DOI: https://doi.org/10.32782/2524-0072/2026-86-2

УДК 657.6

ПЕРСПЕКТИВИ, РИЗИКИ ТА МОДЕЛЬ ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ І ПРОЦЕСНОЇ АВТОМАТИЗАЦІЇ ВНУТРІШНЬОГО АУДИТУ В МІНІСТЕРСТВІ ОБОРОНИ УКРАЇНИ

PROSPECTS, RISKS AND IMPLEMENTATION MODEL OF ARTIFICIAL INTELLIGENCE AND PROCESS AUTOMATION IN THE INTERNAL AUDIT OF THE MINISTRY OF DEFENCE OF UKRAINE

Андрієнко Оксана Олександрівна
старший викладач кафедри фінансового забезпечення військ,
Військовий інститут Київського національного університету
імені Тараса Шевченка
ORCID: https://orcid.org/0000-0002-1181-9586

Мельников Олександр Васильович
викладач кафедри фінансового забезпечення військ,
Військовий інститут Київського національного університету
імені Тараса Шевченка
ORCID: https://orcid.org/0009-0003-8789-7315

Сорока Іван Олександрович
курсант,
Військовий інститут Київського національного університету
імені Тараса Шевченка
ORCID: https://orcid.org/0009-0003-1500-3669

Andriienko Oksana, Melnykov Oleksandr, Soroka Ivan
Military Institute of Taras Shevchenko National University of Kyiv

У статті досліджено перспективи впровадження штучного інтелекту та процесної автоматизації у внутрішньому аудиті Міністерства оборони України з урахуванням вимог законодавства й режимів безпеки інформації. Показано, що аналітика даних і автоматизовані контрольні процедури здатні підсилити ризик-орієнтоване планування, розширити охоплення транзакцій та забезпечити оперативніше виявлення аномалій, а також підтримати моніторинг виконання рекомендацій. Визначено ключові ризики застосування та окреслено мінімальні контрольні вимоги до інструментів на базі штучного інтелекту: контроль доступу, протоколювання операцій, тестування якості й збереження відповідальності аудитора за професійне судження. Практична цінність – модель поетапного впровадження та перелік пріоритетних кейсів для оборонної сфери.

Ключові слова: внутрішній аудит; державний сектор; оборонні ресурси; штучний інтелект; автоматизація; безперервний моніторинг; ризик-орієнтований підхід; управління даними; кібербезпека.

This article examines how artificial intelligence (AI) and process automation can be integrated into the internal audit function of the Ministry of Defence of Ukraine in a way that strengthens assurance over the use of public resources while respecting security, confidentiality and legal constraints. The topic is timely because defence management operates under high transaction volumes, complex supply chains, accelerated decision cycles and increased exposure to fraud, error and cyber threats, while audit units are expected to deliver risk-based assurance and monitor the implementation of recommendations more continuously. The study applies doctrinal analysis of the public-sector internal control and internal audit framework, a comparative review of international approaches to AI risk management and AI auditing, and a design-science method to develop an implementable operating model. The results include: (1) a typology of priority AI-enabled audit use cases (data-driven audit universe updates, dynamic

risk scoring for annual planning, automated tests of controls, anomaly detection in transactional populations, and workflow automation for follow-up); (2) a dual concept of “AI for audit” and “auditing AI” that clarifies when AI outputs may serve only as risk signals, when they may support substantive testing, and which evidence requirements remain strictly human-validated; (3) a baseline of governance and controls for defence organisations covering data classification, access control, audit trails, prompt and output logging, model validation and drift monitoring, supplier and third-party oversight, incident response and cybersecurity safeguards; and (4) a minimal competency profile for internal auditors to work with data, measure model reliability and maintain professional scepticism. Practical value is provided through a phased roadmap with measurable milestones. It starts with data inventory, data quality rules and secure integration with accounting and logistics systems; then introduces dashboards and continuous monitoring indicators; and only after that expands to ML and generative AI components deployed in protected environments. The roadmap links each phase to expected outputs (risk indicators, tested controls, documented assumptions, and improved recommendation closure rates), enabling leadership to evaluate benefits without undermining auditor independence or accountability.

Keywords: internal audit; public sector; defence governance; artificial intelligence; process automation; data analytics; continuous monitoring; AI risk management; cybersecurity.

