

**Адміністративне право і процес**

**УДК 343.35:004.8:351.74**

**DOI** <https://doi.org/10.5281/zenodo.20732060>

**Використання алгоритмів штучного інтелекту для оцінки корупційних ризиків у діяльності правоохоронних органів за міжнародними стандартами**

**Окопник Олена Миколаївна,**

кандидат юридичних наук, доцент, завідувач кафедри галузевого права та правоохоронної діяльності, Центральноукраїнський державний університет імені Володимира Винниченка, м. Кропивницький, Україна,  
<https://orcid.org/0000-0003-0598-0557>

**Кузєв Ігор Олегович,**

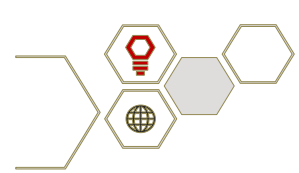
старший викладач кафедри транспортних технологій, Кременчуцький національний університет імені Михайла Остроградського, м. Кременчук, Україна, <https://orcid.org/0000-0002-3403-7069>

**Синявська Олена Юхимівна,**

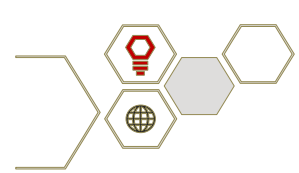
доктор юридичних наук, професор, професор кафедри правоохоронної діяльності, Навчально-науковий інститут № 5, Харківський національний університет внутрішніх справ, м. Харків, Україна,  
<https://orcid.org/0000-0002-6386-4151>

**Прийнято: 17.05.2026 | Опубліковано: 30.05.2026**

**Анотація.** Цифровізація державного управління актуалізує потребу в інструментах раннього виявлення корупційних ризиків у діяльності



правоохоронних органів. Використання алгоритмів штучного інтелекту дає змогу обробляти великі масиви інформації для формування об'єктивного аналізу доброчесності службової діяльності з урахуванням міжнародних вимог до прозорості та підзвітності правоохоронних органів. **Метою** дослідження є обґрунтування шляхів застосування алгоритмічних моделей для ідентифікації та оцінювання корупційних ризиків у правоохоронному секторі відповідно до міжнародних антикорупційних стандартів. Для розв'язання цих завдань застосовано системний аналіз, порівняльно-правовий метод, узагальнення нормативної бази міжнародного рівня та елементи аналітики даних і принципи машинного навчання. Джерельну основу становили міжнародні антикорупційні документи, регуляторні акти та практики цифрового аудиту. Обґрунтовано доцільність використання алгоритмів штучного інтелекту для автоматизованого виявлення ознак корупційних ризиків у діяльності правоохоронних органів шляхом аналізу фінансових операцій, кадрових рішень, службових комунікацій та результатів внутрішнього контролю. З'ясовано, що застосування методів машинного навчання забезпечує виявлення прихованих закономірностей та нетипових поведінкових моделей як ймовірних ознак потенційного зловживання службовим становищем. Водночас доведено ефективність використання предикативної аналітики для прогнозування ризикових ситуацій на ранніх стадіях їхнього виникнення, що сприяє своєчасному реагуванню та мінімізації негативних наслідків. Визначено основні індикатори ризик-оцінювання, зокрема рівень доступу посадових осіб до інформаційних ресурсів, повторюваність нетипових транзакцій, концентрація владних повноважень та відхилення від затверджених процедур ухвалення рішень. Додатково проаналізовано упровадження алгоритмічних моделей, які підвищують точність внутрішнього контролю, знижують вплив суб'єктивного чинника на процес оцінювання та забезпечує аргументованість управлінських рішень у сфері запобігання корупції. Отже, інтеграція алгоритмічних систем аналізу



даних в антикорупційний моніторинг посилює механізми запобігання правопорушенням і сприяє підвищенню прозорості діяльності правоохоронних органів, однак вимагає гармонізації національних процедур із міжнародними стандартами цифрового урядування, удосконалення алгоритмів оброблення даних та уніфікації вимог до використання інформаційних ресурсів.

**Ключові слова:** антикорупційний моніторинг, цифрова аналітика, правоохоронні органи, ризик-аналіз, машинне навчання, доброчесність.

**Use of artificial intelligence algorithms for assessing corruption risks in the activities of law enforcement agencies in accordance with international standards**

**Olena Okopnyk,**

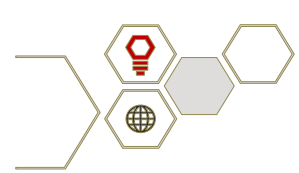
Candidate of Law, Associate Professor, Head of the Department of Branch Law and Law Enforcement Activity, Volodymyr Vynnychenko Central Ukrainian State University, Kropyvnytskyi, Ukraine,  
<https://orcid.org/0000-0003-0598-0557>

**Ihor Kuziev,**

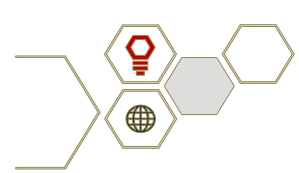
Senior Lecturer of the Department of Transport Technologies, Kremenchuk Mykhailo Ostrohradskyi National University, Kremenchuk, Ukraine,  
<https://orcid.org/0000-0002-3403-7069>

