УДК 343.9:343.13:004.8
DOI: https://doi.org/10.31359/1993-0909-2025-32-3-300

Валерій Петрович Кононенко
Кафедра міжнародного права
Навчально-науковий інститут права
Державного податкового університету
Ірпінь, Україна

Кафедра міжнародних відносин, міжнародної інформації та безпеки
Харківський національний університет імені В. Н. Каразіна
Харків, Україна

Олександр Володимирович Діденко
Державний податковий університет
Ірпінь, Україна

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПРЕВЕНТИВНОГО ВИЯВЛЕННЯ КРИМІНАЛІСТИЧНИХ РИЗИКІВ У СФЕРІ ПІДПРИЄМНИЦТВА: МІЖДИСЦИПЛІНАРНИЙ ПІДХІД

Анотація. *У статті проаналізовано актуальні виклики кримінально-правовій протидії злочинності в сфері підприємництва в умовах цифровізації. Встановлено, що традиційні методи правоохоронної діяльності недостатньо ефективні для попередження нових форм економічних правопорушень. Метою дослідження є обґрунтування доцільності впровадження інструментів штучного інтелекту (далі – ШІ) у кримінально-правову практику для виявлення кримінологічних ризиків. У дослідженні використано системний, порівняльно-правовий і метод, метод моделювання. Представлено концептуальний апарат, зокрема поняття «цифровий профіль суб'єкта господарювання» та «превентивне виявлення кримінологічних ризиків». Розглянуто потенційне застосування концепції «predictive policing», водночас акцентовано на її суперечності з основоположними засадами кримінального процесу – презумпцією невинуватості, індивідуалізацією відповідальності та забороною об'єктивного інкримінування. На підставі результатів аналізу розроблено алгоритм превентивного виявлення кримінологічних ризиків у підприємницькій діяльності. Його етапами є: збирання релевантних даних, алгоритмічна обробка з використанням технологій машинного навчання, формування індексу ризику та надання рекомендацій для реагування з боку держави. Показано, що, на відміну від індивідуального прогнозування, превентивна аналітика не є підставою для притягнення до відповідальності, а виступає орієнтиром для подальших попереджувальних дій. Поняття «превентивне виявлення кримінологічних ризиків у підприємництві» визначено як системний процес виявлення, аналізу й оцінки потенційно загрозливих правових, економічних і фактичних умов у діяльності суб'єктів господарювання, що можуть свідчити про ризик учинення кримінальних правопорушень з метою своєчасного попередження, локалізації*

або нейтралізації в межах кримінально-правового реагування. У висновках обґрунтовано, що впровадження інноваційних цифрових технологій у кримінально-правову політику має базуватися на засадах правової визначеності, алгоритмічної прозорості та недопущення порушення прав людини. Запропоновано напрями вдосконалення нормативного регулювання та створення правового режиму для аналітичної інформації, сформованої із застосуванням ШІ.

Ключові слова: *кримінально-правова протидія, цифровізація, штучний інтелект, превентивна аналітика, прогнозування злочинності, цифровий профіль, кримінологічні ризики.*

Valerii P. Kononenko

Department of International Law
Educational and Scientific Law Institute
State Tax University
Irpin, Ukraine

Department of International Relations,
International Information and Security
V. N. Karazin Kharkiv National University
Kharkiv, Ukraine

Oleksandr Didenko

State Tax University
Irpin, Ukraine

USING ARTIFICIAL INTELLIGENCE FOR THE PREVENTIVE DETECTION OF FORENSIC RISKS IN ENTREPRENEURSHIP: AN INTERDISCIPLINARY APPROACH

Abstract. *This article presents a comprehensive study of innovative methods of criminal law counteraction to crime in the sphere of entrepreneurship under the conditions of the digitalization of the legal system. Particular attention is paid to the integration of modern information technologies, especially artificial intelligence (AI) tools, into the activities of law enforcement agencies for the purposes of preventing, detecting, and investigating economic offenses. The paper emphasizes the application of the concept of «predictive policing,» which involves the use of machine learning algorithms to generate criminological risk models and identify potentially harmful entrepreneurial activity before a crime is committed. The study also addresses the issue of legal admissibility of AI-generated analytical results in criminal proceedings. It highlights the potential risks associated with erroneous conclusions of neural networks (so-called «AI hallucinations») and the difficulties of legal assessment of outcomes generated by opaque algorithms (the «black box» effect). The necessity of developing normative legal mechanisms is substantiated, which would establish criteria for the admissibility, reliability, and verification of analytical information generated with the involvement of artificial intelligence. The article*

concludes that the system of «predictive policing» – i.e., the implementation of technologies for preventive surveillance aimed at forecasting future crimes and individuals potentially capable of committing them, as well as forming profiles of such persons and potential victims – does not comply with the principles of criminal procedural law of Ukraine. In particular, this model contradicts the prohibition of objective imputation – that is, the inadmissibility of holding a person criminally liable for actions or consequences not resulting from their conscious intent or will. Proactive criminal procedural responses based solely on algorithmic forecasting without the commission of a criminal offense violate the presumption of innocence, the principle of individualized responsibility, and the right to a fair trial. At the same time, the aforementioned concerns do not preclude the application of preventive identification of criminogenic risks in the entrepreneurial sphere. Unlike individual behavior prediction, preventive risk identification involves the assessment of business activities based on objectively available indicators – such as anomalies in financial flows, an unusual frequency of changes in beneficial ownership, or suspicious participation in tenders. Such analysis does not constitute grounds for criminal prosecution but serves as a tool for preliminary detection of circumstances that may indicate the commission of a criminal offense.