Постановка проблеми. Нормативна логіка державного внутрішнього фінансового контролю в Україні передбачає, що розпорядники бюджетних коштів зобов'язані організувати внутрішній контроль і внутрішній аудит та забезпечити їх функціонування у підпорядкованих суб'єктах. Законодавство акцентує на незалежності та об'єктивності внутрішнього аудиту, визначає дві «лінії продукту» (надання впевненості та консультації), а також закріплює ідею системного оцінювання й удосконалення управління, внутрішнього контролю та ризик-менеджменту [1, ст. 26; 2; 3, с. 2–3].

Для Міністерства оборони України практична значущість цих норм суттєво посилюється специфікою оборонного управління: високою інтенсивністю операцій, критичністю строків прийняття рішень, чутливістю даних, поєднанням бюджетних і матеріальних потоків, необхідністю підтримувати довіру суспільства й партнерів до прозорості використання ресурсів. Відповідно, внутрішній аудит у системі Міністерства оборони орієнтований на ризик-орієнтований підхід і охоплює оцінювання ефективності внутрішнього контролю, управлінських рішень, запобігання незаконному використанню ресурсів, а також оцінювання надійності інформаційних систем [7, с. 1–3].

За цих умов впровадження штучного інтелекту та автоматизації у внутрішньому аудиті стає практичним інструментом збільшення охоплення контролем, підвищення швидкості виявлення відхилень і якості рекомендацій без втрати незалежності, доказовості й безпеки обробки даних. Проблема полягає в тому, що національні стандарти та методичні вказівки з внутрішнього аудиту для державного сектору досі орієнтовані на класичні процедури з обмеженою автоматизацією. Натомість сучасні інструменти – аналітика великих масивів даних, безперервний моніторинг, моделі машинного навчання – потребують науково обґрунтованих підходів до документування припущень, налаштувань автоматизованих моделей, управління ШІ-ризиками та забезпечення відповідності інструментів ШІ режимам секретності, захисту персональних даних і кібербезпеки [5, с. 8–12; 8, с. 4–5].

Аналіз останніх досліджень і публікацій. Сучасний дискурс щодо ШІ в аудиті розвивається у двох взаємопов’язаних напрямах. Перший – «ШІ для аудиту», тобто використання аналітики даних, машинного навчання, роботизованої автоматизації процесів і генеративних інструментів для покращення планування, тестування систем контролю, виявлення аномалій, комунікації та супроводу рекомендацій. Цей напрям у міжнародній літературі часто прив’язують до концепції безперервного аудиту або безперервного моніторингу, коли автоматизовані процедури та аналітика дозволяють переходити від ретроспективних вибіркових перевірок до частішого (інколи майже у режимі реального часу) контролю показників ризику, про що йдеться у роботах Алассулі А. [16, с. 7–8; 18, с. 123–125].

Другий – «аудит ШІ», тобто перевірка належності управління ШІ-системами: їхньої цілісності, прозорості, безпеки, відповідності політикам і законам, якості даних, контролю доступу, стійкості до збоїв, атак та коректності моніторингу. Професійні організації прямо визнають, що через складність і швидку еволюцію ШІ внутрішній аудит часто може надавати лише обмежену впевненість, а отже потрібне чітке визначення меж відповідальності та ролі аудитора, а також системна інтеграція з підходами врядування [14, с. 12–13].

Управлінські та регуляторні рамки для безпечного застосування ШІ також інтенсивно розвиваються. Наприклад, модель управління

ризиками ШІ пропонує концепцію «надійного ШІ» з характеристиками на кшталт валідності та надійності, безпеки, кіберстійкості, підзвітності, прозорості, пояснюваності, захисту приватності та керування упередженнями; при цьому ризик-менеджмент ШІ розглядається як безперервний цикл упродовж життєвого циклу системи [13, p. 2–3, 20–21].

В українському академічному полі наявні дослідження, зокрема Брайка В., що розкривають методологічну інтеграцію великих мовних моделей і класичних статистичних підходів для аудиторських процедур та водночас наголошують, що ШІ є інструментом підтримки, а не заміни професійного судження аудитора [17].

Водночас, Шпиталь О. у своїх наукових працях зазначає, що з урахуванням особливостей системи Міністерства оборони України вказується на потребу модернізації внутрішнього аудиту, зокрема через невідповідність традиційних підходів динамічному, ризик-орієнтованому та технологічному середовищу оборонного відомства під час війни, а також через потребу посилення методологічної бази та спроможності функції [10, с. 265–266].

