

Кримінальний процес та криміналістика; судова експертиза;  
оперативно-розшукова діяльність

УДК 343.1+343.9

**Виноградов Вадим Ігорович**

*аспірант кафедри криміналістики,*

*детективної та оперативно-розшукової діяльності*

*Національного університету «Одеська юридична академія»*

**Vynohradov Vadym**

*Postgraduate at the Department of Criminalistics,*

*Detective and Investigative Activity*

*National University "Odesa Law Academy"*

*ORCID: 0000-0002-6212-0142*

**ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В РОЗСЛІДУВАННІ  
ЗЛОЧИНІВ У СФЕРІ ПУБЛІЧНИХ ЗАКУПІВЕЛЬ  
APPLICATION OF ARTIFICIAL INTELLIGENCE IN  
INVESTIGATING CRIMES IN PUBLIC PROCUREMENT**

***Анотація.** Вступ. Сфера публічних закупівель є однією з найбільш чутливих до корупційних ризиків, оскільки оперує значними обсягами державних коштів. Зловживання у цій сфері включають змови між учасниками, фаворитизм, підставні компанії, завищення цін та інші деструктивні практики. Виявлення таких правопорушень ускладнено обсягами даних, маскуванням злочинної активності та браком людських ресурсів у правоохоронних органах. На цьому тлі штучний інтелект (ШІ) розглядається як інструмент, здатний підвищити ефективність криміналістичної роботи за рахунок автоматизованого аналізу даних, виявлення аномалій, побудови моделей змов тощо.*

*Мета.* Метою є дослідження можливостей, меж та переваг застосування інструментів ІІІ для розслідування корупційних правопорушень у сфері публічних закупівель, а також визначити, які методи найбільш релевантні до сучасних українських умов.

*Матеріали і методи.* Методологічну базу дослідження становить компаративний аналіз зарубіжних і вітчизняних прикладів застосування AI-інструментів (Alice, GRAS, ProZorro, Dozorro, CMA AI-tool), а також контент-аналіз наукових публікацій, нормативних документів та результатів експертного моделювання. Використано загальнонаукові та спеціальні методи: системний підхід, дедукція, моделювання типових слідчих ситуацій, елементи правового аналізу.

*Результати.* Стаття розкриває низку можливих сценаріїв використання ІІІ в антикорупційному розслідуванні: аналіз тендерних аномалій, побудова графів зв'язків, застосування NLP для аналізу текстів закупівельної документації, виявлення синхронності дій учасників. Обґрунтовано доцільність використання explainable AI для забезпечення правового захисту та прозорості роботи алгоритмів. Визначено бар'єри для впровадження ІІІ в Україні: фрагментованість даних, необхідність нормативного закріплення AI-висновків у доказовій базі, брак інституційної спроможності. У статті проаналізовано ефект запровадження ІІІ-систем на прикладі Dozorro та Alice – зокрема, скорочення часу аналізу даних та підвищення точності виявлення злочинів.

*Перспективи.* У подальших дослідженнях слід зосередити увагу на створенні нормативної бази для використання AI-доказів у кримінальному процесі, адаптації AI-моделей до національного контексту, формуванні системи навчання слідчих щодо роботи з AI, а також міжвідомчій

інтеграції державних даних у форматі, придатному для машинного аналізу.

**Ключові слова:** публічні закупівлі, корупція, штучний інтелект, кримінальне розслідування, машинне навчання, виявлення змов, аналіз даних.

**Summary.** *Introduction.* The public procurement sector is among the most vulnerable to corruption risks, especially in countries where significant portions of state budgets are allocated through tenders. Malpractices such as bid-rigging, favoritism, shell companies, and price inflation often remain undetected due to data complexity, hidden schemes, and limited investigative capacity. Against this background, artificial intelligence (AI) is increasingly regarded as a promising tool for enhancing forensic work through automated data analysis, anomaly detection, and modeling of collusive behavior.

*Purpose.* This study aims to explore the potential, limitations, and advantages of using AI-based tools in investigating procurement-related crimes, and to identify which AI methods are most applicable to current conditions in Ukraine.

*Materials and Methods.* The research is based on a comparative analysis of international and Ukrainian case studies involving AI implementation (e.g., Alice, GRAS, ProZorro, Dozorro, CMA AI-tool), a review of scholarly publications and legal documents, and expert-based scenario modeling. It applies general scientific methods such as system analysis, deduction, legal analysis, and simulation of typical investigative scenarios.