**Olena Syniavska,**

Doctor of Legal Sciences, Professor, Professor of the Department of Law Enforcement, Educational and Research Institute № 5, Kharkiv National University of Internal Affairs, Kharkiv, Ukraine,  
<https://orcid.org/0000-0002-6386-4151>



**Abstract.** The digitalization of public administration underscores the need for tools to detect corruption risks early in law enforcement agency activities. The use of artificial intelligence algorithms enables the processing of large amounts of information to produce objective assessments of the integrity of official activities, taking into account international requirements for transparency and accountability of law enforcement agencies. The purpose of the study is to substantiate the possibilities of using algorithmic models to identify and assess corruption risks in the law enforcement sector in accordance with international anti-corruption standards. To address the tasks set, a system analysis, a comparative legal method, generalization of the international regulatory framework, and elements of data analytics and machine learning were used. The source basis was international anti-corruption documents, regulatory acts and digital audit practices. The feasibility of using artificial intelligence algorithms for automated detection of corruption risks in law enforcement agency activities by analyzing financial transactions, personnel decisions, official communications and internal control results was substantiated. It has been established that machine learning methods can identify hidden patterns and atypical behavioral models that may indicate potential abuse of official position. The effectiveness of using predictive analytics to anticipate risk situations at their early stages has been proven, which contributes to timely responses and the minimization of negative consequences. The main risk assessment indicators have been determined, including officials' access to information resources, the recurrence of atypical transactions, and the concentration of power and deviations from established decision-making procedures. It has been established that the implementation of algorithmic models increases the accuracy of internal controls, reduces the influence of subjective factors on the assessment process, and provides greater justification for management decisions in the field of corruption prevention. Therefore, integrating algorithmic data analysis systems into anti-corruption monitoring strengthens mechanisms for preventing offenses and increases transparency in law enforcement activities, but it requires harmonizing national



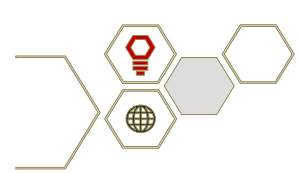
procedures with international digital governance standards, improving data processing algorithms and unifying requirements for the use of information resources.

**Keywords:** anti-corruption monitoring, digital analytics, law enforcement agencies, risk analysis, machine learning, integrity.

**Постановка проблеми.** Ідентифікація та оцінювання корупційних ризиків у діяльності правоохоронних органів залишається актуальним науково-практичним завданням, що зумовлено багаторівневою організацією управлінських процесів, значними масивами неупорядкованих даних та обмеженою спроможністю своєчасно виявляти приховані прояви зловживань. Водночас недостатня формалізація критеріїв ризик-аналізу сприяє зниженню ефективності традиційних процедур контролю та аудиту.

З огляду на це посилення вимог до прозорості та доброчесності діяльності органів правопорядку, закріплених у міжнародних антикорупційних стандартах, визначає потребу в інструментах, здатних забезпечувати безперервний аналіз даних і виявлення аномальних моделей поведінки. У цьому контексті особливого значення набуває використання алгоритмів штучного інтелекту, які можуть обробляти великі масиви інформації та формувати аналітичну експертизу ризиків в умовах, наближених до реального часу.

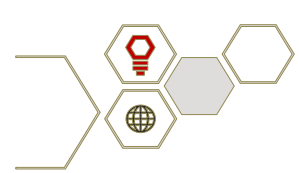
Наукова проблематика полягає у недостатньому розробленні методологічних засад упровадження алгоритмічних моделей для оцінювання корупційних ризиків у правоохоронному секторі з урахуванням міжнародних регуляторних вимог. Практичний аспект проблеми пов'язаний із необхідністю підвищення ефективності внутрішнього контролю у діяльності правоохоронних органів, мінімізації впливу суб'єктивних чинників під час ухвалення управлінських рішень та посилення превентивних механізмів запобігання корупційним правопорушенням. Отримані результати можуть



бути використані для удосконалення процедур антикорупційного моніторингу, цифрового аудиту, внутрішнього комплаєнс-контролю та адаптації міжнародних стандартів доброчесності до практики функціонування правоохоронних органів.

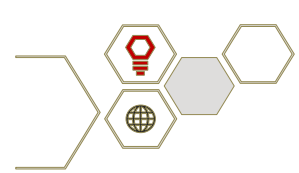
**Аналіз останніх досліджень і публікацій.** У науковій літературі сформовано значний масив досліджень, присвячених використанню штучного інтелекту у правовій сфері, кримінальному провадженні та антикорупційній діяльності, які охоплюють як теоретичні, так і прикладні аспекти цифрової трансформації.