Невирішена частина загальної проблеми полягає у відсутності цілісної прикладної моделі, яка одночасно: а) узгоджує використання ШІ та автоматизації з національними стандартами внутрішнього аудиту й внутрішнього контролю; б) враховує формальні вимоги до незалежності, доступу до даних, конфіденційності та документування; в) відокремлює допустимі «сигнали ризику» від доказів; г) пропонує мінімальний набір контролів для ШІ-інструментів у середовищі оборонного управління (де питання секретності, кіберзахисту та надійності мають першочерговий характер).

Формулювання цілей статті (постановка завдання). Метою статті є обґрунтування та розроблення моделі впровадження штучного інтелекту і процесної автоматизації у внутрішньому аудиті в системі Міністерства оборони України, яка забезпечує підвищення ефективності й оперативності аудиторської функції та зберігає відповідність вимогам незалежності, доказовості, захисту інформації та управління ризиками.

Для досягнення мети поставлено такі завдання: узагальнити нормативні вимоги до внутрішнього аудиту й внутрішнього контролю в державному секторі та в системі Міністерства оборони України; систематизувати сучасні підходи «ШІ для аудиту» та «аудит ШІ»; визначити ключові ризики застосування ШІ та автоматизації в оборонному контексті; сформувати базовий пакет контролів і організаційних рішень, що мінімізують ці ризики; запропонувати поетапну дорожню карту впровадження з пріоритетними кейсами та критеріями готовності.

Виклад основного матеріалу дослідження Нормативне регламентування внутрішнього аудиту в державному секторі формує ієрархія наступних нормативно-правових актів: Бюджетний кодекс визначає обов’язок керівника розпорядника бюджетних коштів організувати внутрішній контроль і внутрішній аудит, а також дає визначення внутрішнього аудиту як незалежної, об’єктивної діяльності запевнювального та консультаційного характеру. Порядок, затверджений Постановою КМУ № 1001, деталізує організацію внутрішнього аудиту та утворення підрозділів; Накази Міністерства фінансів України визначають організаційно-методологічні засади, у тому числі стандарти й кодекс етики.

Наказ Міністерства фінансів України щодо стандартів внутрішнього аудиту закріплює, що сфера застосування внутрішнього аудиту охоплює оцінку ефективності функціонування внутрішнього контролю, виконання і досягнення цілей установи, бюджетні програми, адміністративні послуги та використання ІТ, а також підкреслює вимоги до планування, документування, формування висновків і моніторингу рекомендацій. У контексті цифровізації це означає: автоматизація та ШІ можуть бути інтегровані не поза стандартами, а як технологічні засоби реалізації стандартних процедур – за умови, що результати залишаються перевірюваними, відтворюваними й належно задокументованими.

Методологічні вказівки з внутрішнього аудиту в державному секторі України (2019) підкреслюють адаптацію міжнародних професійних стандартів до національного контексту та деталізують цикл внутрішнього аудиту, включаючи формування «простору аудиту», ідентифікацію та оцінку ризиків, вибір пріоритетних об’єктів і відстеження впровадження рекомендацій. У практичному вимірі це створює природну точку входу для аналітики й автоматизації: оновлення простору аудиту та ризик-скоринг можуть базуватися на більш системному використанні даних, а моніторинг рекомендацій – на автоматизованих індикаторах виконання.

У системі Міністерства оборони України функція внутрішнього аудиту інституційно

конкретизується через затверджене положення про профільний підрозділ: внутрішній аудит визначається як незалежна, об'єктивна діяльність із надання впевненості та консультування, що здійснюється на основі системного та послідовного ризик-орієнтованого підходу; окреслено предметну область оцінювання (внутрішній контроль, ефективність планування та виконання бюджетних програм, управління ресурсами, якість адміністративних послуг, надійність і результативність інформаційних систем і технологій) [7, с. 1–3].