*Results.* The article outlines several scenarios for using AI in anti-corruption investigations: tender anomaly detection, graph analysis of connections between actors, natural language processing (NLP) for document review, and behavioral pattern analysis. It emphasizes the importance of explainable AI (XAI) to ensure transparency and legal defensibility of

*algorithmic outputs. Key implementation challenges in Ukraine are identified: fragmented data systems, lack of legal frameworks for using AI-generated evidence, and limited institutional capacity. Practical outcomes from tools like Dozorro and Alice are analyzed, showing significant gains in efficiency and accuracy of corruption detection.*

*Perspectives. Future research should focus on creating a legal framework for using AI-based evidence in criminal procedures, adapting AI models to local legal and contextual specifics, training investigators in AI tool usage, and developing national data integration strategies to support machine-readable formats for public procurement monitoring.*

**Key words:** *public procurement, corruption, artificial intelligence, criminal investigation, machine learning, collusion detection, data analytics.*

**Постановка проблеми.** Публічні закупівлі є однією з найбільш уразливих до корупції сфер економіки, оскільки через них розподіляються значні державні кошти. Недоброчесні практики – такі як підкуп посадовців, змови між учасниками торгів (бід-ригінг) чи шахрайське завищення цін – призводять до прямих фінансових втрат держави та підривають довіру суспільства. Виявлення та розслідування таких злочинів традиційно є складним завданням. По-перше, обсяг інформації про тендери, контракти та учасників надзвичайно великий, що ускладнює ручний аналіз. По-друге, корупційні схеми постійно адаптуються і маскуються під легітимні процеси, тому розпізнати їх без спеціальних інструментів буває важко. Звичайні аудиторські перевірки нерідко виявляють порушення лише постфактум, через значний час після їх скоєння, а правоохоронні органи залежать від повідомлень викривачів чи випадкових знахідок. Це створює запит на нові підходи, що дозволяють швидше і точніше виявляти підозрілі ситуації в закупівлях.

Одним із перспективних напрямів вирішення цієї проблеми є використання штучного інтелекту. Сучасні алгоритми здатні опрацьовувати великі масиви даних і знаходити приховані закономірності, недоступні для аналізу людиною за розумний час. У сфері закупівель це може означати автоматичний моніторинг усіх тендерів і контрактів на наявність аномальних ознак, сигналів змови чи інших „червоних прапорців” (red flags) корупції. Таким чином, актуальною проблемою є розробка і впровадження таких інтелектуальних систем в діяльність правоохоронних та контролюючих органів. Постає питання: які саме технології ШІ можна застосувати для розслідування злочинів у сфері публічних закупівель, наскільки ефективними вони є на практиці, та які виклики виникають при їх використанні?

**Аналіз останніх досліджень і публікацій.** Проблематика застосування ШІ для протидії корупції в закупівлях активно досліджується протягом останніх років різними науковими спільнотами – від інформаційних технологій до правознавства. Проведено кілька оглядових досліджень, що систематизують наявний досвід. Зокрема, Торрес-Беру та ін. (2020) виконали систематичний аналіз 102 наукових публікацій (2015–2019) і виявили, що найпоширенішими методами ШІ для виявлення корупційних схем є статистичні та машинні алгоритми: байєсовські класифікатори, нейронні мережі, методи опорних векторів (SVM), дерева рішень, логістична і лінійна регресія тощо [7]. Інші автори відзначають, що більшість досліджень зосереджена на виявленні саме шахрайства та змов при торгах (близько 77% публікацій), тоді як питанню хабарництва присвячено лише ~5%, нецільового завищення цін ~7% і кумівства ~4% [6]. Такий перекис пояснюється тим, що шахрайські дії та змови легше виявляти за слідами в даних (аномалії в цінах, повторювані виграти тощо), тоді як хабарі залишають менше цифрових слідів.

Чимало робіт присвячено аналізу великих масивів відкритих даних про тендери і контракти. Дослідники застосовують методи data mining для пошуку нетипових шаблонів: наприклад, виявлення підозрілих зв'язків між учасниками та замовниками, що можуть вказувати на змову [6]. Використовуються як класичні методи класифікації, що "навчаються" на історичних випадках корупції (для прогнозування ймовірності порушень), так і алгоритми пошуку аномалій без навчання на мітках (для автоматичного виокремлення нетипових контрактів або компаній). У оглядовій роботі Modrušan et al. (2021) підкреслено, що окрім моделей класифікації, активно застосовуються асоціативні правила та графові бази даних – вони допомагають виявляти приховані зв'язки між економічними операторами (постачальниками) і замовниками, а також розкривати дочірні/афілійовані компанії, що спільно беруть участь у змові на торгах [5]. Таким чином можна ідентифікувати угруповання підприємств, які систематично „розігрують” тендери між собою.