Так, питання процесуального використання спеціальних знань у кримінальному провадженні через судову експертизу висвітлює А. Тимчишин, акцентуючи на значенні експертних процедур у формуванні доказової бази. Зокрема, проаналізовано еволюцію наукових поглядів на сутність спеціальних знань у системі кримінальної юстиції та розкрито трансформацію підходів до їхнього використання під час кримінального процесу [1; 2]. Медіаправові інструменти захисту прав громадян та протидії корупції досліджують Ю. Бідзіля, В. Шаркань і М. Цвіклінський, підкреслюючи роль інформаційно-правових механізмів у публічному управлінні [3]. Одночасно зміни у кримінальному процесі під впливом штучного інтелекту в умовах воєнного стану аналізують Ж. Удовенко, В. Галаган та В. Шкелебей, оцінюючи вплив цифрових технологій на ухвалення процесуальних рішень та здійснення кримінального провадження [4]. Крім того, адміністративно-правові засади упровадження штучного інтелекту у діяльність органів публічної влади й вирішальну роль цифрових технологій у модернізації управління визначає Т. Губанова [5]. Проблеми правового регулювання застосування штучного інтелекту у судовій системі та пов'язані із цим ризики розкриває Б. Демідонт [6]. А тенденції використання алгоритмічних технологій у кримінальному провадженні та їхній вплив на процесуальні рішення аналізують І. Басиста, Ж. Удовенко та М.-М. Кулинич,



наголошуючи на посиленні ролі цифрових інструментів у доказуванні [7]. Додатково, потенціал і ризики застосування штучного інтелекту у судовій практиці вивчають Д. Белов і М. Белова [8]. На використанні інтелектуальних цифрових технологій для протидії корупції та викликах, що супроводжують їхнє практичне застосування, акцентують Н. Кобіс (N. Köbis), К. Старк (C. Starke) та І. Рахван (I. Rahwan) [9]. Зокрема, потенціал генеративних моделей штучного інтелекту для виявлення та запобігання корупційним проявам аналізують М. Думчіков (M. Dumchikov) та О. Малетова (O. Maletova), визначаючи можливі загрози їхнього застосування для функціонування правової системи [10]. Питання дотримання фундаментальних прав людини та необхідності упровадження надійних правових гарантій їхнього захисту під час використання систем штучного інтелекту у діяльності правоохоронних органів досліджують Д. Касабу́ро (D. Casaburo) та І. Марш (I. Marsh) [11]. Відповідно, межі використання штучного інтелекту у правоохоронній діяльності у контексті європейського законодавства розкриває А. Сахуліду (A. Sachoulidou) [12], тоді як регуляторні моделі Європейського Союзу щодо штучного інтелекту та їхній вплив на правозастосування аналізують К. Содерлунд (K. Söderlund) і С. Ларссон (S. Larsson) [13]. Концепцію машинозчитуваного опису ризиків систем штучного інтелекту, призначену для спрощення процедур контролю за дотриманням правових і регуляторних вимог під час їхнього розроблення та упровадження, удосконалюють Д. Голпайєгані зі співавторами (D. Golpayegani et al.) [14]. У цьому контексті явища алгоритмічної дезінформації та маніпулятивного впливу систем штучного інтелекту аналізують П. С. Парк із колегами (P. S. Park et al.), обґрунтовуючи необхідність запровадження механізмів моніторингу й нагляду за процесами генерації та поширення інформації [15].





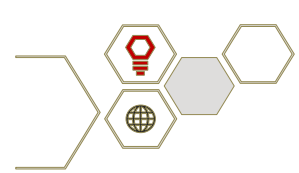
Отже, результати розглянутих досліджень формують теоретичне підґрунтя для подальшого вивчення алгоритмічних інструментів у сфері антикорупційного моніторингу.

**Виділення невирішених раніше частин загальної проблеми.** Попри значний розвиток цифрової аналітики та впровадження алгоритмічних рішень у сфері публічного управління, окремі складники оцінювання корупційних ризиків у діяльності правоохоронних органів залишаються недостатньо опрацьованими. Зокрема, відсутня цілісна методологія поєднання моделей штучного інтелекту із системами антикорупційного контролю відповідно до міжнародних стандартів комплаєнсу та доброчесності. Невизначеними є критерії формалізації ризикових індикаторів, які відображають специфіку службової діяльності, та механізми інтерпретації результатів алгоритмічного аналізу у правовому полі.

Це зумовлено переважанням техніко-математичних досліджень у сфері штучного інтелекту, тоді як правові та управлінські аспекти використання цифрових технологій для запобігання корупції залишаються недостатньо розробленими. Додатковою перешкодою є обмеженість емпіричних даних щодо результатів застосування алгоритмічних систем аналізу корупційних ризиків у діяльність органів державної влади, що ускладнює перевірку наукових положень та контроль ефективності запропонованих рішень. Насамкінець відсутність уніфікованих міжнародних підходів до алгоритмічного оцінювання корупційних ризиків знижує результативність порівняння даних, отриманих у різних країнах і правових системах.

Наявність цих нерозв'язаних питань обмежує ефективність цифрового моніторингу та стримує повноцінне використання інструментів штучного інтелекту в антикорупційній діяльності. Крім цього, недостатня формалізація критеріїв оцінювання та відсутність уніфікованих вимог до алгоритмічного аналізу унеможливають раннє виявлення порушень і використання





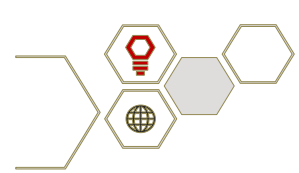
аналітичних рішень у практиці правоохоронних органів відповідно до міжнародних стандартів.

