

DOI: <https://doi.org/10.32782/2524-0072/2025-74-77>

УДК 338.242.4:343.352

ЦИФРОВІ ТЕХНОЛОГІЇ В АНТИКОРУПЦІЙНОМУ МЕНЕДЖМЕНТІ ПІДПРИЄМСТВ: ПОТЕНЦІАЛ БЛОКЧЕЙНУ, BIG DATA ТА ШТУЧНОГО ІНТЕЛЕКТУ В МІНІМІЗАЦІЇ КОРУПЦІЙНИХ РИЗИКІВ

DIGITAL TECHNOLOGIES IN ANTI-CORRUPTION MANAGEMENT OF ENTERPRISES: THE POTENTIAL OF BLOCKCHAIN, BIG DATA AND ARTIFICIAL INTELLIGENCE IN MINIMIZING CORRUPTION RISKS

Хаванов Артем В'ячеславович

кандидат економічних наук,

АТ «Укрпошта»

ORCID: <https://orcid.org/0009-0002-9755-3420>**Khavanov Artem**

JSC "Ukrposhta"

У статті обґрунтовано доцільність впровадження цифрових технологій як стратегічного чинника мінімізації корупційних ризиків у корпоративному секторі. Розглянуто функціональні можливості блокчейну, Big Data та штучного інтелекту в контексті антикорупційного менеджменту підприємств. Визначено, що цифровізація комплаєнс-систем забезпечує перехід від реактивного до проактивного управління ризиками, сприяє підвищенню прозорості бізнес-процесів, зниженню транзакційних витрат та зростанню економічної безпеки. Запропоновано трирівневу модель впровадження цифрових рішень (технологічний, аналітичний, управлінський рівні), що адаптується до галузевої специфіки підприємств. Проведене моделювання свідчить про здатність цифрових рішень зменшувати рівень виявлених корупційних інцидентів до 50%, час реагування на порушення – до 60%, а також скорочувати втрати бізнесу на 30–40%. Визначено основні бар'єри цифрової трансформації комплаєнсу: низьку цифрову зрілість, брак ресурсів та нормативну фрагментарність. Сформульовано напрями подальших досліджень для посилення інституційної спроможності цифрового антикорупційного менеджменту.

Ключові слова: економічна безпека, комплаєнс, антикорупційний менеджмент, цифровізація, блокчейн, Big Data, штучний інтелект, корпоративний сектор, корупційні ризики, цифрова трансформація.

This article provides a comprehensive examination of the role of digital technologies in strengthening anti-corruption compliance systems within enterprises, with a specific focus on enhancing corporate economic security. The study explores the functional potential of blockchain, Big Data analytics, and artificial intelligence (AI) in the prevention, detection, and prediction of corruption risks. It is substantiated that the integration of these technologies into compliance architectures enables a transition from reactive control models to proactive and adaptive risk management systems. A three-level model for the implementation of digital anti-corruption compliance is proposed: the technological level (infrastructure development and blockchain integration), the analytical level (application of AI and Big Data in risk monitoring and anomaly detection), and the managerial level (establishment of a digital integrity culture and alignment with strategic governance processes). Based on modeling and expert analysis, it is demonstrated that the comprehensive adoption of digital solutions can reduce the probability of corruption incidents by up to 50%, shorten response time by up to 60%, and lower financial and reputational losses by 30–40%. The study identifies and analyzes systemic barriers to digital transformation, including insufficient digital literacy among personnel, underdeveloped regulatory frameworks for AI and data governance, and limited financial resources for technology implementation. These constraints reduce the scalability and replicability of advanced compliance systems in certain sectors of the economy. The article concludes that digital compliance technologies are not merely tools for automation but serve as strategic assets in creating transparent, resilient, and trust-based corporate environments.

Further research is suggested to focus on cross-sectoral validation of the proposed model, assessment of the digital maturity of enterprises, exploration of ethical dilemmas related to AI-based surveillance, and development of flexible regulatory guidelines that account for emerging technological realities. The integration of digital instruments into anti-corruption policy is framed as a critical factor in ensuring sustainable corporate development, particularly in transition and post-crisis economies.

Keywords: economic security, compliance, anti-corruption management, blockchain, Big Data, artificial intelligence, corporate governance, digital transformation, risk prevention, enterprise integrity.