Сучасні наукові роботи виходять за рамки просто пошуку фінансових аномалій. З'являються дослідження з використанням обробки текстів (NLP) для аналізу тендерної документації на наявність підозрілих формулювань чи ознак маніпуляцій. Наприклад, наголошується, що аналіз мовних особливостей листування посадовців може виявити ознаки змови чи зловживань ще на етапі комунікації [3]. Інші роботи застосовують глибоке навчання: зокрема, продемонстровано можливість використання глибинних ознак зображень для ідентифікації фіктивних постачальників (тобто виявлення компаній-«фантомів» за непрямыми ознаками у їх профілях) [3].

В контексті прогнозування, Gallego та колеги (2021) розробили модель раннього виявлення недоброчесних практик, що здатна на основі сукупності економічних і політичних факторів передбачати ймовірність

порушень у закупівлях ще до їх здійснення [3]. Загалом література свідчить про значний інтерес до інструментів ШІ як у превентивному, так і в детективному (розшуковому) аспектах антикорупційної діяльності.

**Метою дослідження** є визначення та систематизація основних напрямів застосування штучного інтелекту у процесі розслідування злочинів у сфері публічних закупівель, а також оцінка ефективності і обмежень таких підходів. Для досягнення поставленої мети вирішуються наступні **завдання**: 1) проаналізувати проблематику розслідування зловживань у закупівлях та потреби правоохоронної практики; 2) здійснити огляд сучасних наукових досліджень і технологічних розробок, присвячених застосуванню ШІ в цій сфері; 3) класифікувати основні методи та інструменти ШІ, що можуть бути використані для виявлення ознак злочинів (аномалії, змови, шахрайство тощо) в закупівельних даних; 4) розглянути реальні приклади впровадження таких технологій у світі та в Україні, проаналізувати їх результати; 5) окреслити ключові виклики, пов'язані з впровадженням ШІ у процес розслідування (правові, технічні, етичні), та напрями подальших досліджень для їх подолання.

**Виклад основного матеріалу.** *Застосування ШІ для аналізу закупівельних даних.* Злочини у сфері закупівель залишають різноманітні сліди в даних – від цінових аномалій до неявних зв'язків між учасниками торгів. Штучний інтелект дає змогу автоматично сканувати великі масиви тендерної інформації та сигналізувати про підозрілі випадки. Центральну роль відіграють алгоритми машинного навчання, які можуть виявляти аномалії та закономірності без прямого втручання людини. Наприклад, моделі класифікації можуть бути навчені розрізняти „нормальні” та „підозрілі” тендери на основі історичних даних про відомі порушення. Якщо новий тендер має характеристики, схожі на ті, що були у корупційних випадках (скажімо, виграш фірми з ознаками фіктивності,

значне перевищення середньоринкової ціни, дуже короткий термін подачі пропозицій і т.д.), модель присвоїть йому високий *рейтинг ризику*. Це дозволить слідчим звернути увагу на контракт ще до укладення або невдовзі після, а не через роки.

Інший підхід – пошук аномалій – не вимагає навчання на наперед відомих прикладах корупції. Система аналізує всі тендери і виявляє ті, які статистично вибиваються із загальної картини. Так, алгоритми можуть знайти учасника, що постійно програє, але потім раптово виграє з дуже високою ціною, або ж компанії, між якими розподіл вигравів значно відрізняється від випадкового. Такі відхилення можуть бути маркерами, наприклад, прихованого змовного розподілу ринку чи «відкатів». Важливо, що методи асоціативного аналізу і графового аналізу дозволяють будувати мережі зв'язків: якщо дві різні компанії мають спільних засновників або через ланцюжок фірм пов'язані з одним кінцевим бенефіціаром, це теж сигнал для перевірки. Алгоритми побудови графів і спільнот використовуються для виявлення таких груп змовників у публічних закупівлях [5]. Наприклад, у разі подання для проформи (коли декілька підставних компаній створюють видимість конкурсу, щоб забезпечити перемогу наперед визначеного учасника) аналіз графу участі в торгах покаже, що одна й та сама група компаній неодноразово зустрічається разом у різних тендерах, причому виграє по черзі один із членів групи.

