послідовності подій – наприклад, аналіз серій транзакцій або моделювання поведінки користувача протягом часу. Водночас, на відміну від більш прозорих підходів інтелектуального аналізу, нейромережеві моделі часто функціонують як непрозорі структури, що обмежує можливості їх інтерпретації й пояснення. Це створює виклик у контексті правового регулювання та довіри до рішень систем виявлення шахрайства.

Нейромережеве моделювання посідає особливе місце серед інструментів виявлення шахрайства завдяки здатності обробляти складні нелінійні залежності між численними ознаками. Глибокі нейронні мережі демонструють високу ефективність у випадках, коли взаємозв'язки між параметрами є багаторівневими та динамічними. Особливо перспективним є використання рекурентних нейронних мереж для аналізу часових рядів, оскільки вони дозволяють враховувати послідовність операцій та виявляти нетипові сценарії поведінки. Водночас нейромережеві моделі характеризуються обмеженою інтерпретованістю, що створює труднощі у практичному застосуванні, особливо в умовах регуляторних вимог до прозорості прийняття рішень.

Незважаючи на високу обчислювальну потужність і здатність до самонавчання, нейронні мережі залишаються переважно реактивними інструментами, орієнтованими на виявлення вже наявних, хоча й складних шаблонів. Вони демонструють обмежену здатність до індуктивного виявлення нових або унікальних поведінкових аномалій, які ще не були представлені в даних. Саме тут виявлення аномалій набуває особливого значення, оскільки дозволяє працювати з відхиленнями від усталених моделей без потреби у попередньому маркуванні чи навіть у знанні структури потенційних загроз. На відміну від нейромереж, системи виявлення аномалій функціонують не як «відтворювачі складних патернів», а як «сенсори нетиповості», що робить їх незамінними у боротьбі з новими, раніше не ідентифікованими проявами шахрайства. Водночас така відкритість до аномального часто спричиняє зниження специфічності й потребує подальшої фільтрації або верифікації результатів іншими аналітичними інструментами. Системи виявлення аномалій орієнтовані на ідентифікацію відхилень від усталених шаблонів поведінки без обов'язкового використання попередньо розмічених даних. Такий підхід є доцільним у ситуаціях, коли шахрайські схеми є новими або швидко змінюються. Аномалії розглядаються як потенційні індикатори ризику, проте їх інтерпретація потребує обережності, оскільки не кожне відхилення від норми є проявом шахрайства. Надмірна чутливість систем виявлення аномалій може призводити до значної кількості хибнопозитивних результатів, що знижує ефективність їх практичного використання.

Важливою характеристикою сучасних алгоритмічних рішень є їх адаптивність до змін у середовищі здійснення операцій. Моделі машинного навчання та нейромережі можуть оновлюватися на основі нових даних, що дозволяє їм реагувати на еволюцію шахрайських схем. Разом з тим постає питання контролю цього процесу, оскільки надмірна автоматизація адаптації може створювати ризики зміщення критеріїв нормальної поведінки.

Таким чином, механізми виявлення шахрайства на основі алгоритмів ШІ характеризуються високим аналітичним потенціалом, проте потребують зваженого поєднання різних підходів. Машинне навчання, інтелектуальний аналіз даних, нейромережеве моделювання та системи виявлення аномалій доповнюють одне одного, формуючи багаторівневу систему контролю, у якій технічна ефективність має поєднуватися з інтерпретованістю, надійністю та відповідністю нормативним вимогам.

Зважаючи на багатоваріантність підходів до виявлення шахрайства, актуальним є їх порівняльний аналіз. Кожен з вище розглянутих методів має власні функціональні характеристики, переваги й обмеження, які визначають доцільність їх застосування в конкретному операційному або дослідницькому середовищі. У таблиці 1 нижче узагальнено основні порівняльні ознаки, що дозволяють виявити унікальні риси кожного з підходів.