З погляду доступу до даних і доказів важливо, що декларативні документи внутрішнього аудиту в Міністерстві оборони України підкреслюють право внутрішніх аудиторів на повний і безперешкодний доступ до документів, інформації та баз даних, необхідних для виконання аудиторських завдань, одночасно наголошуючи на вимогах конфіденційності та правилах роботи з документами обмеженого доступу. Це прямо пов'язує цифровий розвиток аудиту з двома умовами: а) доступ має бути організований так, щоб не підривати режим секретності й захист інформації; б) результати автоматизованих перевірок мають бути простежуваними та зберігати доказову силу [9, с. 3–4].

Порядок організації внутрішнього контролю та управління ризиками в системі Міністерства оборони України у чинній редакції закладає термінологічну й процесну основу для даних, які можуть «живити» аналітику й автоматизований моніторинг: реєстр ризиків і відхилень, профіль ризику/відхилення, визначення ключових і залишкових ризиків, дизайн заходів контролю, щорічні звіти про стан функціонування внутрішнього контролю. Ба більше, документ прямо прив'язує внутрішній контроль до функціонування інформаційних (автоматизованих) та інформаційно-комунікаційних систем і вимагає організації управління інформаційними потоками й електронного документообігу як частини контрольного середовища [6, с. 2–5].

Узгодження цього контрольного контуру з внутрішнім аудитом дозволяє сформулювати перший науково-прикладний результат: ШІ та автоматизація у внутрішньому аудиті Міністерства оборони України мають впроваджуватися як розширення ризик-орієнтованого підходу (через кращі дані й індикатори), а не як окрема цифрова ініціатива. Інакше кажучи, модель впровадження повинна починатися з формалізації даних, що вже передбачені системою внутрішнього контролю (ризики, заходи контролю, показники, відхилення, виконання рекомендацій), і лише потім переходити до складніших ШІ-компонентів.

Другий результат – концептуальне розмежування «ШІ для аудиту» та «аудит ШІ» у внутрішньому аудиті Міністерства оборони України. «ШІ для аудиту» – це застосування інструментів аналітики, RPA та моделей для виконання типових аудиторських робіт: швидшого оновлення простору аудиту, пошуку аномалій, автоматизації рутинних процедур (збирання/звірка даних, контроль порогів, підготовка робочих документів), підтримки моніторингу виконання рекомендацій. Перелік типових «даних-входів» для цих кейсів у системі Міністерства оборони України можна логічно прив'язати до бюджетних транзакцій, закупівельних даних, облікових регістрів, складських/логістичних рухів, кадрових і майнових реєстрів – але за умови дотримання режимів захисту інформації.

Натомість «аудит ШІ» – це перевірка того, як організація планує, управляє, захищає та контролює власні ШІ-рішення (або рішення постачальників) у ключових вимірах: врядування, дані, результативність і моніторинг. Для державних організацій ця логіка прямо випливає з настанов щодо аудиту ІТ-тем: аудиторам рекомендується оцінювати практики врядування, документування джерел даних, визначення метрик, а також планів безперервного моніторингу ШІ-систем і коригувальних дій [16, с. 5–6].

Перевага такого розмежування полягає в методологічній дисципліні щодо доказів. У багатьох випадках ШІ-інструмент (особливо генеративний) видає результат, який за своєю природою є ймовірним і може містити помилки або не відтворюватися буквально при повторному запиті. Тому в моделі пропонується вважати ШІ-виходи переважно «сигналами ризику» та аналітичною підтримкою (supporting analysis), а аудиторськими доказами – лише ті дані, які мають перевірюване походження (ідентифіковане джерело), контроль цілісності, відтворюваний метод отримання та документований ланцюг зберігання/обробки. Такий підхід узгоджується із загальною лінією професійних рамок, де аудитори фокусуються на врядуванні та контролях, а не сліпо покладаються на «чорну скриньку» алгоритму [15, p. 4–5; 14, с. 11–13].

Третій результат – сформульований мінімальний набір контрольних вимог до ШІ та автоматизації, адаптований до оборонного

середовища. Він базується на поєднанні підходів управління ризиками ШІ (життєвий цикл, функції врядування, вимірювання, моніторинг), професійних настанов внутрішнього аудиту щодо ШІ, а також українських вимог до внутрішнього контролю й захисту інформації. Ключовими елементами є:

1) класифікація даних і визначення «червоних зон» (категорії даних, які не можуть передаватися в зовнішні середовища або в неатестовані інструменти);

2) контроль доступу (рольова модель, принцип мінімальних привілеїв, ізоляція середовищ, управління обліковими даними);