*Обробка текстових даних та інших неструктурованих даних.* Окрім числових даних (цін, дат, кількості учасників тощо), у сфері закупівель є великий масив текстової інформації: описи предмета закупівлі, технічні вимоги, пояснення замовників, переписка тощо. Тут у нагоді стають методи Natural Language Processing (NLP) – обробки природної мови. Вони дозволяють шукати лінгвістичні патерни, що можуть свідчити про

порушення. Досвід Європейського офісу боротьби з шахрайством (OLAF) показує, що аналіз службових електронних листів із застосуванням NLP здатен виявити «сигнали» корупції – наприклад, незвично часте використання певних ключових слів чи виразів, пов'язаних з неформальними домовленостями [5]. В контексті закупівель це можуть бути ознаки того, що тендерні вимоги пишуться «під свого» постачальника (наприклад, специфічні характеристики товару, які відповідають лише одному виробнику). ШІ-алгоритми можуть порівнювати тендерну документацію з типовими шаблонами і виявляти нетипові відхилення або ж навіть генерувати гіпотези про навмисне обмеження конкуренції.

Інноваційним напрямом є аналіз інших неструктурованих даних – зображень, PDF-документів тощо. Деякі дослідники використовують комп'ютерний зір для перевірки достовірності інформації, поданої учасниками. Приміром, може проводитися аналіз фотографій чи сканів документів, що додаються до тендерних пропозицій. В одному з досліджень було продемонстровано, що на основі глибинних ознак зображень можна ідентифікувати фейкових постачальників – йдеться про компанії, які існують лише на папері і створені для махінацій [5]. Такі компанії можуть подавати стандартні зображення або схожі шаблонні документи, і ШІ здатний знайти перетини або аномалії (наприклад, багато різних фірм завантажують документи, створені на одному комп'ютері чи мають однакові візуальні артефакти). Хоча цей напрям ще розвивається, він підкреслює широкі можливості ШІ: від аналізу цифр до „читання” текстів і перегляду зображень задля виявлення ознак злочинних схем.

Приклади практичного впровадження ШІ-інструментів. Світовий досвід уже має низку успішних прикладів застосування штучного

інтелекту для виявлення і розслідування зловживань у публічних закупівлях. Наведемо найбільш показові кейси:

- Система “Alice” в Бразилії. Ще у 2015 році Офіс генерального контролера Бразилії запровадив бота під назвою Alice, що комбінує аналіз даних, машинне навчання та регулярні вирази для моніторингу державних тендерів [5]. Alice автоматично перевіряє тендерні пропозиції та контракти на типові ознаки розтрата, змови чи антиконкурентних дій і сповіщає аудиторів про потенційні порушення. За повідомленнями, впровадження Alice значно підвищило можливості уряду з виявлення шахрайських схем – фінансові втрати в перевірених випадках зменшилися на 30% завдяки своєчасному виявленню проблем [8]. Цей приклад демонструє, що ШІ може реально зекономити кошти, попередивши укладення сумнівних контрактів або забезпечивши раннє втручання.
- Інструмент GRAS (Governance Risk Assessment System). Світовий банк нещодавно (листопад 2023) запустив пілотний проєкт GRAS у Бразилії – систему оцінки ризиків з використанням передової аналітики даних для виявлення ризиків шахрайства, корупції та змови в державних закупівлях [3]. Ця система інтегрує різні джерела даних про закупівлі і дозволяє ранжувати тендери за рівнем ризику, допомагаючи контрольним органам спрямувати зусилля на перевірку найбільш проблемних випадків. GRAS є прикладом сучасного підходу, що поєднує rule-based індикатори ризику з алгоритмами машинного навчання.
- Моніторинг листування OLAF. На наднаціональному рівні в ЄС теж експериментують з ШІ. Європейське агентство OLAF заявляло, що використовує NLP-алгоритми для автоматичного відстеження підозрілих формулювань в електронних листах чиновників [3]. Хоча

це стосується внутрішніх розслідувань, технологія аналогічна тій, що потрібна для закупівель: вона показує здатність ІІІ відслідковувати великий масив текстової інформації і позначати ті фрагменти, які можуть свідчити про неформальні домовленості або порушення процедур.