Keywords: *criminal law counteraction to crime, artificial intelligence, algorithm for preventive identification of criminogenic risks, predictive policing.*

ВСТУП

У сучасних умовах стрімкого розвитку цифрових технологій традиційні методи кримінально-правової протидії злочинності виявляються недостатньо ефективними, особливо в такій динамічній сфері, як підприємництво. Злочинність у цій галузі все частіше набуває латентних, мережевих і транскордонних форм, що ускладнює її своєчасне виявлення та реагування з боку держави. Особливу актуальність набуває необхідність зміщення акцентів із реактивного реагування на превентивне виявлення криміналістичних ризиків. У зв'язку з цим постає потреба в упровадженні інноваційних цифрових рішень, зокрема технологій штучного інтелекту, для прогнозування злочинної поведінки й оцінки потенційної небезпеки суб'єктів господарювання.

Однак існує низка теоретичних і практичних проблем, що стримують реалізацію такого підходу: від відсутності усталеного понятійного апарату (наприклад, «цифровий профіль суб'єкта господарювання», «превентивна ідентифікація криміналістичних ризиків») до неврегульованості правового статусу алгоритмічних висновків ШІ у кримінальному процесі. Додатково ускладнює ситуацію недостатня прозорість (ефект «чорної скриньки») та ризики «галюцинацій» ШІ, що ставить під сумнів достовірність таких прогнозів як підстав для кримінально-правового реагування. Отже, нагальною є потреба в розробці концептуальних і нормативних засад застосування цифрових технологій, зокрема штучного інтелекту, у системі кримінальної юстиції з урахуванням вимог законності, прав людини та принципів кримінального процесу.

Метою статті є обґрунтування доцільності використання сучасних цифрових технологій, зокрема інструментів штучного інтелекту, для прогнозування,

виявлення та запобігання злочинності у сфері підприємництва в межах кримінально-правової протидії.

Цілі статті: проаналізувати концепцію «predictive policing», сформувати понятійний апарат для аналізу ризиків у господарській діяльності, зокрема через введення категорій «цифровий профіль суб'єкта господарювання», «превентивна ідентифікація криміналістичних ризиків у сфері підприємництва», запропонувати алгоритм превентивної ідентифікації криміналістичних ризиків суб'єктів господарювання.

Наукова новизна роботи. Уперше обґрунтовано відмінність між неприйнятною в умовах українського кримінального процесу практикою «predictive policing» і допустимою моделлю превентивної ідентифікації криміналістичних ризиків у сфері підприємництва, яка ґрунтується на аналізі об'єктивно доступних даних і не порушує презумпції невинуватості;

– запропоновано авторське визначення поняття «цифровий профіль суб'єктів господарювання» як структурованого масиву даних, що відображає економічну активність, фінансову поведінку, ділову репутацію та ризики правопорушень;

– визначено зміст категорії «превентивна ідентифікація криміналістичних ризиків у сфері підприємництва» як системного процесу виявлення потенційно небезпечних обставин із метою своєчасного реагування в межах кримінального права;

– оґрунтовано концептуальне розмежування між превентивною ідентифікацією криміналістичних ризиків та алгоритмічним прогнозуванням злочинів, з урахуванням принципів кримінального процесу, зокрема презумпції невинуватості, індивідуалізації відповідальності та допустимості доказів.

1. МАТЕРІАЛИ ТА МЕТОДИ

У процесі наукового дослідження інноваційних методів кримінально-правової протидії злочинності у сфері підприємництва було застосовано комплекс загальнонаукових, спеціально-юридичних та міждисциплінарних методів, які дозволили отримати обґрунтовані результати. Основною дослідницькою базою виступили нормативно-правові акти України та міжнародні договори, рекомендації міжнародних організацій, а також приклади функціонування алгоритмічних систем у правоохоронній діяльності зарубіжних країн. Емпіричну основу становив аналіз сучасних прикладів використання штучного інтелекту в правоохоронній діяльності.

Для забезпечення наукової достовірності результатів було використано метод *системного аналізу* – для структурування понять «цифровий профіль суб'єкта господарювання», «превентивна ідентифікація криміналістичних ризиків»; *формально-логічний* метод – для обґрунтування алгоритмічної послідовності дій щодо оцінювання криміногенного ризику; *порівняльно-правовий* – для аналізу зарубіжного досвіду в сфері застосування «predictive policing» та оцінки його сумісності

з українським законодавством; метод моделювання – при розробці структури цифрового профілю підприємства та побудові алгоритму виявлення ризиків.

Особливу увагу приділено використанню технологій машинного навчання, що дозволили сформулювати принципову модель криміналістичного ризик-індексу з урахуванням багатофакторного впливу. Було проведено умовне тестування роботи зазначеного алгоритму на змодельованих прикладах фінансової діяльності підприємств із відкритих джерел (наприклад, публічні тендери, судові реєстри, бази податкових порушень), що дозволило оцінити валідність аналітичного підходу.

Метод аналізу змісту використовувався для вивчення публікацій, що стосуються проблеми допустимості аналітичних висновків, сформованих ШІ в кримінальному процесі, зокрема щодо поняття «галюцинацій ШІ» і «ефекту чорної скриньки».

Всі етапи дослідження відповідають вимогам відтворюваності, що забезпечує можливість подальшої апробації запропонованого алгоритму іншими науковцями або в межах експериментального впровадження в органах кримінальної юстиції.