3) журналювання та аудит-трейл (логування запитів/відповідей, параметрів моделей, версій, джерел даних, часу виконання, користувачів; зберігання логів як частини робочої документації);

4) оцінювання якості та надійності (метрики точності, помилок, стійкості, контроль дрейфу моделі; періодичні тести);

5) кіберзахист (шифрування, контроль периметра, виявлення вторгнень, тестування на проникнення, правила реагування на інциденти);

6) human-in-the-loop як обов'язковий принцип: жодне суттєве аудиторське судження або висновок не приймається «автоматично» без перевірки аудитором і без підкріплення доказами з надійних джерел [13, p. 2–3, 20–21; 14, с. 10–11].

Окремої уваги потребує питання використання зовнішніх провайдерів, хмарних сервісів та постачальників ШІ. Професійні настанови з аудиту ШІ підкреслюють необхідність оцінювання контролів постачальника, увагу до доступу адміністратора, отримання звітів про контрольне середовище постачальника та включення в угоди права на аудит (right to audit). Для оборонного сектора ці вимоги мають бути посилені у частині ланцюгів постачання та забезпечення, перевірки відповідності режимам секретності й обмеженням щодо даних.

Четвертий результат – запропонована поетапна модель впровадження ШІ та автоматизації у внутрішньому аудиті Міністерства оборони України, побудована за принципом зростання складності та зменшення ризиків на ранніх етапах. Логіка поетапності узгоджується з тим, що сучасні технології (віддалена взаємодія, автоматизація процесів, ШІ та хмарні рішення) створюють не лише переваги, а й нові виклики та ІТ-ризики, що мають бути враховані у внутрішньому аудиті [19].

Перший етап (дані та контрольне середовище) передбачає інвентаризацію джерел даних, опис потоків, визначення відповідальних, установлення правил якості даних, формалізацію доступів і налаштування журналювання. У термінах внутрішнього контролю це відповідає підсиленню «інформації та комунікації» й «моніторингу» як елементів системи внутрішнього контролю та підготовці бази для ризик-орієнтованого управління.

Другий етап (низько ризикова автоматизація) доцільно спрямувати на роботизацію рутинних задач без прийняття рішень моделлю: збір даних з визначених систем, звірки, формування контрольних звітів, автоматизовані сповіщення про перевищення порогів ризику, контроль дедлайнів та виконання рекомендацій. У дослідженнях про RPA зазначено, що роботизована автоматизація здатна зменшувати операційні витрати, знижувати людські помилки, згладжувати процеси та підтримувати безперервний аудит і більш оперативне управління ризиками [18, с. 122–125].

Третій етап (аналітика та безперервний моніторинг) передбачає побудову системи ризик-індикаторів/дашбордів для внутрішнього аудиту: динамічний ризик-скоринг для планування; автоматизовані тести ключових контролів; алгоритмічні пошуки аномалій у транзакціях; «триангуляцію» даних з кількох незалежних джерел (де це можливо) для підвищення надійності висновків. Такий підхід узгоджується з сучасним зміщенням акценту внутрішнього аудиту від суто ретроспективної перевірки до перспективної гарантії (forward-looking assurance) та орієнтації на результат і цінність.

Четвертий етап (ШІ-компоненти під контролем) включає застосування моделей машинного навчання та, в обмеженому режимі, генеративних інструментів у захищених середовищах – переважно для обробки великих масивів неструктурованих даних (текстів), первинного класифікування документів, витягування атрибутів для аудиторських робочих документів, порівняння умов договорів із політиками тощо. Українські методологічні роботи з ШІ в аудиті, попри інший предмет (фінансова звітність приватного сектору), методологічно підтверджують доцільність «гібридної» архітектури: поєднання текстового аналізу (LLM) з класичними числовими/статистичними перевірками та багаторівневою валідацією результатів [4].

П’ятий етап (системний «аудит ШІ») включає розробку програм аудитів для ШІ-систем, що використовуються в управлінні оборонними ресурсами або в підтримці управлінських рішень. Тут доцільно використовувати логіку чотирьох функцій управління ризиками ШІ (врядування, картування контексту, вимірювання, управління/моніторинг) як основу для структури аудиторських критеріїв: чи визначені ролі та відповідальність; чи описані дані та їх походження; чи встановлені метрики якості; чи діє моніторинг і реагування на інциденти; чи забезпечені прозорість та підзвітність.