- Система "Datacros". Цей інструмент, розроблений дослідницьким центром Transcrime, вже впроваджується органами влади в кількох країнах (Румунія, Франція, Литва) для оцінки ризиків у діяльності компаній [3]. Datacros використовує великий обсяг даних про структуру власності фірм, їх зв'язки, фінансові показники тощо, аби виявити аномалії, які вказують на ризики змови, відмивання коштів чи корпоративної корупції. Для закупівель це означає, що система може сигналізувати, якщо, приміром, у двох різних учасників тендеру виявляється спільний власник, або якщо низка компаній-переможців пов'язані через ланцюжок аффілійованих осіб. Таким чином виявляються приховані конфлікти інтересів та корупційні мережі ще до початку формального розслідування.
- ProZorro та модулі ІІІ в Україні. Вітчизняний досвід теж розвивається. Україна з 2016 року експлуатує систему електронних закупівель ProZorro, яка забезпечує відкритість даних про тендери. На основі цієї системи у співпраці з міжнародними організаціями та громадськістю було впроваджено інструменти моніторингу з елементами ІІІ, що допомагають виявляти порушення у публічних закупівлях та запобігати нецільовому витрачанню коштів. Зокрема, громадський модуль DoZorro використовує алгоритми для автоматичного пошуку ознак порушень в тендерних процесах. Ще у 2018 році повідомлялося про запуск "алгоритмів зради" – спеціальних модулів, що сканують базу ProZorro на типові

порушення (наприклад, учасник з однаковими документами в різних тендерах, нехарактерні стрибки ціни тощо) [9]. Державна аудиторська служба також впровадила систему ризик-індикаторів, яка автоматично маркує підозрілі тендери для подальшого аналізу аудиторами. У 2025 році, в умовах воєнного стану, продовжується удосконалення таких інструментів, аби мінімізувати людський фактор і швидко реагувати на зловживання навіть при спрощених процедурах закупівель. Таким чином, українська практика підтверджує ефективність тандему відкритих даних і ШІ: база ProZorro дає основу для алгоритмів, а алгоритми натомість підсилюють можливості контролю.

- Пілотний проект СМА у Великій Британії. Окремо варто згадати досвід боротьби зі змовами на торгах у розвинутих країнах. Управління з питань конкуренції та ринків Великої Британії (СМА) у 2024–2025 рр. випробовує AI-інструмент для виявлення бідригінгу (змовного змінювання цін) у державних закупівлях [1]. Ця система вміє сканувати великий масив даних про тендерні пропозиції та знаходити аномальні сценарії, коли конкуруючі компанії, ймовірно, координували свої дії для штучного завищення цін. За словами керівника СМА Сари Карделл, нові можливості дозволяють аналізувати тендерні дані у масштабі, неможливому раніше, і виявляти відхилення в поведінці учасників, що можуть свідчити про антиконкурентну змову [1]. Цей пілотний проект уже привів до розслідування конкретних випадків (наприклад, підряди на ремонт шкільних дахів) та накладення штрафів на компанії-змовники. Британський досвід демонструє, що правоохоронні та регуляторні органи все активніше використовують ШІ не тільки для

пост-фактум розслідувань, але й для проактивного виявлення злочинних схем на ранніх стадіях.

Наведенні приклади підтверджують: штучний інтелект успішно інтегрується в антикорупційну діяльність різних країн і реально допомагає викривати складні злочини у сфері закупівель. Системи на зразок Alice чи модулів ProZorro за лічені секунди обробляють те, на що людині знадобилися б тижні роботи, і видають перелік підозрілих кейсів для перевірки. Водночас, впровадження таких систем висвітлює і низку проблемних питань, які слід враховувати.

*Обмеження та виклики впровадження III.* Попри оптимістичні результати, застосування III в розслідуванні корупційних злочинів стикається з низкою викликів. Перший з них – якість та доступність даних. Ефективність моделей машинного навчання значною мірою залежить від повноти і достовірності вхідних даних [5]. У країнах, де цифровізація державних процесів недостатня, дані про закупівлі можуть бути неповними або неструктурованими. Як зауважують експерти, у той час як в окремих державах (наприклад, скандинавських) більшість інформації давно оцифровано, в інших регіонах відсутня необхідна цифрова інфраструктура даних [8]. Це обмежує можливості тренування алгоритмів – «сирі» неструктуровані дані потребують попереднього очищення та підготовки, що є трудомістким процесом. В Україні завдяки ProZorro ситуація з відкритими даними одна з кращих у світі, але і тут є нюанси: наприклад, на час воєнного стану окремі дані можуть тимчасово не розкриватися публічно з міркувань безпеки, що зменшує «видимість» для автоматичних систем.