2. РЕЗУЛЬТАТИ ТА ОБГОВОРЕННЯ

Традиційна модель протидії злочинності зводилася шляхом реагування правоохоронних органів на протиправні дії правопорушника та окремих заходів запобігання. Однак світ зазнає швидких трансформацій, і забезпечення його сталого розвитку вже неможливе без системної глобальної інформатизації [14, с. 354], у тому числі й у правоохоронній сфері. Стрімкий розвиток технологій зумовлює пріоритетність превентивного підходу протидії злочинності, а саме – ідентифікації осіб або груп, які потенційно можуть стати правопорушниками до моменту вчинення правопорушення, що визначається терміном «predictive policing» – «прогнозний поліцейський нагляд». Для ефективного впровадження системи превентивного нагляду важливим є окреслення основних напрямів її застосування. Ця система повинна забезпечувати прогнозування як майбутніх злочинів, так і осіб, здатних їх учинити; формування профілів таких осіб та потенційних жертв.

Таким завданням щодо прогнозування, запобігання та виявлення злочинів відповідають можливості штучного інтелекту. Так, система Zero Trust, розроблена Академією наук Китаю, дозволяє виявляти підозрілі транзакції, пов’язані з незаконним відчуженням або набуттям майна, незаконним будівництвом [див.: 1, с. 32]. Прискорення технічного прогресу не лише наближає людство до пророкованої ери технологічної сингулярності, а й постійно збільшує пов’язані з цим криміногенні ризики [Див.: 20, с. 173–174]. Застосування штучного інтелекту для прогнозування злочинів уже показало свою ефективність. Так, згідно зі статистикою після впровадження відповідних технологій у деяких містах рівень злочинності знизився. Наприклад, у британському графстві Кент насильницькі злочини зменшилися на 6% лише за чотири місяці після запровадження програми PredPol.

У місті Санта-Круз (штат Каліфорнія, США) рівень збройних пограбувань знизився на 19%, а кількість крадіжок – на 4% за півроку. Загалом у містах, де використовуються технології алгоритмічного прогнозування, загальний рівень злочинності впав на 35% у порівнянні з тими, де такі технології не застосовуються. Як наслідок, у США стрімко зростає кількість поліцейських підрозділів, що використовують методи предиктивної аналітики: з 2016 року їх налічується вже понад 50, і більшість північноамериканських країн, найімовірніше, у найближчому майбутньому будуть спиратися саме на ці технології. Особливо це актуально у боротьбі зі злочинами «білих комірців» [3, с. 344].

Основна ідея полягає у використанні можливостей аналізу й обробки значних обсягів інформації за допомогою технологій штучного інтелекту. Це дозволяє формувати обґрунтовані прогнози для оптимізації використання наявних ресурсів та ефективного виконання поліцейських функцій. Формування й розвиток криміналістичних знань, упровадження інновацій і новітніх технологій стають відповіддю на виклики сьогодення, зокрема на появу нових способів і механізмів злочинної діяльності під впливом сучасних тенденцій розвитку науки і техніки [19, с. 360]. На переконання О. Юхна, криміналістика має працювати на прогнозування та запобіганням можливим злочинам у найближчому майбутньому [21, с. 52].

Розробка та застосування таких технологій у правоохоронній діяльності для протидії злочинності може здійснюватися за такими напрямами: 1) забезпечення інформаційно-аналітичної підтримки правоохоронної діяльності; 2) надання інформаційно-довідкової підтримки правоохоронним органам; 3) розробка спеціалізованих інформаційних інтелектуальних систем для оперативно-розшукової роботи; 4) формування відомчих спеціалізованих інтелектуальних інформаційних систем [2, p. 135–140]. Тим більше, що області криміналістики, інструменти ШІ активно використовуються з метою генерації та видачі експертних оцінок [22, с. 72].

Звісно, доцільно розглянути й антикриміногенний потенціал участі громадян у запобіганні злочинності [9, с. 135], але сучасні технології дають змогу більш ефективно автоматизовано прогнозувати ймовірність правопорушення за допомогою алгоритмічного аналізу [3, с. 342].

На думку В. Оболенцева, робота в напрямі системного аналізу запобігання злочинності має здійснюватися за загальноприйнятими етапами системного підходу [15, с. 138–139]. На першому етапі в рамках підготовчих процедур формального характеру необхідно визначити аналітичну позицію дослідника, окреслити цілі функціонування системи, її межі та зовнішнє середовище, а також сформулювати основну проблему, контекст її розгляду, загальну мету та завдання системного аналізу. Другий етап передбачає збирання й опрацювання інформації про об’єкт аналізу. На основі зібраних даних формується модель системи запобігання злочинності та розробляються практичні рекомендації для усунення виявлених проблем і підвищення ефективності відповідних заходів [15, с. 160].

Інноваційні цифрові інструменти дозволяють запобігати злочинам на ранніх етапах – під час формування злочинного умислу, підготовки чи замаху на правопорушення – шляхом моделювання потенційної поведінки конкретних осіб, що забезпечує розробку обґрунтованих прогнозів якісних і кількісних показників злочинності [18, с. 134–138].

Технологія прогнозованої поліцейської діяльності визначається як програмне забезпечення, що використовується для передбачення ситуацій або тенденцій щодо злочинності, включаючи характеристики або профіль будь-якої особи (осіб), яка може вчинити злочин, місця або частоту злочинів, або особу (осіб), на яку вплине прогнозований злочин [4].

Для кримінально-правової протидії злочинності в сфері підприємництва слід створювати цифровий профіль суб'єктів господарювання, тобто сукупність даних та інформації, що характеризують суб'єкт у цифровому просторі. Цей профіль охоплює різноманітні дані, зібрані з різних джерел, служить для ідентифікації суб'єкта в електронних системах [8] та прогнозування його активності. Поняття «цифровий профіль суб'єктів господарювання» для мети «predictive policing» слід розуміти як структурований масив цифрових даних про юридичну або фізичну особу-підприємця, сформований на основі автоматизованої обробки інформації з відкритих, спеціалізованих та оперативних реєстрів, який відображає комплексну характеристику господарської діяльності, фінансової поведінки, ділової репутації, зв'язків із іншими суб'єктами та потенційних ризиків правопорушень.