**Формулювання цілей статті (визначення завдання).** Метою дослідження є обґрунтування можливостей застосування алгоритмічних моделей штучного інтелекту для оцінювання корупційних ризиків у діяльності правоохоронних органів відповідно до міжнародних антикорупційних стандартів.

Для досягнення мети дослідження визначено такі завдання:

- проаналізувати міжнародні стандарти, рекомендації та регуляторні документи, які обґрунтовують вимоги до застосування технологій штучного інтелекту у сфері антикорупційного контролю та правоохоронної діяльності;
- охарактеризувати можливості інтелектуальних моделей у процесах виявлення та оцінювання корупційних ризиків у діяльності правоохоронних органів;
- сформулювати рекомендації щодо інтеграції штучного інтелекту у систему антикорупційного моніторингу та внутрішнього контролю правоохоронних органів.

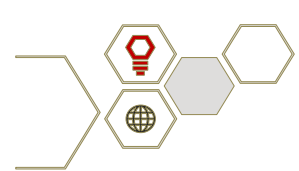
**Виклад основного матеріалу дослідження.** Поширення цифрових технологій у сфері публічного управління зумовлює трансформацію механізмів запобігання та виявлення корупційних ризиків у діяльності правоохоронних органів. А зростання обсягів інформаційних потоків, ускладнення управлінських процедур і підвищення вимог до прозорості службових рішень актуалізують використання аналітичних інструментів, здатних забезпечити системне опрацювання великих масивів даних. На цьому тлі алгоритмічні моделі штучного інтелекту формують інструментарій, що дає змогу підвищити об'єктивність оцінювання службової діяльності та посилити превентивний складник антикорупційного контролю відповідно до міжнародних стандартів доброчесності та підзвітності [3].



У цьому аспекті значущим є дослідження послідовного формування впливу штучного інтелекту на затвердження управлінських рішень. Так, поняття «штучного інтелекту» бере початок із Дартмутської конференції 1956 року, де воно було запропоноване для позначення обчислювальних систем, здатних імітувати окремі інтелектуальні функції людини. У науковому розумінні штучний інтелект охоплює широкий спектр алгоритмічних технологій, пов'язаних з аналізом даних, машинним навчанням, обробленням природної мови та створенням прогнозних рішень. До таких технологій належать генеративні системи на кшталт ChatGPT, Gemini та Copilot, які демонструють здатність до створення текстового контенту та підтримки процесів ухвалення рішень на основі великих масивів даних.

Відповідно, нормативне регулювання використання інтелектуальних технологій у правоохоронній сфері ґрунтується на міжнародних актах, що визначають базові принципи доброчесності, прозорості та захисту прав людини. Зокрема, Конвенція Організації Об'єднаних Націй проти корупції (United Nations Convention against Corruption, UNCAC) закріплює необхідність формування ефективних механізмів запобігання корупції та розвитку систем контролю в публічному секторі [16]. Водночас рекомендації Організації економічного співробітництва та розвитку з питань доброчесності публічного сектору (Organisation for Economic Co-operation and Development, OECD) визначають принципи підзвітності, відкритості процедур і управління ризиками [17]. Регламент Європейського Союзу про штучний інтелект (Artificial Intelligence Act, AI Act) запроваджує ризико орієнтований підхід до використання алгоритмічних систем, передбачаючи вимоги до їхньої безпечності, контрольованості, прозорості та мінімізації ризиків для прав людини [18].

Саме інтеграція алгоритмічних моделей у процеси оцінювання корупційних ризиків у діяльності правоохоронних органів потребує врахування міжнародних регуляторних вимог, які визначають основні



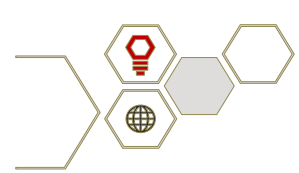
механізми функціонування інтелектуальних систем у сфері публічної безпеки та правопорядку. Особливого значення набуває узгодження національних практик із положеннями глобальних антикорупційних конвенцій, рекомендаціями щодо доброчесності публічного сектору та європейськими підходами до ризико орієнтованого регулювання штучного інтелекту. Систематизований огляд базових міжнародних документів, які регламентують прозорість, підзвітність і контрольованість алгоритмічних рішень, наведено у таблиці 1.

**Таблиця 1**

Міжнародні стандарти застосування алгоритмічних систем для оцінювання корупційних ризиків у діяльності правоохоронних органів

| Міжнародний документ / стандарт      | Регулятивні вимоги                                                         | Зміст для алгоритмічних моделей                                         | Практичні наслідки для правоохоронної діяльності                          |
|--------------------------------------|----------------------------------------------------------------------------|-------------------------------------------------------------------------|---------------------------------------------------------------------------|
| UNCAC (Конвенція ООН проти корупції) | Прозорість, запобігання корупції, ефективний контроль                      | Вимога до виявлення ризиків через аналіз даних і запобігання порушенням | Запровадження систем раннього виявлення корупційних ризиків               |
| OECD Public Integrity Framework      | Доброчесність, управління ризиками, підзвітність                           | Ризико орієнтоване моделювання поведінки посадових осіб                 | Формування профілів ризику службової діяльності                           |
| EU AI Act                            | Ризико орієнтована класифікація штучного інтелекту, високоризикові системи | Обов'язковий аналіз впливу, контроль даних, прозорість рішень           | Регламентування використання штучного інтелекту у правоохоронних системах |
| OECD AI Principles                   | Надійність, безпека, прозорість алгоритмів                                 | Вимоги до якості даних і мінімізації упередженості моделей              | Зменшення помилкових ризикових класифікацій                               |
| Council of Europe AI Guidelines      | Захист прав людини, недискримінація                                        | Контроль алгоритмічних рішень щодо впливу на права осіб                 | Юридичний аудит рішень штучного інтелекту                                 |
| FATF Recommendations (AML/CFT)       | Виявлення фінансових злочинів                                              | Аналіз підозрілих транзакцій і фінансових потоків                       | Інтеграція штучного інтелекту у фінансовий моніторинг                     |