Другий виклик – необхідність верифікації та юридична значимість доказів, здобутих III. Алгоритм може видати сигнал про порушення, але сам по собі цей сигнал ще не є доказом у юридичному сенсі.

Правоохоронці повинні перевірити та підтвердити його традиційними методами слідства (огляд документів, допити тощо). На практиці були випадки, коли ШІ-система правильно виявляла аномалії, але зібраної інформації виявлялося недостатньо для висунення обвинувачень. Показовим є приклад бота "Rosie" в Бразилії, що аналізував витрати парламентарів: він знаходив багато підозрілих випадків, проте згодом з'ясувалося, що ці знахідки важко використати в суді – потрібні додаткові докази [8]. У результаті початковий ентузіазм спав, і бот перестали активно використовувати. Звідси урок: ШІ-інструменти мають слугувати допоміжним засобом для слідчого, своєрідною підказкою, але не заміною розслідування. Необхідно налагодити тісну взаємодію між аналітиками даних та детективами, щоб кожен сигнал штучного інтелекту проходив осмислену перевірку і доведення до стадії юридичного доказу.

Ще одна проблема – прозорість і довіра до алгоритмів. Багато моделей машинного навчання (особливо глибинні нейронні мережі) діють як «чорний ящик», видаючи результат без чіткого пояснення, чому саме цей тендер позначено ризикованим. Для правника та суду надзвичайно важливо розуміти логіку виявлення порушення. Якщо алгоритм непояснюваний, його висновки можуть бути поставлені під сумнів стороною захисту. Тому актуальним напрямом є розвиток інтерпретованого ШІ (explainable AI) – щоб системи не лише сигналізували про проблему, а й вказували, які фактори на це вплинули (наприклад: «ціна на 30% перевищує середню, переможець пов'язаний з іншим учасником через спільного власника» тощо).

Не можна не згадати і етичні та правові аспекти. Алгоритми можуть мимоволі успадковувати упередження, наявні в даних. Якщо в історичних даних корупційні справи порушувалися переважно щодо певних регіонів чи галузей, модель може вважати їх „апріорі підозрілими” і прогавити

схеми в інших місцях. Або навпаки – надмірно часто хибно сигналізувати на типові, але добросовісні випадки (так звані *false positives*). Відомий скандал з системою SyRI в Нідерландах (хоч вона стосувалася соцстрахування, а не закупівель) показав, що без належного контролю алгоритми ризикують дискримінувати окремі групи населення [3]. SyRI аналізувала дані різних відомств для виявлення шахрайства з соціальними виплатами, але згодом з'ясувалося, що вона непропорційно часто обирала для перевірок бідні райони, фактично тавруючи мешканців за соціально-економічною ознакою. Систему довелося припинити через суспільний резонанс та судові рішення про порушення прав людини. Цей приклад є застереженням: впровадження ШІ у чутливій сфері потребує чітких правил і контролю, аби технологія не порушувала принцип недискримінації та презумпції невинуватості.

Нарешті, технічний і кадровий аспект: для успішного використання ШІ потрібні фахівці, здатні його розробити, налаштувати і експлуатувати. У сфері правоохоронних органів це вимагає *міждисциплінарного підходу* – юристи повинні співпрацювати з дата-аналітиками. Потрібні навчальні програми, що ознайомлять слідчих із можливостями та обмеженнями алгоритмів. Без розуміння того, як працює система, складно впровадити її результати в реальні кейси. Тому поряд із технічним розвитком алгоритмів не менш важливим є розвиток інституційної спроможності правоохоронних структур користуватися такими інструментами.

**Висновки і перспективи подальших досліджень.** Результати проведеного аналізу показують, що штучний інтелект відкриває нові горизонти у розслідуванні злочинів у сфері публічних закупівель. Сучасні ШІ-системи здатні значно підвищити ефективність виявлення складних корупційних схем – передусім завдяки швидкій обробці великих обсягів даних та виявленню прихованих взаємозв'язків і аномалій. Існуючі

прикладі на міжнародному рівні (Бразилія, Великобританія, ЄС, Україна тощо) демонструють реальний вплив: впровадження алгоритмів машинного навчання дозволило скоротити втрати від шахрайства, виявити раніше непомітні змови між учасниками торгів, підвищити прозорість і підзвітність закупівель. Для української системи ProZorro інтеграція ШІ-модулів стала логічним кроком у розвитку електронних закупівель і вже зараз сприяє зміцненню фінансової дисципліни та попередженню зловживань.