Такий профіль може включати:

– ідентифікаційні дані (назва, код, адреса, КВЕДи, дата реєстрації);

– власників, керівництво та пов'язані особи;

– інформацію про участь у публічних закупівлях, судових спорах, податковій історії;

– аналіз зв'язків із іншими компаніями (включно з офшорами, ФОПами, фіктивними структурами);

– індикатори ризику (наявність ознак фіктивності, тендерних змов, аномальних фінансових потоків тощо);

– оцінку надійності, ризик-індекс та прогноз потенційної кримінальної активності (за результатами алгоритмів штучного інтелекту).

Звісно збільшення позицій профілю збільшує коректність висновків. Натомість питання надійності та точності висновків, сформованих штучним інтелектом, залишається надзвичайно актуальним. Результати, які генерують нейронні мережі, потребують критичної оцінки, оскільки такі системи здатні створювати недостовірні відомості, вигадані факти або помилкові формулювання. Це явище, відоме як марення (галюцинації) ШІ. І воно настільки поширене, що відповідний термін був визнаний словом 2023 року за версією Кембриджського словника. Як зазначають представники Словника, здатність ШІ «галюцинувати» підкреслює

необхідність збереження критичного мислення під час використання таких технологій [17].

Причинами такого явища можуть бути як обмеження навчальної вибірки, так і особливості побудови математичних моделей, які формують висновки на основі ймовірнісних припущень, а не об'єктивних фактів. Штучний інтелект, не маючи власного критичного мислення й емпіричного досвіду, не здатен відрізнити достовірну інформацію від хибної або суперечливої. Більш того, у разі відсутності достатньої кількості даних чи контексту система може генерувати некоректні пояснення або висновки, що виглядають логічно обґрунтованими, але насправді є помилковими.

Також алгоритми, запатентовані приватними компаніями й покладені в основу «передбачуваного поліцейського нагляду», нагадують «чорну скриню» (blackboxing) і зі зростанням складності технологій результати їхнього застосування можуть ставати дедалі менш прозорими та більш неоднозначними [7, с. 112]. Така непрозорість алгоритмів має ефект «чорної скриньки» (коли можна бачити, що входить і що виходить, але її внутрішня робота прихована або оповита таємницею) [6].

Щодо правомірності використання штучного інтелекту для прогнозування злочинів, то попри ризики, пов'язані з можливим порушенням конституційного права на захист персональних даних, вони можуть бути мінімізовані за умови, що законодавець установить кримінально-правові гарантії захисту таких даних, та врегулює процедуру використання відповідних технологій [3, с. 342].

М. Демура стверджує, що технології прогнозування злочинів на основі ШІ, на відміну від запобіжних заходів, не обмежують прав чи свобод людини, не накладають санкцій, не мають карального характеру. Їх роль – інформаційна, попереджувальна, що повністю відповідає природі слідчих дій (дій зі збирання доказів). Напрям використання ШІ з метою попередження кримінальних правопорушень реалізується шляхом застосування численних інформаційних засобів для запобігання вчиненню злочинних діянь [10, с. 25]. На підставі викладених аргументів слід дійти висновку, що використання систем штучного інтелекту для прогнозування злочинів у сфері підприємництва є цілком правомірним та доцільним. Воно повинно підпадати під правовий режим дозволених заходів розшукового або аналітичного характеру, які відповідають нормам кримінального процесуального права й не суперечать конституційним правам громадян, міжнародним договорам України, зокрема, Європейській конвенції про захист прав людини і основоположних свобод [12] (яка вже є частиною національного законодавства [13, с. 97–98]), але з погляду системи кримінального провадження слід визнати, що використання таких технологій не повинно мати характеру слідчих дій, більш того використання алгоритмічного прогнозування злочинів у практиці досудового розслідування несумісне з принципом законності, презумпцією невинуватості та правом на захист [3, с. 348–349], тому отримані дані не можуть бути визнані доказами.

У контексті обговорення впливу штучного інтелекту на сферу протидії злочинності доцільно виокремити такі дискусійні положення, запропоновані М. В. Карчевським:

– початковою передумовою для наукової дискусії щодо використання штучного інтелекту в механізмах протидії злочинності має слугувати об'єктивна оцінка реального стану розвитку відповідних технологій;

– аналіз впливу сучасних інструментів штучного інтелекту на систему кримінальної юстиції доцільно здійснювати в трьох основних вимірах: а) поява нових форм злочинної поведінки; б) трансформація діяльності правоохоронних і судових органів;

– використання елементів штучного інтелекту в правоохоронній та судовій діяльності об'єктивно обмежене через особливості принципів його функціонування;

– запровадження національних інструментів штучного інтелекту в сфері протидії злочинності має розпочинатися зі створення інтегрованої системи інформаційного забезпечення кримінально-правового регулювання [11, с. 41].

Ми вважаємо, що впровадження ШІ у сфері протидії злочинності повинно базуватися на поєднанні інституційних механізмів контролю, законодавчої регламентації та етичних обмежень, а не лише на технологічному прогресі. Лише при такому підході можливо забезпечити баланс між інноваціями та фундаментальними гарантіями кримінального процесу.

Постає також питання: наскільки законним є алгоритмічне прогнозування злочинів, яке передбачає збір та обробку персональних даних громадян та інформацію щодо юридичних осіб, які здійснюють підприємницьку діяльність (а також аналіз коректності здійснення такої діяльності – наприклад, щодо банківських транзакцій (без розкриття власника рахунку та отримувача коштів, що не буде мати ознак порушення банківської таємниці).