Таблиця 1

Характеристики підходів до виявлення шахрайства

Критерій	**Машинне навчання**	**Інтелектуальний аналіз даних**	**Нейромережеве моделювання**	**Системи виявлення аномалій**
Тип даних	Переважно розмічені	Розмічені та нерозмічені	Великі обсяги складних, багатовимірних даних	Нерозмічені, з ознаками нестандартності
Призначення	Класифікація, прогнозування	Виявлення структур, закономірностей, кластеризація	Виявлення складних шаблонів, послідовностей	Детекція відхилень від норми
Гнучкість до нових типів помилок	Обмежена (залежить від навчальних даних)	Вища завдяки аналізу прихованих зв’язків	Середня, залежить від архітектури та глибини мережі	Висока здатність виявляти нові аномальні дії
Інтерпрето-ваність результатів	Середня	Висока (особливо на рівні візуалізації зв’язків)	Низька («чорна скринька»)	Залежить від алгоритму; зазвичай низька
Потреба в експертному супроводі	Помірна	Висока (інтерпретація результатів часто ручна)	Низька після налаштування, але складна в обґрунтуванні	Висока (необхідна валідація аномалій)

ISSN 3041-2129

Критерій	Машинне навчання	Інтелектуальний аналіз даних	Нейромережеве моделювання	Системи виявлення аномалій
Переваги	Висока точність за наявності якісних даних	Широкі можливості виявлення прихованих патернів	Потужність у моделюванні складних взаємозв'язків	Виявлення нових або невідомих типів шахрайства
Недоліки	Схильність до перенавчання, потреба в якісному маркуванні	Складність масштабування, залежність від експерта	Обмежена пояснюваність, висока обчислювальна складність	Велика кількість хибнопозитивних результатів

Джерело: власна розробка автора

Розгляд механізмів виявлення шахрайства із застосуванням технологій ШІ дозволяє глибше зрозуміти функціональні можливості та аналітичний потенціал таких підходів у сфері фінансового контролю. Водночас окремий аналіз інструментів є лише частиною ширшої проблематики – доцільності інтеграції ШІ у внутрішні бізнес-процеси підприємств. Саме тому логічним продовженням дослідження постає оцінка економічної ефективності впровадження таких технологій, зокрема у сфері аудиту та внутрішнього контролю, де використання ШІ здатне не лише забезпечити більш точне виявлення порушень, а й сприяти підвищенню загальної результативності управлінських рішень. Особливу увагу при цьому привертають функціональні сфери, пов'язані з аудитом і внутрішнім контролем, оскільки саме тут традиційно концентруються значні обсяги рутинних, формалізованих завдань, які потребують високої точності та системності.

З економічної точки зору, впровадження ШІ в аудит та контроль забезпечує низку стратегічних переваг, що дозволяють розглядати такі інвестиції як доцільні та обґрунтовані. Насамперед ідеться про скорочення витрат часу та трудових ресурсів. Алгоритми машинного навчання здатні автоматично обробляти великі обсяги фінансових, транзакційних та операційних даних, виявляючи відхилення, аномалії та потенційні порушення без участі людини або з мінімальним

залученням аудиторів. Це дає змогу значно знизити витрати на ручну перевірку первинних документів, формування звітності та попередній аналіз ризиків.

Крім прямої економії, ШІ забезпечує підвищення якості прийняття управлінських рішень. Високоточна аналітика, яка ґрунтується на об'єктивних даних, дозволяє ідентифікувати не лише факти порушень, а й системні слабкості внутрішнього контролю, що відкриває можливості для вдосконалення процесів. Раннє виявлення фінансових ризиків сприяє запобіганню потенційним збиткам, що в довгостроковій перспективі формує стійкі економічні вигоди, які виходять за межі короткотермінового ефекту.

Ще одним важливим аспектом є масштабованість і адаптивність ШІ-рішень. Після первинного налаштування системи можуть працювати в режимі постійного самооновлення на основі нових даних, що дозволяє підтримувати контроль навіть у разі змін у внутрішньому середовищі підприємства або в зовнішньому регуляторному полі. Це забезпечує не лише гнучкість, а й економію на майбутніх витратах з обслуговування та оновлення традиційних систем контролю.

Варто також враховувати опосередковані економічні ефекти, які формуються внаслідок підвищення довіри до внутрішніх процедур контролю з боку інвесторів, партнерів та регуляторів. Наявність сучасної ШІ-системи моніторингу та аудиту може сприйматися як свідчення належного корпоративного управління, що, у свою чергу, позитивно впливає на ринкову вартість компанії, її репутацію та доступ до капіталу.