Джерело: систематизовано автором на основі [16–21]

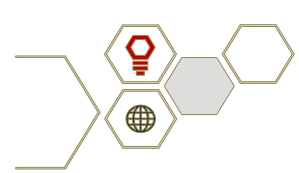


Таким чином, аналіз міжнародних нормативних актів засвідчує формування багаторівневої регуляторної архітектури використання інтелектуальних технологій у сфері протидії корупційним проявам. UNCAS регламентує базові вимоги щодо запобігання неправомірній поведінці через посилення прозорості управлінських процесів і дієвості контролю, обґрунтовуючи упровадження аналітичних механізмів у правоохоронному середовищі. Одночасно рекомендації OECD деталізують стандарти доброчесності публічного сектору, акцентуючи на ризико орієнтованому управлінні та підзвітності рішень, що прямо узгоджується із застосуванням алгоритмічних засобів для оцінювання службової поведінки.

Регламент ЄС щодо штучного інтелекту формує класифікацію інтелектуальних систем за рівнями загрози та визначає підвищені вимоги до високоризикових рішень, зокрема у правоохоронній сфері відповідно до забезпечення прозорості обчислювальних процедур, контрольованості інформаційних масивів і можливості пояснення результатів автоматизованого аналізу. Додаткові міжнародні керівні документи OECD AI Principles та рекомендації Ради Європи конкретизують стандарти надійності, недискримінаційності та захисту прав людини під час експлуатації інтелектуальних систем.

Узагальнення міжнародних вимог щодо цифрового антикорупційного моніторингу та комплаєнсу у секторі правопорядку формує нормативно-методологічне підґрунтя застосування алгоритмічних рішень для оцінювання корупційних ризиків. Воно охоплює затвердження принципів прозорості алгоритмів, підзвітності результатів автоматизованого аналізу, верифікованості джерел даних та контрольованості процедур оброблення інформації, що визначають межі допустимого використання штучного інтелекту у правоохоронній діяльності.

Алгоритмічні моделі у правоохоронній діяльності виконують функцію багатовимірного аналізу даних, спрямованого на виявлення поведінкових і



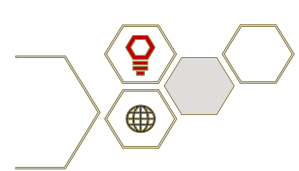
фінансових відхилень, яким притаманні нетипова структура операцій, повторюваність аномальних транзакцій та дисбаланс між службовими повноваженнями та фактичними управлінськими рішеннями. Застосування таких обчислювальних інструментів сприяє ідентифікації прихованих зв'язків між адміністративними діями, фінансовими потоками та показниками службової активності, формуючи підстави для оцінювання рівня ризикованості професійної поведінки посадових осіб [5, с. 17].

Отже, формалізація розпізнавання ризикових проявів передбачає їхню систематизацію за змістовними категоріями, що охоплюють фінансові, поведінкові, мережеві та документальні індикатори ризикової активності. Узагальнені характеристики ризик-оцінювання та інструменти їхнього виявлення наведено у таблиці 2.

**Таблиця 2**

Параметри формалізованого оцінювання корупційних ризиків у діяльності правоохоронних органів та інструменти алгоритмічного аналізу

| Параметр оцінювання           | Змістова характеристика                                                    | Приклади індикаторів ризику                                                            | Інструменти / алгоритмічні рішення                          |
|-------------------------------|----------------------------------------------------------------------------|----------------------------------------------------------------------------------------|-------------------------------------------------------------|
| Аномалії фінансових операцій  | Виявлення нетипових грошових потоків у службовій або пов'язаній діяльності | Часті транзакції однакових сум; дроблення платежів; невідповідність доходів витратам   | Isolation Forest, Random Forest, кредитні скорингові моделі |
| Поведінкові відхилення        | Аналіз службової активності та управлінських рішень                        | Повторювані нестандартні рішення; концентрація повноважень; відхилення від регламентів | Кластеризація (K-means), нейронні мережі                    |
| Мережеві зв'язки              | Виявлення прихованих взаємозалежностей між суб'єктами                      | Повторювані контакти із ризиковими контрагентами; непрозорі зв'язки                    | Graph Neural Networks, Social Network Analysis              |
| Документальні невідповідності | Порівняння офіційних даних із фактичними показниками                       | Розбіжності у звітності; дублювання записів; підроблені дані                           | NLP-моделі (BERT, GPT-класифікація), OCR-аналітика          |
| Ризик концентрації рішень     | Оцінювання рівня централізації службових повноважень                       | Надмірна кількість рішень в одного суб'єкта; відсутність розподілу функцій             | Статистичне моделювання, Bayesian networks                  |