Відповідно до ст. 5 Закону України «Про доступ до публічної інформації» до інформації з обмеженим доступом не відноситься інформація про отримання фізичною особою бюджетних коштів, державного чи комунального майна в будь-якій формі, а також відомості про структуру, принципи формування й розмір оплати праці, винагороди чи додаткових благ керівників, їхніх заступників, членів наглядових рад юридичних осіб публічного права, державних чи комунальних підприємств або організацій, що мають на меті отримання прибутку, а також осіб, які постійно чи тимчасово займають посади у виконавчих органах або входять до наглядових рад господарських товариств, у яких понад 50% акцій (часток, паїв) прямо чи опосередковано належать державі або територіальній громаді, за винятком деяких випадків, визначених ст. 6 Закону [16]. Тому з урахуванням більш м'яких обмежень на збір інформації щодо діяльності суб'єктів господарювання та необхідності кримінально-правової протидії злочинності у сфері підприємництва можна говорити про

можливість превентивної ідентифікації криміналістичних ризиків у сфері підприємництва.

Адаптація концепції «predictive policing» до підприємницького середовища дозволяє виявляти потенційні економічні злочини шляхом аналізу аномальної ділової активності/бездіяльності, інших маркерів, що вказують на наявність ризиків учинення кримінального правопорушення. Такий підхід сприяє впровадженню проактивного реагування державних органів через інструменти позапланового контролю або оперативно-розшукових дій у разі встановлення високого рівня ризику.

Категорію превентивної ідентифікації криміналістичних ризиків у сфері підприємництва слід розуміти як процес системного виявлення, аналізу й оцінювання потенційно небезпечних юридичних і фактичних обставин у діяльності суб'єктів господарювання, які можуть свідчити про ймовірність вчинення кримінальних правопорушень або створювати умови для їх вчинення з метою своєчасного запобігання, локалізації або нейтралізації таких ризиків у межах кримінально-правового реагування.

Цей процес може здійснюватися з використанням методів кримінального аналізу, правової аналітики, а також сучасних цифрових технологій (у т.ч. штучного інтелекту) з урахуванням вимог матеріального та процесуального права.

З метою використання методів сучасних цифрових технологій для цілей превентивної ідентифікації криміналістичних ризиків у сфері підприємництва формується повний цифровий профіль суб'єкта господарювання (та пов'язаних із ним осіб/структур), який стає базою для подальшого аналізу криміналістичних ризиків на наступних етапах алгоритму.

Таким чином, алгоритм превентивної ідентифікації криміналістичних ризиків у сфері підприємництва може виглядати наступним чином:

I. Збір і систематизація релевантних даних

1. Інтеграція відкритих та закритих державних реєстрів

– податкові дані, реєстр юридичних осіб, тендерні платформи, судові рішення, митні декларації, фінансові звіти;

– дані про пов'язаних осіб, історії змін засновників, частоту перереєстрацій, змін адреси.

2. Використання цифрових джерел непрямої аналітики

– інформація з публічних API банків, дані з бірж, соціальні профілі, мас-медіа;

– телеметричні дані (трафік транзакцій, аномалії у витратах, нетипові транзакційні маршрути).

3. Попередня обробка інформації (1-й фільтр)

– видалення повторів, узгодження форматів, структурування для введення в AI-модель;

– уточнення ідентичностей через автоматизовану звірку імен, кодів, адрес.

II. Аналітична обробка даних за допомогою ШІ

1. Моделювання ризиків із використанням машинного навчання

– створення класифікаційних моделей на основі історичних кейсів злочинної діяльності;

– визначення ймовірності скоєння економічного правопорушення для конкретного підприємства.

2. Виявлення аномалій (антифрод-механізми)

– застосування алгоритмів типу Isolation Forest, K-Means для виявлення поведінкових відхилень;

– автоматичне маркування підозрілих схем.

3. Оцінка ступеня ризику за шкалою ризик-індексу

– присвоєння рейтингу ризику компаніям (від «низький» до «високий») з урахуванням об'єктивних факторів;

– побудова heat map секторів або регіонів із підвищеною концентрацією ризиків.

ІІІ. Превентивне реагування

1. Автоматичне створення аналітичного звіту на основі ризик-оцінки

Результати обробки даних ШІ-моделлю формалізуються у вигляді структурованого аналітичного висновку, який включає:

– коротку характеристику суб'єкта господарювання;

– тип виявленого ризику (наприклад, ознаки фіктивності, узгоджених тендерних дій, необґрунтованого зростання активності в офшорних юрисдикціях);

– рівень ризику за шкалою: низький / середній / високий / критичний;

– перелік параметрів, що вплинули на присвоєння ризик-індексу.

2. Рекомендація щодо реагування державних органів залежно від рівня ризику

– середній ризик – рекомендації про направлення інформації до контролюючого органу (наприклад, ДПС, ДАСУ, АМКУ) для проведення позапланової документальної перевірки за наявності правових підстав;

– високий або критичний ризик – рекомендації про направлення даних до органів досудового розслідування або оперативно-розшукової діяльності в якості оперативної аналітичної інформації.

З урахуванням позицій наведеного алгоритму пропонуються наступні зміни до законодавства:

1) до п. 78.1.1 ПКУ:

78.1. Документальна позапланова перевірка здійснюється за наявності хоча б однієї з таких підстав:

78.1.1 отримано… **дані про ймовірне порушення податкового законодавства**;

2) до ч. 1 ст. 6 Закону України «Про основні засади державного нагляду (контролю)»:

1. Підставами для здійснення позапланових заходів є:

– **отримання обґрунтованої інформації про порушення вимог законодавства.**

Такий алгоритм із відповідними змінами до законодавства дозволить ефективно застосовувати сучасні технології для кримінально-правової протидії злочинності у сфері підприємництва.