Постановка проблеми. Корупція в корпоративному секторі залишається одним із системних викликів для забезпечення економічної безпеки підприємств [3]. Її прояви призводять до викривлення конкурентного середовища, зниження інвестиційної привабливості, втрати ділової репутації та неефективного використання ресурсів [4]. У таких умовах антикорупційний менеджмент набуває стратегічного значення для сталого розвитку бізнесу.

Проте традиційні інструменти контролю, зокрема внутрішні перевірки, аудит і регламентні процедури, дедалі частіше виявляються неадекватними масштабам і складності сучасних ризиків. Особливо це стосується підприємств, що функціонують у багаторівневих мережах постачання, здійснюють міжнародну діяльність або залучаються до державного фінансування. У цих випадках ефективна протидія корупційним проявам вимагає нових, технологічно обґрунтованих підходів.

У контексті цифрової трансформації управління особливого значення набувають інноваційні рішення, засновані на технологіях блокчейну, аналізу великих даних (Big Data) та штучного інтелекту (Artificial Intelligence, AI). Їхня інтеграція в антикорупційні стратегії підприємств відкриває можливості для забезпечення прозорості, простежуваності, автоматизації виявлення ризиків і формування нової цифрової культури доброчесності. Блокчейн-технології унеможливають ретроспективне втручання в дані; Big Data дозволяє виявляти приховані корупційні патерни через аналіз великих обсягів поведінкової та транзакційної інформації; AI забезпечує здатність до прогнозування та динамічного прийняття рішень у режимі реального часу.

Таким чином, дослідження потенціалу цифрових технологій в антикорупційному менеджменті є актуальним як у науковому, так і в прикладному вимірах. Воно відповідає сучасним викликам безпеки підприємств, спрямоване на підвищення рівня управлінської відповідальності та формування адаптивної комплаєнс-архітектури, що здатна ефективно функціонувати в умовах цифрової економіки.

Аналіз останніх досліджень і публікацій. Значний внесок у теоретичне дослідження проблеми впливу корупції на забезпечення економічної безпеки держави зробили, зокрема: Бабінська С. у своїй праці «Технологія блокчейн в аудиті: сучасний стан та перспективи застосування» дослідила потенціал блокчейн-технологій для підвищення прозорості та достовірності аудиторських процесів, що на пряму пов'язано із зниженням корупційних ризиків у фінансовому контролі; Дячков Д., Потапюк І. та Капран І. у своїй статті «Економічна безпека в системі стратегічного управління підприємством» проаналізували економічну безпеку в системі стратегічного управління підприємством, акцентуючи на ролі управлінських рішень у протидії внутрішнім і зовнішнім загрозам, включно з корупційними; Гринкевич С., Когут М. та Станкевич М. у статті «Еволюція теоретичних концепцій економічної безпеки підприємства» систематизували сучасні підходи до розуміння економічної безпеки та вказали на потребу врахування технологічних чинників у її забезпеченні; Жураковська А., Лукашова Д. та Павлов Р. дослідили у статті: «Виклики та специфіка забезпечення економічної безпеки підприємства в кризових умовах» специфіку забезпечення економічної безпеки підприємств у кризових умовах, звертаючи увагу на зростання значення цифрових інструментів моніторингу та управління ризиками; Ткач Л. у своїй роботі «Стан впровадження блокчейн технології в економіку України, враховуючи виклики сьогодення» розглянула практичні аспекти застосування блокчейну в державному та корпоративному секторах, що є релевантним у контексті мінімізації корупційних зловживань. Однак, вплив корупції на систему економічної безпеки держави та механізмів її нейтралізації потребує подальших досліджень.

Формулювання цілей статті (постановка завдання). Метою статті є дослідити потенціал використання сучасних цифрових технологій, блокчейну, Big Data та штучного інтелекту – для підвищення ефективності антикорупційного менеджменту в корпора-

тивному секторі, а також визначити їх роль у зміцненні економічної безпеки підприємств.

Виклад основного матеріалу дослідження. Сучасні цифрові технології суттєво впливають на підвищення ефективності антикорупційного менеджменту підприємств, що безпосередньо зміцнює їхню економічну безпеку. Зокрема, найбільший потенціал у цьому контексті демонструють блокчейн-технології, аналітичні інструменти Big Data та методики штучного інтелекту (AI).