Ключовим «запобіжником» моделі є забезпечення незалежності внутрішнього аудиту як третьої лінії (third line). Концепція трьох ліній підкреслює, що внутрішній аудит має бути незалежним від управлінських функцій, забезпечуючи об’єктивну впевненість і консультації щодо адекватності врядування, управління ризиками та контролів, і що визначальною характеристикою третьої лінії є незалежність від менеджменту [12, p. 2–6].

Це корелює з вимогами Глобальних стандартів внутрішнього аудиту, які визначають стандарти як основу для підвищення якості функції та включають вимоги щодо компетентностей, методології, технологічних ресурсів і моніторингу виконання рекомендацій [11].

З огляду на правові обмеження щодо інформації, модель передбачає, що кожен кейс застосування ШІ та автоматизації має попередньо проходити правову й безпекову оцінку: чи можуть оброблювані дані містити персональні дані, чи підпадають під режим державної таємниці або службової інформації, чи дотримані вимоги захисту інформації в інформаційно-комунікаційних системах, а також чи забезпечено кіберзахист як елемент внутрішнього контролю.

Управлінський контекст розвитку ШІ в Україні також не є нейтральним: Концепція розвитку штучного інтелекту в Україні визначає ШІ як один із пріоритетних напрямів технологічного розвитку, що логічно підсилює актуальність формування безпечних процедур його застосування у публічному секторі, включаючи контрольні та аудиторські функції [4]

На підставі вище наведеного, прикладний перелік рекомендацій для внутрішнього аудиту в системі Міністерства оборони України у сфері ШІ та автоматизації доцільно формувати як узгоджену тріаду:

1) методологія (внутрішні стандартизовані процедури та шаблони документування для автоматизованих/ШІ-процедур відповідно до національних стандартів внутрішнього аудиту);

2) технологія (захищене середовище даних, інструменти аналітики/автоматизації, керування версіями й логування);

3) врядування (аудиторський комітет як платформа нагляду за межами застосування, ризик-апетитом та незалежністю; а також узгодження з внутрішнім контролем і кібербезпекою). Наявність такої тріади, на відміну від точкових інструментальних «пілотів», зменшує ризик того, що цифрові рішення стануть джерелом нових ризиків або конфлікту інтересів і не дадуть вимірюваної доданої вартості.

Висновки. У статті обґрунтовано, що використання штучного інтелекту та процесної автоматизації у внутрішньому аудиті в системі Міністерства оборони України є практично необхідним для підвищення оперативності та охоплення аудиторських процедур і моніторингу, але має здійснюватися в суворій відповідності до нормативних вимог державного сектору щодо незалежності, доказовості, внутрішнього контролю та режимів захисту інформації.

Запропоновано модель, яка: по-перше, розмежовує «ШІ для аудиту» та «аудит ШІ»; по-друге, визначає ШІ-виходи переважно як сигнали ризику і підтримку аналітики, а не як самостійні аудиторські докази; по-третє, формує мінімальний набір контрольних вимог (класифікація даних, контроль доступу, журналювання, валідація якості, кіберзахист, human-in-the-loop); по-четверте, пропонує поетапну дорожню карту впровадження від даних та низькоризикової автоматизації до аналітики, а далі – до контрольованих ML/LLM-компонентів.

Перспективи подальших досліджень пов’язані з: розробленням конкретних методик аудитів для класів ШІ-рішень (з урахуванням життєвого циклу моделі, постачальників і даних); визначенням метрик результативності цифрових інструментів у внутрішньому аудиті (скорочення часу циклу аудиту, зростання охоплення транзакцій, підвищення частки виконаних рекомендацій); апробацією підходів на пілотних процесах із різним рівнем секретності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Бюджетний кодекс України : Кодекс України від 08.07.2010 № 2456-VI. URL: https://zakon.rada.gov.ua/laws/show/2456-17 (дата звернення: 01.03.2026).

2. Деякі питання здійснення внутрішнього аудиту та утворення підрозділів внутрішнього аудиту : Постанова Кабінету Міністрів України від 28.09.2011 № 1001. URL: https://zakon.rada.gov.ua/laws/show/1001-2011-п (дата звернення: 01.03.2026).