Питання щодо підстави для внесення результатів використання алгоритму ШІ до ЄРДР згідно з ч. 1 ст. 214 КПК України або для ініціювання проведення оперативно-розшукових заходів для попередження, своєчасного виявлення й припинення кримінальних правопорушень згідно зі ст. 7 ЗУ «Про оперативно-розшукову діяльність» – залишається дискуційним.

Дискуційним також є питання, чи слід результат використання алгоритму ШІ розглядати на рівні інформації, що є підставою для превентивного реагування (і не є доказом як така) чи він потребує процесуального оформлення. Останнє з урахуванням відсутності відповідного законодавчого регулювання, а також проблем «чорної скрині» та «марення штучного інтелекту» на існуючому етапі технологічного контролю роботи алгоритмів ШІ та законодавчого врегулювання уявляється спірним.

*Обговорення***.** Проведене дослідження підтверджує, що сучасні цифрові інструменти, зокрема штучний інтелект, здатні трансформувати підходи до кримінально-правової протидії злочинності у сфері підприємництва. Запропонований алгоритм превентивної ідентифікації криміналістичних ризиків є прикладом впровадження принципів «predictive analytics» у юридичну практику, що відповідає загальносвітовим тенденціям переходу до проактивної моделі правозастосування. Такий підхід також узгоджується з висновками дослідників, зокрема Chukaieva і Matulienė [1], які вказують на ефективність інтелектуального аналізу даних у правоохоронній діяльності. Однак обґрунтовані побоювання викликають етичні, правові та технологічні аспекти використання алгоритмів ШІ. Насамперед, ідеться про проблему прозорості алгоритмів («ефект чорної скриньки») та ймовірність генерування хибних висновків («галюцинації ШІ»), що прямо впливають на допустимість і достовірність зібраної інформації в кримінальному процесі. Це співвідноситься з позицією М. В. Карчевського [11], який наголошує на потребі чіткого нормативного регулювання використання штучного інтелекту в межах кримінальної юстиції.

Окрему увагу заслуговує правова оцінка можливості використання таких прогнозів як підстави для позапланових перевірок чи оперативно-розшукових заходів. Згідно з чинним законодавством така інформація може кваліфікуватися як оперативна аналітика, але не як доказ. Це свідчить про потребу в удосконаленні законодавства, зокрема Кодексу України про адміністративні правопорушення, Податкового кодексу України, а також Закону України «Про оперативно-розшукову діяльність».

На думку автора, розмежування між допустимістю аналітичних даних для ініціювання перевірки та їх використанням у доказуванні є критично важливим. З огляду на висновки Elsherif [3], важливо встановити правовий режим, який до-

зволяє використання ШІ в запобіганні злочинам, не порушуючи принцип презумпції невинуватості та права на захист.

Нарешті, особливістю підприємницької діяльності є її динамічність, що вимагає адаптивних правових інструментів. Запровадження «цифрових профілів суб'єктів господарювання» як елементу превентивної аналітики створює підґрунтя для персоніфікованого моніторингу правопорушень у бізнес-середовищі, що відповідає рекомендаціям М. Демури [10] й О. О. Юхно [21] щодо цифровізації кримінального процесу.

Таким чином, результати дослідження демонструють потенціал інноваційного підходу до запобігання злочинності в економічному секторі, одночасно підкреслюючи необхідність міждисциплінарного діалогу між юристами, ІТ-фахівцями та законодавцями для формування ефективної й правомірної моделі застосування штучного інтелекту в кримінальному праві.

ВИСНОВКИ

Система «predictive policing» – «прогнозний поліцейський нагляд», яка передбачає впровадження технологій превентивного нагляду з метою прогнозування як майбутніх злочинів, так і осіб, здатних їх учинити, а також формування профілів таких осіб і потенційних жертв, не відповідає принципам кримінального процесуального законодавства України. Зокрема, така модель суперечить забороні об'єктивного інкримінування – недопущенню притягнення особи до кримінальної відповідальності за дії або наслідки, які не є результатом її свідомого волевиявлення та наміру. Кримінально-процесуальне проактивне реагування виключно на підставі алгоритмічного прогнозу без факту вчинення кримінального правопорушення порушує презумпцію невинуватості, принципи індивідуалізації відповідальності та справедливого судового розгляду.

Водночас зазначене не суперечить здійсненню превентивної ідентифікації криміналістичних ризиків у сфері підприємництва. На відміну від індивідуального прогнозування поведінки конкретної особи, превентивна ідентифікація ризиків передбачає оцінку діяльності суб'єктів господарювання на підставі об'єктивно доступних показників – таких як аномалії у фінансових потоках, незвичайна частота змін бенефіціарів, підозріла участь у тендерах тощо. Такий аналіз не є підставою для кримінального переслідування, а лише виступає інструментом попереднього виявлення обставин, що можуть свідчити про вчинення кримінального правопорушення.

Сформульовано поняття «цифровий профіль суб'єктів господарювання», який слід розуміти як структурований масив цифрових даних про юридичну або фізичну особу-підприємця, сформований на основі автоматизованої обробки інформації з відкритих, спеціалізованих та оперативних реєстрів, який відображає комплексну характеристику господарської діяльності, фінансової поведінки, ділової репутації, зв'язків із іншими суб'єктами та потенційних ризиків правопорушень.

Надано визначення категорії «превентивна ідентифікація криміналістичних ризиків у сфері підприємництва» як процесу системного виявлення, аналізу й оцінювання потенційно небезпечних юридичних, економічних і фактичних обставин у діяльності суб'єктів господарювання, які можуть свідчити про ймовірність учинення кримінальних правопорушень з метою своєчасного запобігання, локалізації або нейтралізації таких ризиків у межах кримінально-правового реагування.