Водночас, застосування ШІ не є панацеєю і потребує зваженого підходу. Алгоритми повинні працювати під наглядом людини – роль слідчого та аудитора залишається центральною. ШІ здатний швидко знайти „голку в копиці сіна”, але оцінити, чи ця голка справді є доказом злочину, мусить фахівець. Тому важливо налагодити ефективну взаємодію між технологічними рішеннями та традиційними методами криміналістики. Одним із перспективних напрямків є розвиток інтерпретованих і дружніх до користувача ШІ-систем: щоб аналітичні панелі чітко пояснювали, чому певний тендер вважається ризиковим, які фактори вплинули на оцінку, та яка ймовірність помилки. Це підвищить довіру слідчих до рекомендацій системи і полегшить обґрунтування висновків в юридичній площині.

Перспективи подальших досліджень включають також удосконалення алгоритмів з урахуванням специфіки національного законодавства та контексту. Наприклад, в Україні корисно було б навчити моделі на даних про уже розслідувані випадки змов у закупівлях, щоб вони виявляли схожі шаблони в інших держзамовниках. Варто продовжити роботу над інтеграцією різних джерел даних: поєднання відкритих даних ProZorro з реєстрами компаній, податковою інформацією, даними про публічних службовців тощо для створення комплексної

картини і виявлення складних мультифакторних схем. Також необхідно досліджувати питання нормативно-правового забезпечення використання ШІ: від стандартів якості даних до процедур легалізації отриманих аналітичних матеріалів як доказів. На міжнародному рівні актуальним є обмін досвідом між країнами щодо успішних ШІ-рішень у публічних закупівлях і спільна розробка етичних стандартів їх застосування.

На завершення, можна констатувати, що штучний інтелект наразі виступає потужним інструментом, який доповнює арсенал криміналістики в боротьбі з корупцією. Правильне впровадження та використання ШІ-систем у сфері публічних закупівель здатне змінити правила гри: з реактивного реагування на вже скоєні правопорушення на проактивне попередження і своєчасне виявлення злочинних намірів. Це сприятиме підвищенню прозорості державних закупівель, економії бюджетних коштів та зміцненню верховенства права. Подальший прогрес у цій галузі залежатиме від тісної співпраці між розробниками технологій, науковцями-правниками та практиками правоохоронних органів з метою створення безпечного, ефективного і справедливого механізму використання штучного інтелекту на благо суспільства.

### **Література**

1. CMA launches trial of new AI tool to detect bid-rigging in public procurement. *Competition & Markets Authority UK*. 2023. URL: <https://www.gov.uk/government/news/cma-trials-new-ai-tool-to-detect-bid-rigging-in-public-procurement> (дата звернення: 23.04.2025).
2. Gallego J., Rivero G., Martínez J. Preventing rather than punishing: An early warning model of malfeasance in public procurement. *International Journal of Forecasting*. 2021. Vol. 37, №1. P. 360–377. DOI: 10.1016/j.ijforecast.2020.06.006.

3. Gerli C. How public organisations can use AI in anti-corruption: What we know so far and why we need to learn more about it. *Centre for Digital Governance Blog*. 2024. URL: <https://www.hertie-school.org/en/digital-governance/research/blog/detail/content/how-public-organisations-can-use-ai-in-anti-corruption-what-we-know-so-far-and-why-we-need-to-learn-more-about-it> (дата звернення: 23.04.2025).

4. Lomas N. UK uses AI to tackle 'bid-rigging' collusion in public procurement contracts. *TechCrunch*. 2025. URL: <https://techcrunch.com/2025/01/06/uk-uses-ai-to-tackle-bid-rigging-collusion-in-public-procurement-contracts/> (дата звернення: 23.04.2025).

5. Modrušan N., Rabuzin K., Mršić L. Review of public procurement fraud detection techniques powered by emerging technologies. *International Journal of Advanced Computer Science and Applications*. 2021. Vol. 12, №2. DOI: 10.14569/IJACSA.2021.0120272.

6. Nai R., Sulis E., Meo R. Public Procurement Fraud Detection and Artificial Intelligence Techniques: A Literature Review. *CEUR Workshop Proceedings*. 2022. Vol. 3256. P. 1–13. URL: <http://ceur-ws.org/Vol-3256/> (дата звернення: 23.04.2025).