3. Про затвердження Основних засад здійснення внутрішнього контролю розпорядниками бюджетних коштів : Постанова Кабінету Міністрів України від 12.12.2018 № 1062. URL: https://zakon.rada.gov.ua/laws/show/1062-2018-п (дата звернення: 01.03.2026). 12 с.

4. Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р (дата звернення: 03.03.2026).

5. Про затвердження Стандартів внутрішнього аудиту : Наказ Міністерства фінансів України від 04.10.2011 № 1247. URL: https://zakon.rada.gov.ua/laws/show/z1219-11 (дата звернення: 03.03.2026). 20 с.

6. Про затвердження Порядку організації в системі Міністерства оборони України внутрішнього контролю та управління ризиками : Наказ Міністерства оборони України від 02.04.2019 № 145 (у редакції наказу від 22.10.2025 № 709). 55 с.

7. Положення про Департамент внутрішнього аудиту Міністерства оборони України (у редакції наказу від 28.11.2025 № 825). 10 с.

8. Методологічні вказівки з внутрішнього аудиту в державному секторі України. Київ : Міністерство фінансів України, 2019. 162 с.

9. Декларація внутрішнього аудиту Міністерства оборони України. Київ, 2023. 5 с.

10. Шпиталь О. Можливі шляхи вдосконалення внутрішнього аудиту в системі Міністерства оборони України: аналіз, виклики та стратегічні рекомендації. *Social Development and Security*. 2025. Vol. 15, No. 5. С. 264–283. DOI: https://doi.org/10.33445/sds.2025.15.5.21.

11. The Institute of Internal Auditors. Глобальні Стандарти Внутрішнього Аудиту. Флорида, 2024. 129 с.

12. The Institute of Internal Auditors. The IIA's Three Lines Model: An Update of the Three Lines of Defense. Lake Mary, 2020. 14 p.

13. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0) : NIST AI 100-1. Gaithersburg, 2023. 48 p.

14. The Institute of Internal Auditors. Artificial Intelligence Auditing Framework (September 2024 Update). Lake Mary, 2024. 32 p.

15. ISACA. Auditing Artificial Intelligence. Rolling Meadows, 2018. 13 p.

16. Appendix I: Additional IT Audit Topics of Interest. INTOSAI Development Initiative. Oslo, [б.р.]. 10 p.

17. Брайко В. С. Штучний інтелект в аудиті фінансових результатів: методологічні аспекти та практична реалізація. *Економіка і регіон*. 2025. № 4 (99). С. 139–145. DOI: https://doi.org/10.26906/EiR.2025.4(99).4165.

18. Alassuli A. Impact of artificial intelligence using the robotic process automation system on the efficiency of internal audit operations at Jordanian commercial banks. *Banks and Bank Systems*. 2025. Vol. 20, Iss. 1. P. 122–135. DOI: https://doi.org/10.21511/bbs.20(1).2025.11.

19. Оптимізація діяльності з внутрішнього аудиту в кризові часи. Київ : Міністерство фінансів України, [б.р.]. 43 с.

REFERENCES:

1. Biudzhetnyi kodeks Ukrainy [Budget Code of Ukraine]: Kodeks Ukrainy vid 08.07.2010 № 2456-VI. Available at: https://zakon.rada.gov.ua/laws/show/2456-17 (accessed March 01, 2026).

2. Deiaki pytannia zdiisnennia vnutrishnoho audytu ta utvorennia pidrozdiliv vnutrishnoho audytu [Some issues of internal audit implementation and establishment of internal audit units]: Postanova Kabinetu Ministriv Ukrainy vid 28.09.2011 № 1001. Available at: https://zakon.rada.gov.ua/laws/show/1001-2011-п (accessed March 01, 2026).

3. Pro zatverdzhennia Osnovnykh zasad zdiisnennia vnutrishnoho kontroliu rozporiadnykamy biudzhetnykh koshtiv [On approval of the Basic Principles of Internal Control by Budget Fund Managers]: Postanova Kabinetu Ministriv Ukrainy vid 12.12.2018 № 1062. Available at: https://zakon.rada.gov.ua/laws/show/1062-2018-п (accessed March 01, 2026). 12 p.

4. Pro skhvalennia Kontseptsii rozvytku shtuchnoho intelektu v Ukraini [On approval of the Concept for the Development of Artificial Intelligence in Ukraine]: Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 02.12.2020 № 1556-r. Available at: https://zakon.rada.gov.ua/laws/show/1556-2020-р (accessed March 03, 2026).