Запропоновано алгоритм превентивної ідентифікації криміналістичних ризиків у сфері підприємництва, який включає три основні етапи: (1) збір і систематизацію релевантних даних з усіх доступних джерел; (2) аналітичну обробку інформації з використанням ШІ шляхом моделювання ризиків, виявлення аномалій та присвоєння ризик-індексу; (3) превентивне реагування, що передбачає формування аналітичного висновку та рекомендації щодо подальших дій – від позапланової перевірки до передачі інформації органам досудового розслідування в разі високого або критичного рівня ризику.

Подальші дослідження доцільно зосередити на розробці нормативного регулювання використання штучного інтелекту в кримінальному процесі, зокрема щодо допустимості алгоритмічних висновків як доказів; удосконаленні цифрового профілю суб'єкта господарювання як інструменту превентивної аналітики; визначенні переліку релевантних даних для виявлення криміногенних ризиків; формуванні єдиних підходів до електронних доказів у кримінальному судочинстві; а також на вивченні й адаптації міжнародного досвіду.

ПОДЯКИ

Дякуємо доктору юридичних наук, професору, директору навчально-наукового інституту права Державного податкового університету, заслуженому юристу України за всебічну допомогу в дослідженні

КОНФЛІКТ ІНТЕРЕСІВ

Немає

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Чукайєва А., Матулєне С. Можливості застосування штучного інтелекту в роботі правоохоронних органів. *Науковий вісник Національної академії внутрішніх справ*. 2023. №28(3). С. 28–37. URL: https://doi.org/10.56215/naia-herald/3.2023.28.

[2] Baltrūnienė J., Shevchuk V. Artificial Intelligence Technologies in Law Enforcement and Justice: *Ukrainian and European experience. Digital transformation of criminal proceedings under martial law: materials of the All-Ukrainian round table* (Kharkov, December 16, 2022) ; National Law University named after Yaroslav the Wise. Kharkiv, 2022. P. 135–140.

[3] Elsherif M. The legal nature and legality of crime prediction by artificial intelligence. *AJFSFM*. 2021. №3(2). P. 341–359. URL: https://doi.org/10.26735/NGSO4969.

[4] Guariglia M. Technology Can't Predict Crime, It Can Only Weaponize Proximity to Policing. *Electronic Frontier Foundation*. 03.09.2020. URL: https://www.eff.org/deeplinks/2020/09/technology-cant-predict-crime-it-can-onlyweaponize-proximity-policing (дата звернення: 26.05.2025).
[5] Mittal N., Singh R. Criminal identification system using face detection with artificial intelligence. *In Blockchain applications for healthcare informatics: Beyond 5G*. Cambridge : Academic press, 2022. P. 421–430. URL: https://doi.org/10.1016/B978-0-323-90615-9.00001–3.
[6] Unlocking the 'Black Box' of Team Performance & Motivation. Growth Pitstop. URL: https://growthpitstop.com/2021/04/06/the-black-box-of-team-motivation/ (дата звернення: 26.05.2025).
[7] Wilson D. Algorithmic patrol: the futures of predictive policing. Big data, crime and social control. New York, 2018. P. 108–127. URL: https://doi.org/10.4324/9781315395784
[8] Васильєва Н. Що таке цифровий профіль і як він допоможе розбудувати економіку України. *ZN.UA*. 03.08.2024. URL: https://zn.ua/ukr/reforms/shcho-take-tsifrovij-profil-i-jak-vin-dopomozhe-rozbuduvati-ekonomiku-ukrajini.html (дата звернення: 26.05.2025).
[9] Громадськість у запобіганні і протидії злочинності: вітчизняний та міжнародний досвід : монографія / В. В. Голіна, М. Г. Колодяжний, С. С. Шрамко та ін. ; за заг. ред.: В. В. Голіни, М. Г. Колодяжного. Харків : Право, 2017. 284 с.
[10] Демура М. Міжнародний досвід використання алгоритмів штучного інтелекту у кримінальному провадженні. *Використання технологій штучного інтелекту у протидії злочинності* : матеріали Наук.-практ. онлайн-семінару (м. Харків, 5 листоп. 2020 р.). Харків : Право, 2020. С. 24–28.
[11] Карчевський М. В. Штучний інтелект та протидія злочинності. *Використання технологій штучного інтелекту у протидії злочинності :* матеріали Наук.-практ. онлайн-семінару (м. Харків, 5 листоп. 2020 р.). Харків : Право, 2020. С. 32–43.
[12] Конвенція про захист прав людини і основоположних свобод (з протоколами) від 04.11.1950. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 26.05.2025).
[13] Кононенко В. П. Законодавство чи закон? *Право України*. 2004. № 4. С. 96–98.
[14] Кононенко В. П., Новікова Л. В., Копицька П. О. Політика міжнародних організацій з питань інформаційної безпеки. *Науковий вісник Ужгородського національного університету. Серія Право*. 2021. № 65. Т. 1. С. 353–358. URL: https://doi.org/10.24144/2307–3322.2021.65.64
[15] Оболенцев В. Ф., Ющенко О. Г. Застосування методів штучного інтелекту у юриспруденції. *Протидія організованій злочинності і корупції :* матеріали XIX Всеукр. наук. конф. з кримінології для студентів, аспірантів та молодих вчених (м. Харків, 2 груд. 2019 р.) / за заг. ред. : А. П. Гетьмана, Б. М. Головкіна. Харків : Право, 2019. С. 138–139.
[16] Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939–17#Text (дата звернення: 26.05.2025).
[17] Чайковська В. Галюцинувати: Кембриджський словник визначив слово року. DW. 15.11.2023. URL: https://www.dw.com/uk/galucinuvati-kembridzskij-slovnik-viznaciv-slovo-roku/a-67406110 (дата звернення: 26.05.2025).
[18] Шевчук В. Проблеми застосування штучного інтелекту у правоохоронній діяльності в контексті російсько-української війни. *Правоохоронна діяльність» нової формації: напрями освітнього та наукового забезпечення :* матеріали Всеукр. наук.-пед.