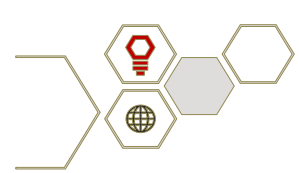


|                               |                                                      |                                                |                                   |
|-------------------------------|------------------------------------------------------|------------------------------------------------|-----------------------------------|
| Динаміка службової активності | Аналіз змін у поведінкових та операційних показниках | Різкі зміни активності; нетипові піки операцій | Аналіз часових рядів, LSTM-моделі |
|-------------------------------|------------------------------------------------------|------------------------------------------------|-----------------------------------|

Джерело: власна розробка авторів на основі [6–8]

Таке поєднання параметрів формалізованого оцінювання в алгоритмічні моделі аналізу ґрунтується на трактуванні фінансових, поведінкових, мережових і документальних індикаторів як взаємопов'язаних елементів ризик-профілю службової діяльності. Інтеграція цих груп показників забезпечує багатовимірність оцінювання та дає змогу виявляти приховані кореляції між управлінськими рішеннями, фінансовими потоками й організаційними зв'язками, що у традиційних контрольних процедурах залишаються недоступними для повної ідентифікації. Зокрема, застосування алгоритмічних засобів під час цього процесу підвищує точність і відтворюваність результатів ризик-аналізу та створює умови для стандартизації процедур внутрішнього моніторингу у правоохоронній сфері.

Водночас перехід до практичного використання штучного інтелекту у сфері антикорупційного моніторингу передбачає зміщення акценту з опису структурних параметрів ризик-аналізу на оцінювання їхньої функціональної ефективності в умовах реального правоохоронного середовища. У цьому контексті особливого значення набуває здатність алгоритмічних систем не лише фіксувати наявні ризикові індикатори, а й формувати прогностичне оцінювання на основі їхніх взаємозв'язків та динаміки змін. Вирішального значення при цьому набуває предикативна аналітика, яка забезпечує виявлення потенційних порушень на ранніх етапах їхнього формування. Саме вона ґрунтується на статистичному та алгоритмічному опрацюванні масивів історичних даних, що охоплюють службову активність, фінансові операції та управлінські рішення. У процесі обчислювального оброблення визначаються повторювані конфігурації поведінки, нетипові транзакційні операції та



відхилення від регламентованих процедур, які є первинними індикаторами ризикових ситуацій [14].

Ще одним етапом є розкриття таких індикаторів, яке здійснюється через застосування методів машинного навчання, орієнтованих на побудову багатовимірних моделей оцінювання. У таких моделях кожна ознака набуває значущості залежно від ступеня впливу на імовірність виникнення порушень, що забезпечує виявлення прихованих зв'язків між фінансовими потоками, управлінськими діями та поведінковими характеристиками службових осіб.

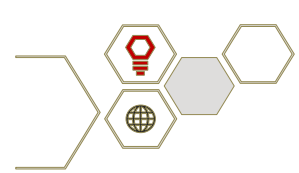
Подальше аналітичне опрацювання охоплює часові закономірності зміни даних, які дають змогу фіксувати динаміку службової активності та ідентифікувати короткострокові аномальні коливання. Порівняння часових інтервалів між операціями та рішеннями сприяє виявленню синхронізованих відхилень, що ймовірно засвідчуватимуть формування ризикових сценаріїв.

Відповідно, отримані результати прогностного моделювання трансформуються у структуровані ризикові профілі, які використовуються для визначення пріоритетних напрямів контрольної діяльності. Одночасно формується можливість концентрації аналітичних ресурсів на сегментах із підвищеною щільністю аномальних індикаторів, що підсилює превентивний характер моніторингу.

У прикладному вимірі предикативні моделі застосовуються для виявлення фінансових аномалій у службовій діяльності, зокрема у випадках дроблення платежів на суми нижче порогів фінансового контролю, багаторазових транзакцій між пов'язаними рахунками та невідповідності між задекларованими доходами й фактичними витратами. Алгоритмічне зіставлення банківських операцій із деклараційними даними та службовими повноваженнями формує підстави для фіксації потенційних корупційних проявів [15].

Окремий сегмент охоплює аналіз управлінських рішень щодо кадрових призначень, преміювання та розподілу адміністративних і фінансових





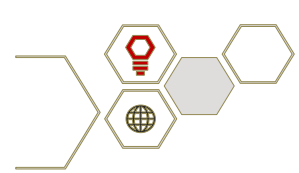
ресурсів, де виявляються повторювані рішення на користь обмеженого кола осіб, надмірна концентрація дискреційних повноважень або відсутність обґрунтованих критеріїв їхнього розподілу. Такі відхилення від стандартної адміністративної поведінки ідентифікуються через порівняння рішень у часовій динаміці та між структурними підрозділами.