Таким чином, економічна доцільність впровадження технологій ШІ у внутрішні бізнес-процеси, особливо в сегменті аудиту та контролю, обґрунтовується як прямими вигодами (оптимізація витрат, підвищення точності та швидкості), так і непрямими ефектами (зміцнення довіри, підвищення конкурентоспроможності, зниження ризиків) (рис. 1). Усе це формує підґрунтя для стратегічного переосмислення ролі цифрових технологій у системі

корпоративного контролю та підвищення загальної ефективності управління підприємством.

ВИТРАТИ ТА ВИГОДИ ВІД ВПРОВАДЖЕННЯ ШІ В АВТОМАТИЗАЦІЮ БІЗНЕС-ПРОЦЕСІВ ПІДПРИЄМСТВА З МЕТОЮ ЗАПОБІГАННЯ ФІНАНСОВОМУ ШАХРАЙСТВУ

ВИТРАТИ

Категорія витрат	Опис
Інвестиції у технології	Закупівля програмного забезпечення ШІ, хмарних платформ, сенсорів, серверного обладнання
Розробка та адаптація	Витрати на створення або кастомізацію моделей під специфіку підприємства
Навчання персоналу	Курси, тренінги та сертифікації для бухгалтерів, аудиторів, IT-фахівців
Підтримка та обслуговування	Регулярні оновлення, технічна підтримка, інфраструктурні витрати
Кібербезпека	Забезпечення захисту даних, резервного копіювання, безпеки доступу
Юридичні й етичні ризики	Витрати на правову експертизу, аудит відповідності GDPR/ISO/нац. стандартам
Опір змінам в організації	Непродуктивність у перехідний період, конфлікти через автоматизацію

ВИГОДИ

Категорія вигод	Опис
Зниження рівня шахрайства	Виявлення підозрілих транзакцій, аномалій, схем обману в реальному часі
Підвищення точності аудиту	Мінімізація людських помилок, автоматизовані перевірки 24/7
Економія ресурсів	Зменшення витрат на ручну обробку даних, перевірки, інтерв'ювання
Оперативність прийняття рішень	Швидка аналітика, попередження ризиків ще до настання збитків
Покращення внутрішнього контролю	Постійний моніторинг дій користувачів, доступу, фінансових потоків
Підвищення довіри до компанії	Прозорість процесів для інвесторів, аудиторів, регуляторів
Масштабованість	Можливість легко інтегрувати ШІ в інші процеси (логістика, закупівлі, HR)
Аналітична глибина	ШІ виявляє складні схеми шахрайства, недоступні для класичного аналізу

Рис. 1. Основні витрати та вигоди від впровадження ШІ в автоматизацію бізнес-процесів підприємства з метою запобігання фінансовому шахрайству

Джерело: складено автором на основі аналізу [1,3-7,14-18]

Обґрунтування економічної доцільності інтеграції ШІ в аудит свідчить про наявність вагомих підстав для його впровадження у бізнес-процеси підприємств. Однак поряд із потенційними вигодами, такими як зниження витрат, підвищення точності перевірок та своєчасне виявлення шахрайства, слід враховувати і низку ризиків та обмежень. Їх ігнорування може нівелювати очікуваний ефект та поставити під загрозу цілісність аудиторської функції. У зв’язку з цим доцільним

є критичний аналіз факторів, які ускладнюють ефективне впровадження цифрових рішень в аудит. Одним із ключових стримувальних чинників є недостатня регламентація використання ШІ в аудиті. У більшості юрисдикцій відсутні чіткі нормативні акти або стандарти, які б окреслювали межі відповідальності при застосуванні алгоритмів для виявлення шахрайства, а також вимоги до якості даних, що використовуються для навчання моделей. Це створює правову невизначеність, особливо в аспектах оцінки надійності висновків, сформованих автоматизованими системами, і може викликати сумніви щодо юридичної сили таких результатів.

Не менш суттєвим є ризик професійної неготовності аудиторів до роботи з інструментами ШІ. Дефіцит цифрових компетентностей, складність інтерпретації результатів, сформованих алгоритмами, та обмежене розуміння принципів роботи моделей можуть призвести до хибних висновків або надмірної довіри до систем, що функціонують як «чорні скриньки». Це, своєю чергою, знижує якість аудиту та підвищує ймовірність некоректної оцінки фінансових ризиків.