5. Pro zatverdzhennia Standartiv vnutrishnoho audytu [On approval of Internal Audit Standards]: Nakaz Ministerstva finansiv Ukrainy vid 04.10.2011 № 1247. Available at: https://zakon.rada.gov.ua/laws/show/z1219-11 (accessed March 03, 2026). 20 p.

6. Pro zatverdzhennia Poriadku orhanizatsii v systemi Ministerstva oborony Ukrainy vnutrishnoho kontroliu ta upravlinnia ryzykamy [On approval of the Procedure for Internal Control and Risk Management in the Ministry of Defence of Ukraine]: Nakaz Ministerstva oborony Ukrainy vid 02.04.2019 № 145 (u redaktsii nakazu vid 22.10.2025 № 709). 55 p.

7. Polozhennia pro Departament vnutrishnoho audytu Ministerstva oborony Ukrainy [Regulation on the Internal Audit Department of the Ministry of Defence of Ukraine] (u redaktsii nakazu vid 28.11.2025 № 825). 10 p.

8. Ministerstvo finansiv Ukrainy (2019) Metodolohichni vkazivky z vnutrishnoho audytu v derzhavnomu sektori Ukrainy [Methodological Guidelines on Internal Audit in the Public Sector of Ukraine]. Kyiv: Ministerstvo finansiv Ukrainy, 162 p. (in Ukrainian)

9. Ministerstvo oborony Ukrainy (2023) Deklaratsiia vnutrishnoho audytu Ministerstva oborony Ukrainy [Internal Audit Declaration of the Ministry of Defence of Ukraine]. Kyiv, 5 p. (in Ukrainian)

10. Shpytal O. (2025) Mozhlyvi shliakhy vdoskonalennia vnutrishnoho audytu v systemi Ministerstva oborony Ukrainy: analiz, vyklyky ta stratehichni rekomendatsii [Possible ways to improve internal audit in the system of the Ministry of Defence of Ukraine: analysis, challenges and strategic recommendations]. *Social Development and Security*, vol. 15, no. 5, pp. 264–283. DOI: https://doi.org/10.33445/sds.2025.15.5.21.

11. The Institute of Internal Auditors (2024) *Global Internal Audit Standards*. Lake Mary: The Institute of Internal Auditors, 129 p.

12. The Institute of Internal Auditors (2020) *The IIA's Three Lines Model: An Update of the Three Lines of Defense*. Lake Mary: The Institute of Internal Auditors, 14 p.

13. National Institute of Standards and Technology (2023) *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*: NIST AI 100-1. Gaithersburg: NIST, 48 p.

14. The Institute of Internal Auditors (2024) *Artificial Intelligence Auditing Framework* (September 2024 Update). Lake Mary: The Institute of Internal Auditors, 32 p.

15. ISACA (2018) *Auditing Artificial Intelligence*. Rolling Meadows: ISACA, 13 p.

16. INTOSAI Development Initiative (n.d.) *Appendix I: Additional IT Audit Topics of Interest*. Oslo: INTOSAI Development Initiative, 10 p.

17. Braiko V. S. (2025) Shtuchnyi intelekt v audyti finansovykh rezultativ: metodolohichni aspekty ta praktychna realizatsiia [Artificial intelligence in financial performance auditing: methodological aspects and practical implementation]. *Ekonomika i rehion – Economy and Region*, no. 4 (99), pp. 139–145. DOI: https://doi.org/10.26906/EiR.2025.4(99).4165.

18. Alassuli A. (2025) Impact of artificial intelligence using the robotic process automation system on the efficiency of internal audit operations at Jordanian commercial banks. *Banks and Bank Systems*, vol. 20, iss. 1, pp. 122–135. DOI: https://doi.org/10.21511/bbs.20(1).2025.11.

19. Ministerstvo finansiv Ukrainy (n.d.) Optymizatsiia diialnosti z vnutrishnoho audytu v kryzovi chasy [Optimization of internal audit activities in times of crisis]. Kyiv: Ministerstvo finansiv Ukrainy, 43 p. (in Ukrainian)

Дата надходження статті: 20.04.2026
Дата прийняття статті: 08.05.2026
Дата публікації статті: 15.05.2026