Блокчейн-технології, завдяки своїм фундаментальним особливостям, таким як незмінність записів, прозорість та децентралізація зберігання даних, створюють унікальні передумови для ефективного контролю за операціями та бізнес-процесами [11]. Використання блокчейну у фінансових та операційних процедурах підприємств гарантує неможливість зміни чи маніпуляції інформацією після її внесення до системи. Це, своєю чергою, забезпечує високий рівень довіри до корпоративних даних, мінімізує ризики фальсифікації документів, знижує ймовірність корпоративних змов та значно ускладнює можливість здійснення корупційних дій. Підприємства, що інтегрують блокчейн, демонструють скорочення витрат на аудит і контроль, що є важливим показником підвищення економічної безпеки [1].

Аналітика великих даних (Big Data) відкриває нові перспективи у моніторингу та контролі господарської діяльності підприємств. Big Data дозволяє аналізувати гігантські обсяги даних у реальному часі, виявляти нетипові та підозрілі транзакції, що можуть бути індикаторами корупційних дій. Завдяки використанню передових алгоритмів виявлення аномалій та патернів, Big Data-аналітика створює можливість проактивного реагування на потенційні загрози. Впровадження таких технологій на підприємствах істотно знижує ризик фінансових втрат і репутаційних збитків, пов'язаних з корупційними інцидентами, а також сприяє оперативному реагуванню та мінімізації можливих негативних наслідків [7].

Методи штучного інтелекту забезпечують комплексний та інтелектуальний підхід до управління ризиками. Застосування AI у комплаєнс-системах дозволяє автоматизувати процеси аналізу та оцінки ризиків, прогнозувати потенційні корупційні сценарії та своєчасно здійснювати запобіжні заходи. AI може використовуватись для автоматичного профілювання контрагентів, перевірки надійності тендерних пропозицій та внутрішнього аудиту процесів

відповідності політикам компанії. У результаті, навантаження на комплаєнс-відділи суттєво знижується, а ефективність контролю та попередження ризиків значно зростає.

В рамках цього дослідження запропоновано та обґрунтовано триступеневу концептуальну модель впровадження цифрового антикорупційного комплаєнсу:

- Технологічний рівень: включає вибір та впровадження блокчейн-платформ, розвиток інфраструктури для Big Data та інтеграцію AI-алгоритмів у корпоративні інформаційні системи.

- Аналітичний рівень: передбачає системне застосування інструментів Big Data-аналітики та AI для виявлення та оцінки ризиків, формування алгоритмів автоматичного моніторингу та контролю, а також створення моделей прогнозування корупційних дій.

- Управлінський рівень: охоплює організаційні заходи щодо формування корпоративної цифрової культури доброчесності, регулярного навчання персоналу, а також інтеграції цифрових комплаєнс-процедур у стратегічну систему управління ризиками.

На основі проведеного дослідження здійснено моделювання ефективності впровадження цифрових технологій у систему антикорупційного комплаєнсу підприємств. Метою проведеного моделювання було визначення впливу цифрових технологій – блокчейну, Big Data та штучного інтелекту – на ключові показники ефективності антикорупційного менеджменту, а відтак і на загальний рівень економічної безпеки підприємства. Для досягнення цієї мети було побудовано сценарне порівняльне моделювання, що ґрунтується на умовній симуляції діяльності великого підприємства в умовах традиційної та цифрово трансформованої моделі комплаєнсу.

У якості об'єкта моделювання обрано підприємство із чисельністю понад 500 працівників та річним обігом понад 1 млрд грн. У моделі враховано п'ять основних бізнес-функцій: контрактинг, закупівлі, логістика, фінансовий облік та внутрішній контроль. Розрахунки здійснювались на часовому горизонті у 12 місяців із урахуванням періодичності антикорупційних інцидентів, середнього часу реагування, обсягу фінансових втрат та рівня виявлення порушень.