У межах цифрової інфраструктури правоохоронних органів аналізу підлягають журнали доступу до інформаційних систем, реєстрів і баз даних. Нетипова активність, зокрема звернення до закритих ресурсів поза межами службових повноважень, підвищена частота запитів або доступ у часові проміжки, не характерні для виконання посадових обов'язків, розглядаються як ознаки ризикової поведінки.

Додаткове поєднання фінансових, управлінських і цифрових слідів формує інтегровані ризик-профілі, на основі яких здійснюється ідентифікація зон підвищеної ймовірності порушень та визначення пріоритетів аналітичного контролю.

З огляду на це формування організаційно-правових засад упровадження алгоритмічних рішень потребує нормативного закріплення повного життєвого циклу функціонування моделей штучного інтелекту у правоохоронних органах, що охоплює етапи їхнього розроблення, тестування, валідації та періодичного оновлення. Тож, доцільним є створення єдиного реєстру алгоритмічних систем із фіксацією версій, характеристик навчальних вибірок і результатів перевірок на упередженість та відповідність нормативним вимогам.

Крім того, забезпечення прозорості аналітичних процедур передбачає упровадження механізмів прозорості алгоритмічних рішень, які дають змогу відтворювати логіку формування ризикового оцінювання у межах контрольних і аудиторських процедур. Одночасно потребує нормативного визначення обмеження щодо використання результатів автоматизованого



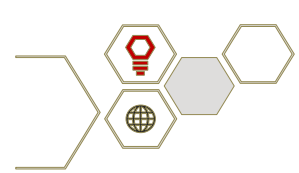
аналізу виключно як допоміжного інструменту без надання їм статусу самостійної підстави для ухвалення управлінських рішень.

Обов'язковим складником цього процесу є зниження ризику дискримінаційних викривлень, яке може бути забезпечене через процедуру регулярного незалежного аудиту даних і моделей, спрямованого на перевірку правильності вхідної інформації, стабільності прогнозних результатів і дотримання принципів недискримінаційності та правової визначеності.

Для підвищення рівня підзвітності необхідно визначити персональну відповідальність посадових осіб за використання результатів алгоритмічного аналізу та обов'язкове документування кожного випадку застосування таких систем із зазначенням підстав, контексту та мети ухваленого рішення.

Отже, упровадження запропонованих заходів сприятиме формуванню нової моделі антикорупційного моніторингу, у якій поєднуються обчислювальне оброблення великих масивів даних та нормативно затверджені вимоги до прозорості й підзвітності. Узгодження технологічних можливостей штучного інтелекту із міжнародними стандартами доброчесності дасть змогу забезпечити підвищення точності виявлення ризикових ситуацій і посилити превентивний потенціал контрольних процедур. Ефективність інтеграції таких систем вимагатиме належного правового регулювання, інституційної готовності та постійного моніторингу їхнього функціонування, що зумовлює подальші перспективи розвитку цифрових інструментів у сфері протидії корупції.

**Висновки.** Узагальнення отриманих результатів засвідчує, що упровадження алгоритмічних моделей штучного інтелекту у процеси оцінювання корупційних ризиків у діяльності правоохоронних органів підвищує аналітичну спроможність контрольних механізмів та забезпечує більш раннє виявлення потенційних порушень. Використання предикативних методів аналізу даних дає змогу ідентифікувати приховані залежності між фінансовими операціями, управлінськими рішеннями та поведінковими



індикаторами службової діяльності, що формує основу для ризико-орієнтованого моніторингу.

Доведено, що міжнародні стандарти у сфері доброчесності та регулювання штучного інтелекту визначають базові вимоги до прозорості, підзвітності та контролюваності алгоритмічних систем, які застосовуються у правоохоронному секторі. Їхнє чітке дотримання є необхідною умовою для забезпечення правової визначеності та мінімізації ризиків упереджених або помилкових рішень автоматизованих моделей.

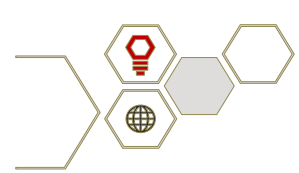
Перспективи подальших досліджень пов'язані з удосконаленням методів інтерпретації результатів алгоритмічного аналізу, розробленням уніфікованих підходів до оцінювання якості даних та розширенням інструментарію перевірки надійності прогнозних моделей у сфері антикорупційного контролю.

### Список використаних джерел

1. Тимчишин А. М. Судова експертиза як процесуальна форма використання спеціальних знань у кримінальному провадженні. *Південноукраїнський правовий часопис*. 2023. № 1. С. 228–235. DOI: <https://doi.org/10.32850/sulj.2023.1.40>

2. Тимчишин А. М. Генезис наукових уявлень про спеціальні знання у забезпеченні діяльності органів кримінальної юстиції. *Актуальні питання діяльності підрозділів кримінальної поліції*: матеріали Всеукр. наук.-практ. конф. (м. Кропивницький, 14 квітня 2023 р.). Кропивницький: ДонДУВС, 2023. С. 45–49. URL: [https://dnuvs.ukr.education/wp-content/uploads/2023/06/zbirnyk\\_materialiv\\_konferencziyi\\_ord\\_ta\\_ib\\_14\\_04\\_2023.pdf](https://dnuvs.ukr.education/wp-content/uploads/2023/06/zbirnyk_materialiv_konferencziyi_ord_ta_ib_14_04_2023.pdf) (дата звернення: 31.03.2026).