Особливу увагу слід приділити етичній вразливості ШІ-систем, що проявляється у потенційному алгоритмічному упередженні, порушенні принципу незалежності або недотриманні конфіденційності. Алгоритми, які використовують історичні дані, можуть відтворювати наявні упередження, закладені в системі, що створює ризик дискримінаційного підходу або неправомірного виявлення шахрайства. Також виникають етичні дилеми, пов’язані з відсутністю людського контролю над остаточними рішеннями, що суперечить традиційним цінностям аудиторської професії.

Таким чином, ефективне впровадження ШІ в аудит вимагає не лише технічної готовності, а й створення нормативного, етичного та освітнього підґрунтя, яке забезпечить належну інтерпретацію, відповідальність і безпечне функціонування цифрових рішень у межах професійної практики.

 ISSN 3041-2129

З урахуванням виявлених ризиків і обмежень, стає очевидним, що цифровізація аудиту не може розглядатися лише як технічне оновлення. Це – стратегічний процес, що потребує комплексного підходу до регулювання, професійної підготовки та етичного осмислення ролі ШІ в ухваленні рішень. Лише за умови гармонійного поєднання інноваційних інструментів із цінностями професії можливе досягнення справжньої якості й довіри в сучасному аудиті.

Висновки. Інтеграція ШІ у бізнес-процеси підприємства трансформує підходи до аудиту, перетворюючи його з постфактум-контролю на динамічну систему превентивного виявлення ризиків. Сучасні технології ШІ, зокрема алгоритми машинного навчання та системи розпізнавання аномалій, створюють нові можливості для боротьби з фінансовим шахрайством. Разом із тим, впровадження таких рішень супроводжується низкою викликів – від нормативної невизначеності до професійної неготовності до роботи з новими інструментами. Недостатній рівень цифрової компетентності або некритичне прийняття результатів роботи ШІ можуть призвести до зниження об’єктивності аудиторських висновків і нових форм викривлення інформації.

Застосування ШІ в аудиті вимагає не лише технічної інтеграції, а й переосмислення ролі аудитора як гаранта достовірності даних у цифровому середовищі. Це підкреслює необхідність формування нового професійного мислення, що базується на поєднанні аналітичних навичок, етичної стійкості та здатності до роботи в умовах швидкоплинної цифрової трансформації. Такий підхід сприяє не лише підвищенню якості аудиту, а й зміцненню довіри до фінансової інформації як основи ефективного управління.

Список використаних джерел

1. Ramos S., Perez-Lopez J. A., Abreu R. Bibliometric analysis of artificial intelligence trends in auditing and fraud detection. *Corporate Governance and*

Organizational Behavior Review. 2024. Vol. 8, № 2. P. 330–342. DOI: https://doi.org/10.22495/cgobrv8i2sip8

2. Yaseen H., Al-Amarneh A. Adoption of artificial intelligence-driven fraud detection in banking: the role of trust, transparency, and fairness perception in financial institutions in the United Arab Emirates and Qatar. *Journal of Risk and Financial Management*. 2025. Vol. 18, № 4. P. 217. DOI: https://doi.org/10.3390/jrfm18040217

3. Bou Reslan F., Jabbour Al Maalouf N. Assessing the transformative impact of AI adoption on efficiency, fraud detection, and skill dynamics in accounting practices. *Journal of Risk and Financial Management*. 2024. Vol. 17, № 12. P. 577. DOI: https://doi.org/10.3390/jrfm17120577

4. Nguyen T. C., Le H. H., Pham N. D. Predicting financial reports fraud by machine learning. *Cogent Business & Management*. 2025. Vol. 12, № 1. P. 1–18. DOI: https://doi.org/10.1080/23311975.2025.2510556

5. Hernandez Aros L., Bustamante Molano L. X., Gutierrez-Portela F. [et al.]. Financial fraud detection through the application of machine learning techniques: a literature review. *Humanities and Social Sciences Communications*. 2024. Vol. 11, № 1. P. 1130. DOI: https://doi.org/10.1057/s41599-024-03606-0