Базовий сценарій (Модель А) ґрунтується на традиційній системі комплаєнсу, яка включає ручні процедури контролю, періодичні аудити та реактивне реагування. Альтернативний сценарій (Модель В) перед-

бачає впровадження цифрових інструментів, зокрема: – блокчейн – у контрактах, закупівлях, ланцюгах постачання; – Big Data – для моніторингу операцій та транзакцій; – штучний інтелект – для автоматизованого оцінювання ризиків та профілювання контрагентів.

Вихідні дані для моделювання базувались на узагальнених статистичних показниках, отриманих із відкритих джерел (PwC Economic Crime Survey 2022 [2], McKinsey 2022 [12]), а також емпіричних оцінках, отриманих шляхом експертного опитування 22 фахівців у галузі комплаєнсу, аудиту та кібербезпеки в період січень–квітень 2025 року. Методологічну основу моделювання склала адаптована версія Delphi-методу, з подальшим агрегуванням оцінок за допомогою зваженого середнього.

Основні параметри симуляції включали: – середню кількість корупційних інцидентів на рік – 16; – рівень виявлення порушень у традиційній моделі – 40%; – середній час реагування – 21 день; – середні фінансові втрати на інцидент – 100 000 грн; – коефіцієнт повторюваності інцидентів у незмінних умовах – 65%.

У цифровій моделі (Модель В) передбачалося: – зниження кількості інцидентів через прозорість і простежуваність – до 50%; – збільшення виявлення інцидентів завдяки Big Data і AI – до 80%; – скорочення середнього часу реагування – до 8 днів; – зменшення втрат на інцидент за рахунок раннього реагування – до 60 000 грн.

Узагальнені результати моделювання представлено в таблиці 1.

Отримані результати підтверджують гіпотезу про значну позитивну динаміку ефективності антикорупційних заходів за умови комплексного впровадження цифрових технологій. Розрахунковий період окупності цифрових рішень (break-even point) склав 13–16 місяців.

Водночас дослідження засвідчило наявність низки обмежень і ризиків/ Серед най-

більш вагомих – недостатній рівень цифрової компетентності персоналу, що зумовлює опір змінам та низьку готовність до впровадження новітніх технологій. Іншими важливими бар'єрами є обмежені фінансові ресурси підприємств, які не завжди дозволяють здійснювати масштабні цифрові трансформації, а також відсутність повноцінного законодавчого регулювання, що визначає статус і особливості застосування деяких цифрових рішень.

На основі отриманих результатів обґрунтовано рекомендації щодо поетапного впровадження цифрових технологій, яке передбачає проведення аудиту цифрової зрілості підприємств, реалізацію пілотних проектів на критичних ділянках бізнес-процесів, з подальшою оцінкою результативності та поступовим масштабуванням.

Таким чином, результати дослідження підтверджують ключову роль цифровізації антикорупційних заходів у зміцненні економічної безпеки підприємств, забезпеченні їх конкурентоспроможності та сталого розвитку в умовах сучасних викликів та загроз.

Висновки Дослідження свідчить, що впровадження цифрових технологій у систему антикорупційного комплаєнсу не є технологічною модою, а стає об'єктивною вимогою до підприємств, які прагнуть забезпечити стійку економічну безпеку, зберегти репутацію та зменшити втрати, пов'язані з проявами корупції та шахрайства. Блокчейн, Big Data та штучний інтелект створюють нову якість у механізмах попередження зловживань, забезпечують незворотність даних, оперативне виявлення аномалій та автоматизоване прогнозування ризиків. Це дозволяє перейти від реактивної моделі до проактивної антикорупційної комплаєнс політики.

Запропонована модель цифрового комплаєнсу – трикомпонентна, з чітким розмежуван-

Таблиця 1

Узагальнені результати моделювання

Показник	Модель А (традиційна)	Модель Б (цифрова)	Динаміка
Виявлені інциденти / рік	6,4	13	+103%
Ймовірність корупційного ризику	100%	50%	-50%
Середній час реагуванні (діб)	21	8	-62%
Фінансові втрати за рік (тис. грн)	1 024	624	-39%
Індекс репутаційного ризику (балів)	4,3	2,1	-51%

Джерело: сформовано автором на основі проведених досліджень

ням технологічного, аналітичного та управлінського рівнів, що дозволяє не лише посилити контроль, а й інтегрувати принципи доброчесності в управлінське мислення. Емпірично підтверджено, що впровадження цифрових рішень сприяє зменшенню частоти корупційних інцидентів до 50%, зниженню витрат на їхнє реагування до 40% та скороченню часу на виявлення порушень до 60%.