3. Бідзіля Ю. М., Шаркань В. В., Цвіклінський М. В. Медіаправо як інструмент захисту прав громадян у боротьбі з корупцією. *Український*



політико-правовий                      дискурс.                      2025.                      № 8.                      DOI:  
<https://doi.org/10.5281/zenodo.14843295>

4. Удовенко Ж. В., Галаган В. І., Шкелебей В. А. Використання штучного інтелекту у кримінальних процесах під час воєнного стану. *Law and Safety*. 2025. Т. 3, № 98. С. 78–90. DOI: <https://doi.org/10.32631/pb.2025.3.07>

5. Губанова Т. О. Використання штучного інтелекту в діяльності органів публічної влади: адміністративно-правове регулювання. *Київський юридичний журнал*. 2025. № 8. С. 13–20. DOI: <https://doi.org/10.32782/klj-2025-8.02>

6. Демідонт Б. О. Штучний інтелект у судовій системі: осмислення правового поля. *Аналітично-порівняльне правознавство*. 2025. Т. 1, № 6. С. 53–58. DOI: <https://doi.org/10.24144/2788-6018.2025.06.1.7>

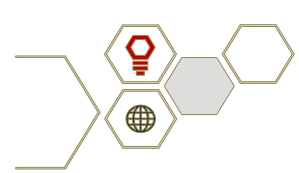
7. Басиста І. В., Удовенко Ж. В., Кулинич М.-М. А. Огляд тенденцій щодо штучного інтелекту та його перспективність для процесуальних рішень у перебігу кримінального провадження. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. Т. 3, № 81. С. 19–38. DOI: <https://doi.org/10.24144/2307-3322.2024.81.3.3>

8. Белов Д. М., Белова М. В. Штучний інтелект у судових процесах і судових рішеннях: потенціал і ризики. *Ужгородський національний університет. Серія: Право*. 2023. Т. 2, № 78. С. 315–320. DOI: <https://doi.org/10.24144/2307-3322.2023.78.2.50>.

9. Köbis N., Starke C., Rahwan I. Artificial intelligence as an anti-corruption tool (AI-ACT): potentials and pitfalls for top-down and bottom-up approaches. *arXiv preprint*. 2021. DOI: <https://doi.org/10.48550/arXiv.2102.11567>

10. Dumchikov M., Maletova O. Generative artificial intelligence systems in the fight against corruption: potential, threats and prospects for Ukraine. *International Journal of Criminology and Sociology*. 2025. Vol. 14. P. 106–115. DOI: <https://doi.org/10.6000/1929-4409.2025.14.10>

11. Casaburo D., Marsh I. Ensuring fundamental rights compliance and trustworthiness of law enforcement AI systems: the ALIGNER fundamental rights



impact assessment. *AI and Ethics*. 2024. Vol. 4. P. 1569–1582. DOI: <https://doi.org/10.1007/s43681-024-00560-0>

12. Sachoulidou A. Harnessing AI for law enforcement: solutions and boundaries from the forthcoming AI Act. *Computer Law & Security Review*. 2024. Vol. 15, № 2. DOI: <https://doi.org/10.1177/20322844241260114>

13. Söderlund K., Larsson S. Enforcement design patterns in EU law: an analysis of the AI Act. *Digital Society*. 2024. Vol. 3. Art. 41. DOI: <https://doi.org/10.1007/s44206-024-00129-8>

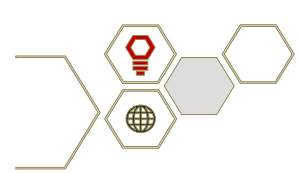
14. Golpayegani D., Hupont I., Panigutti C., Pandit H. J., Schade S., O’Sullivan D., Lewis D. AI cards: towards an applied framework for machine-readable AI and risk documentation inspired by the EU AI Act. *arXiv preprint*. 2024. DOI: <https://doi.org/10.48550/arXiv.2406.18211>

15. Park P. S., Goldstein S., O’Gara A., Chen M., Hendrycks D. AI deception: a survey of examples, risks, and potential solutions. *arXiv preprint*. 2023. DOI: <https://doi.org/10.48550/arXiv.2308.14752>

16. United Nations Convention against Corruption (UNCAC): international document. *United Nations Office on Drugs and Crime*. URL: <https://www.unodc.org/unodc/en/corruption/uncac.html> (дата звернення: 31.03.2026).

17. Anti-corruption and integrity. *Organisation for Economic Co-operation and Development*. URL: <https://www.oecd.org/gov/ethics/public-integrity.htm> (дата звернення: 31.03.2026).

18. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). *EUR-Lex*. URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (дата звернення: 31.03.2026).



19. OECD AI Principles overview. *Organisation for Economic Co-operation and Development*. URL: <https://oecd.ai/en/ai-principles> (дата звернення: 31.03.2026).

20. Council of Europe and Artificial Intelligence. *Council of Europe*. URL: <https://www.coe.int/en/web/artificial-intelligence> (дата звернення: 31.03.2026).

21. The FATF Recommendations. *FATF*. URL: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html> (дата звернення: 31.03.2026).