7. Torres-Berrú Y., López Batista V. F., Torres-Carrión P., Jimenez M. G. Artificial intelligence techniques to detect and prevent corruption in procurement: A systematic literature review. *Applied Technologies* / Eds. M. Botto-Tobar et al. Cham: Springer, 2020. P. 254–268. DOI: 10.1007/978-3-030-64616-5\_21.

8. Unlocking AI's potential in anti-corruption: Hype vs. reality. *U4 Anti-Corruption Resource Centre*. 2025. URL: <https://www.u4.no/blog/unlocking-ai-s-potential-in-anti-corruption-hype-vs-reality> (дата звернення: 23.04.2025).

9. Алгоритми “зради”: як штучний інтелект DOZORRO знаходитиме порушення в ProZorro. *Transparency International Ukraine*.

2018. URL: <https://ti-ukraine.org/news/algorytmy-zrady-yak-shtuchnyj-intelekt-dozorro-znahodytyme-porushennya-v-prozorro/> (дата звернення: 23.04.2025).

10. Карпенко О., Карпенко Ю., Герман Д. Штучний інтелект як інструмент зниження корупційних ризиків у сфері публічних закупівель. *Аспекти публічного управління*. 2023. Т. 11, № 2. С. 129–135. DOI: 10.15421/152328.

### References

1. Competition & Markets Authority UK (2023) CMA launches trial of new AI tool to detect bid-rigging in public procurement. Available at: <https://www.gov.uk/government/news/cma-trials-new-ai-tool-to-detect-bid-rigging-in-public-procurement> (Accessed 23 Apr. 2025).

2. Gallego, J., Rivero, G. and Martínez, J. (2021) 'Preventing rather than punishing: An early warning model of malfeasance in public procurement', *International Journal of Forecasting*, 37(1), pp. 360–377. doi:10.1016/j.ijforecast.2020.06.006.

3. Gerli, C. (2024) How public organisations can use AI in anti-corruption: What we know so far and why we need to learn more about it. Centre for Digital Governance Blog. Available at: <https://www.hertie-school.org/en/digital-governance/research/blog/detail/content/how-public-organisations-can-use-ai-in-anti-corruption-what-we-know-so-far-and-why-we-need-to-learn-more-about-it> (Accessed 23 Apr. 2025).

4. Lomas, N. (2025) UK uses AI to tackle 'bid-rigging' collusion in public procurement contracts. TechCrunch. Available at: <https://techcrunch.com/2025/01/06/uk-uses-ai-to-tackle-bid-rigging-collusion-in-public-procurement-contracts/> (Accessed 23 Apr. 2025).

5. Modrušan, N., Rabuzin, K. and Mršić, L. (2021) 'Review of public procurement fraud detection techniques powered by emerging technologies',

International Journal of Advanced Computer Science and Applications, 12(2).  
doi:10.14569/IJACSA.2021.0120272.

6. Nai, R., Sulis, E. and Meo, R. (2022) 'Public Procurement Fraud Detection and Artificial Intelligence Techniques: A Literature Review', CEUR Workshop Proceedings, 3256, pp. 1–13. Available at: <http://ceur-ws.org/Vol-3256/> (Accessed 23 Apr. 2025).

7. Torres-Berrú, Y., López Batista, V.F., Torres-Carrión, P. and Jimenez, M.G. (2020) 'Artificial intelligence techniques to detect and prevent corruption in procurement: A systematic literature review', in Botto-Tobar, M. et al. (eds.) Applied Technologies. Cham: Springer, pp. 254–268. doi:10.1007/978-3-030-64616-5\_21.

8. U4 Anti-Corruption Resource Centre (2025) Unlocking AI's potential in anti-corruption: Hype vs. reality. Available at: <https://www.u4.no/blog/unlocking-ai-s-potential-in-anti-corruption-hype-vs-reality> (Accessed 23 Apr. 2025).

9. Transparency International Ukraine (2018) Alhorytmy "zrady": yak shtuchnyi intelekt DOZORRO znakhodytyme porushennia v ProZorro. Available at: <https://ti-ukraine.org/news/alhorytmy-zrady-yak-shtuchnyj-intelekt-dozorro-znahodytyme-porushennya-v-prozorro> (Accessed 23 Apr. 2025).

10. Karpenko, O., Karpenko, Y. and Herman, D. (2023) 'Shtuchnyi intelekt yak instrument znyzhennia koruptsiinykh ryzykiv u sferi publichnykh zakupivel', Aspekty publichnoho upravlinnia, 11(2), pp. 129–135. doi:10.15421/152328.