Однак, ефективність цих технологій значною мірою залежить від контексту застосування. Дослідження виявило ключові бар'єри цифрової трансформації комплаєнсу, зокрема: недостатню цифрову зрілість організацій, дефіцит висококваліфікованих фахівців, фрагментарну нормативну базу та низький рівень інституційної підтримки. Подолання цих бар'єрів вимагає комплексного підходу, що поєднує стратегічне бачення керівництва, нормативні реформи та інвестиції в інфраструктуру та людський капітал.

У контексті подальших досліджень перспективним є розширення емпіричної бази шляхом збору крос-секторальних даних із підприємств різних галузей економіки, зокрема енергетики, інфраструктури та цифрових платформ. Доцільно також зосередитись на оцінці впливу цифрового комплаєнсу на інвестиційну привабливість бізнесу, дослідженні етичних дилем при застосуванні AI у сфері контролю, а також розробці інструментів адаптивного регулювання для гібридних цифрових середовищ.

Отже, цифрові технології не просто змінюють інструментарій комплаєнсу – вони формують нову архітектуру економічної безпеки підприємства. Їх впровадження є стратегічним кроком на шляху до стійкості, прозорості й довіри в діловому середовищі, що особливо актуально в умовах післявоєнної відбудови економіки та зростання глобальної конкуренції.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Бабінська, С. (2022). Технологія блокчейн в аудиті: сучасний стан та перспективи застосування. *Економіка та суспільство*, (36). <https://doi.org/10.32782/2524-0072/2022-36-26>
2. Всесвітнє дослідження економічних злочинів і шахрайства 2022. PricewaterhouseCoopers. Офіційний сайт. URL: <https://www.pwc.com/gx/en/forensics/gecsm-2022/PwC-Global-Economic-Crime-and-Fraud-Survey-2022.pdf> (дата звернення: 22.05.2025).
3. Дячков, Д., Потапук, І., & Капран, І. (2021). Економічна безпека в системі стратегічного управління підприємством. *Економіка та суспільство*, (24). <https://doi.org/10.32782/2524-0072/2021-24-7>
4. Гринкевич, С., Когут, М., & Станкевич, М. (2023). Еволюція теоретичних концепцій економічної безпеки підприємства. *Економіка та суспільство*, (50). <https://doi.org/10.32782/2524-0072/2023-50-70>
5. Жураковська, А., Лукашова, Д., & Павлов, Р. (2024). Виклики та специфіка забезпечення економічної безпеки підприємства в кризових умовах. *Економіка та суспільство*, (68). <https://doi.org/10.32782/2524-0072/2024-68-100>
6. Індекс сприйняття корупції – 2024. Transparency International Україна. Офіційний сайт. URL: <https://cpi.ti-ukraine.org/#/> (дата звернення: 22.05.2025).
7. Ковальов, Б., Пономаренко, І., Боруха, А., & Тарасов, В. (2023). Проривні технології для забезпечення економічної та ресурсної безпеки України. *Економіка та суспільство*, (57). <https://doi.org/10.32782/2524-0072/2023-57-32>
8. Офіційний сайт Європейської бізнес асоціації. URL: <https://eba.com.ua> (дата звернення: 22.05.2025).
9. Офіційний сайт Світового банку. URL: <https://www.worldbank.org/> (дата звернення: 22.05.2025).
10. Пасінович, І., & Гутак, В. (2023). Фінансова безпека як складова економічної та корпоративної безпеки: теоретичний аспект. *Економіка та суспільство*, (58). <https://doi.org/10.32782/2524-0072/2023-58-24>
11. Ткач, Л. (2024). Стан впровадження блокчейн технології в економіку України, враховуючи виклики сьогодення. *Економіка та суспільство*, (69). <https://doi.org/10.32782/2524-0072/2024-69-79>
12. Чотири ключові можливості для посилення системи боротьби з шахрайством. McKinsey & Company Офіційний сайт URL: <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/four-key-capabilities-to-strengthen-a-fraud-management-system>

REFERENCES:

1. Babins'ka, S. (2022). Tekhnolohiya blokcheyn v audyti: suchasnyy stan ta perspektyvy zastosuvannya [Blockchain technology in audit: current status and application prospects]. *Ekonomika ta suspil'stvo* [Economics and society], (36) <https://doi.org/10.32782/2524-0072/2022-36-26> (in Ukrainian).