6. Compagnino A. A., Pisani G., Ragozzine B., Sciacca E., Ambrosino F., Bellina F. An introduction to machine learning methods for fraud detection. *Applied Sciences*. 2025. Vol. 15, № 21. P. 11787. DOI: https://doi.org/10.3390/app152111787

7. Tümmler M., Quick R. How to detect fraud in an audit: a systematic review of experimental literature. *Management Review Quarterly*. 2025. Vol. 75, № 2. P. 115–132. DOI: https://doi.org/10.1007/s11301-024-00480-7

8. Kokina J., Blanchette S., Davenport T. H., Pachamanova D. Challenges and opportunities for artificial intelligence in auditing: evidence from the field. *International Journal of Accounting Information Systems*. 2025. Vol. 56. P. 100734. DOI: https://doi.org/10.1016/j.accinf.2025.100734

9. Sanz Martín L., Parra Domínguez J., Corchado J. M., Zafra-Gómez E., Castillo-Ramos V., Zafra-Gómez J. L. Recent evolution and growth of AI and

advanced technologies in accounting and finance: systematic review and bibliometric analysis. *Spanish Journal of Finance and Accounting / Revista Española de Financiación y Contabilidad*. 2025. Vol. 54, № 1. P. 1–42. DOI: https://doi.org/10.1080/02102412.2025.2582120

10. Reyes Lazo M. D., Córdova Espinoza L. F., De La Cruz Vargas M., Soto Córdova J. Financial auditing as an effective tool for fraud detection: a systematic review. *Journal of Risk and Financial Management*. 2025. Vol. 18, № 9. P. 523. DOI: https://doi.org/10.3390/jrfm18090523

11. Qatawneh A. M. The role of artificial intelligence in auditing and fraud detection in accounting information systems: moderating role of natural language processing. *International Journal of Organizational Analysis*. 2025. Vol. 33, № 6. P. 1391–1409. DOI: https://doi.org/10.1108/IJOA-03-2024-4389

12. Bhattacharya I., Mickovic A. Accounting fraud detection using contextual language learning. *International Journal of Accounting Information Systems*. 2024. Vol. 53. P. 100682. DOI: https://doi.org/10.1016/j.accinf.2024.100682

13. Georgiou I., Sapuric S., Lois P., Thrassou A. Blockchain for accounting and auditing – accounting and auditing for cryptocurrencies: a systematic literature review and future research directions. *Journal of Risk and Financial Management*. 2024. Vol. 17, № 7. P. 276. DOI: https://doi.org/10.3390/jrfm17070276

14. Hafez I. Y., Hafez A. Y., Saleh A., Abd El-Mageed A. A., Abohany A. A. A systematic review of AI-enhanced techniques in credit card fraud detection. *Journal of Big Data*. 2025. Vol. 12, № 1. P. 6. DOI: https://doi.org/10.1186/s40537-024-01048-8

15. Sodnomdavaa T., Lkhagvadorj G. Financial statement fraud detection through an integrated machine learning and explainable AI framework. *Journal of Risk and Financial Management*. 2026. Vol. 19. P. 13. DOI: https://doi.org/10.3390/jrfm19010013

16. Leocádio D., Malheiro L., Reis J. Artificial intelligence in auditing: a conceptual framework for auditing practices. *Administrative Sciences*. 2024. Vol. 14, № 10. P. 238. DOI: https://doi.org/10.3390/admsci14100238

17. Murikah W., Nthenge J. K., Musyoka F. M. Bias and ethics of AI systems applied in auditing: a systematic review. *Scientific African*. 2024. Vol. 25. P. e02281. DOI: https://doi.org/10.1016/j.sciaf.2024.e02281

18. Murphy B., Feeney O., Rosati P., Lynn T. Exploring accounting and AI using topic modelling. *International Journal of Accounting Information Systems*. 2024. Vol. 55. P. 100709. DOI: https://doi.org/10.1016/j.accinf.2024.100709

19. Odeyemi O., Ibeh C. V., Mhlongo N. Z., Asuzu O. F., Olatoye F. O., Awonuga K. F. Forensic accounting and fraud detection: a review of techniques in the digital age. *Finance & Accounting Research Journal*. 2024. Vol. 6, № 2. P. 202–214. DOI: https://doi.org/10.51594/farj.v6i2.788