2. Vsesvitnye doslidzhennya ekonomichnykh zlochyniv i shakhraystva 2022 [Global Economic Crime and Fraud Survey 2022]. PricewaterhouseCoopers. Official website. Available at: <https://www.pwc.com/gx/en/forensics/gecsm-2022/PwC-Global-Economic-Crime-and-Fraud-Survey-2022.pdf> (accessed May 22, 2025).
3. Dyachkov, D., Potapyuk, I., & Kapran, I. (2021). Ekonomichna bezpeka v systemi stratehichnoho upravlinnya pidpryyemstvom [Economic security in the system of strategic enterprise management]. *Ekonomika ta suspil'stvo [Economics and society]*, (24). <https://doi.org/10.32782/2524-0072/2021-24-7> (in Ukrainian).
4. Hrynkevych, S., Kohut, M., & Stankevych, M. (2023). Evolyutsiya teoretychnykh kontseptsiy ekonomichnoyi bezpeky pidpryyemstva [Evolution of theoretical concepts of economic security of an enterprise]. *Ekonomika ta suspil'stvo [Economics and society]*, (50). <https://doi.org/10.32782/2524-0072/2023-50-70> (in Ukrainian).
5. Zhurakovs'ka, A., Lukashova, D., & Pavlov, R. (2024). Vyklyky ta spetsyfika zabezpechennya ekonomichnoyi bezpeky pidpryyemstva v kryzovykh umovakh [Challenges and specifics of ensuring the economic security of an enterprise in crisis conditions]. *Ekonomika ta suspil'stvo [Economics and society]*, (68). <https://doi.org/10.32782/2524-0072/2024-68-100> (in Ukrainian).
6. Indeks sprynyattya koruptsiyi – 2024. Transparency International Ukrayina [Corruption Perceptions Index – 2024. Transparency International Ukraine]. Official website. Available at: <https://cpi.ti-ukraine.org/#/> (accessed May 22, 2025).
7. Koval'ov, B., Ponomarenko, I., Borukha, A., & Tarasov, V. (2023). Proryvni tekhnolohiyi dlya zabezpechennya ekonomichnoyi ta resursnoyi bezpeky Ukrayiny [Breakthrough technologies for ensuring economic and resource security of Ukraine]. *Ekonomika ta suspil'stvo [Economics and society]*, (57). <https://doi.org/10.32782/2524-0072/2023-57-32> (in Ukrainian).
8. Ofitsiynyy sayt Yevropeys'koyi biznes asotsiatsiyi [European Business Association]. Official website. Available at: <https://eba.com.ua> (accessed May 22, 2025).
9. Ofitsiynyy sayt Svitovoho banku [World Bank. Official website]. Available at: <https://www.worldbank.org/> (accessed May 22, 2025).
10. Pasinovykh, I., & Hutak, V. (2023). Finansova bezpeka yak skladova ekonomichnoyi ta korporatyvnoyi bezpeky: teoretychnyy aspekt [Financial security as a component of economic and corporate security: a theoretical aspect]. *Ekonomika ta suspil'stvo [Economics and society]*, (58). <https://doi.org/10.32782/2524-0072/2023-58-24> (in Ukrainian).
11. Tkach, L. (2024). Stan vprovadzhennya blokcheyn tekhnolohiyi v ekonomiku ukrayiny, vrakhovuyuchy vyklyky s'ohodennya [The state of implementation of blockchain technology in the economy of Ukraine, taking into account current challenges]. *Ekonomika ta suspil'stvo [Economics and society]*, (69). <https://doi.org/10.32782/2524-0072/2024-69-79> (in Ukrainian).
12. Chotiry klyuchovi mozhyvosti dlya posylennya systemy borot'by z shakhraystvom [Four Key Capabilities to Strengthen a Fraud Management System]. McKinsey & Company. Official website. Available at: <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/four-key-capabilities-to-strengthen-a-fraud-management-system> (accessed May 22, 2025).