підвищ. кваліф. (4 берез. – 14 квіт. 2024 р.). Львів – Торунь : Liha-Pres, 2024. С. 134–138.

[19] Шевчук В. Роль технологій штучного інтелекту у правоохоронній діяльності та забезпеченні безпеки та обороноздатності України. *Юридичний науковий електронний журнал*. 2024. №6. С. 356–361. URL: https://doi.org/10.32782/2524–0374/2024–6/88

[20] Юртаєва К. В. Deepfake: криміногенні ризики на порозі ери технологічної сингулярності. *Злочинність і протидія їй в умовах сингулярності: тенденції та інновації* : зб. тез доп. наук.-практ. конф. (м. Харків, 16 квіт. 2021 р.) / МВС України, Харків. нац. ун-т внутр. справ, Кримінол. асоц. України. Харків : ХНУВС, 2021. С. 173–174.

[21] Юхно О. О. Генезис та проблемні питання використання сучасних технологій та штучного інтелекту в криміналістиці, експертній діяльності та досудовому слідстві. *Теорія і практика судової експертизи та криміналістики*. 2023. №3(25). С. 40–59. URL : https://doi.org 10.32353/khrife.3.2021.04

[22] Яровий К. Штучний інтелект як інструмент протидії злочинності. *Юридичний вісник*. 2024. №2. С. 68–76. URL : https://doi.org/10.32782/yuv.v2.2024.9

REFERENCES

[1] Chukaieva, A., & Matulienė, S. (2023). Possibilities of applying artificial intelligence in the work of law enforcement agencies. *Scientific Journal of the National Academy of Internal Affairs*, 28(3), 28–37. Retrieved from https://doi.org/10.56215/naia-herald/3.2023.28

[2] Baltrūnienė, J., & Shevchuk, V. (2022). Artificial Intelligence Technologies in Law Enforcement and Justice: Ukrainian and European experience. In *Digital transformation of criminal proceedings under martial law: materials of the All-Ukrainian round table (Kharkiv, December 16, 2022)* (pp. 135–140). National Law University named after Yaroslav the Wise.

[3] Elsherif, M. (2021). The legal nature and legality of crime prediction by artificial intelligence. *AJFSFM*, 3(2), 341–359. Retrieved from https://doi.org/10.26735/NGSO4969

[4] Guariglia, M. (2020, September). Technology can't predict crime, it can only weaponize proximity to policing. *Electronic Frontier Foundation*. Retrieved from https://www.eff.org/deeplinks/2020/09/technology-cant-predict-crime-it-can-onlyweaponize-proximity-policing

[5] Mittal, N., & Singh, R. (2022). Criminal identification system using face detection with artificial intelligence. In *Blockchain applications for healthcare informatics: Beyond 5G* (pp. 421–430). Cambridge: Academic Press. Retrieved from https://doi.org/10.1016/B978-0-323-90615-9.00001–3

[6] Growth Pitstop. (2021, April). *Unlocking the 'Black Box' of Team Performance & Motivation.* Retrieved from https://growthpitstop.com/2021/04/06/the-black-box-of-team-motivation/

[7] Wilson, D. (2018). Algorithmic patrol: the futures of predictive policing. In *Big data, crime and social control* (pp. 108–127). New York. Retrieved from https://doi.org/10.4324/9781315395784

[8] Vasylyeva, N. (2024, August). What is a digital profile and how it can help to develop the Ukrainian economy. *ZN.UA*. Retrieved from https://zn.ua/ukr/reforms/shcho-take-tsifrovij-profil-i-jak-vin-dopomozhe-rozbuduvati-ekonomiku-ukrajini.html

[9] Holina, V. V., Kolodiazhnyi, M. H., Shramko, S. S., & et al. (2017). *The Public in the Prevention and Counteraction of Crime: Domestic and International Experience.* In V. V. Holina & M. H. Kolodiazhnyi (Eds.). Kharkiv: Pravo.

[10] Demura, M. (2020). International experience in the use of artificial intelligence algorithms in criminal proceedings. In *Use of Artificial Intelligence Technologies in Combating Crime: Proceedings of the Scientific and Practical Online Seminar (Kharkiv, November 5, 2020)* (pp. 24–28). Kharkiv.

[11] Karchevskyi, M. V. (2020). Artificial Intelligence and Crime Prevention. In *Use of Artificial Intelligence Technologies in Combating Crime: Proceedings of the Scientific and Practical Online Seminar (Kharkiv, November 5, 2020)* (pp. 32–43). Kharkiv: Pravo.

[12] Convention for the Protection of Human Rights and Fundamental Freedoms (with Protocols). (1950, November). Retrieved from https://zakon.rada.gov.ua/laws/show/995_004#Text

[13] Kononenko, V. P. (2004). Law or Legislation? *Law of Ukraine*, 4, 96–98.

[14] Kononenko, V. P., Novikova, L. V., & Kopytska, P. O. (2021). The Policy of International Organizations on Information Security. *Scientific Bulletin of Uzhhorod National University. Law Series*, 65(1), 353–358. Retrieved from https://doi.org/10.24144/2307–3322.2021.65.64

[15] Obolentsev, V. F., & Yushchenko, O. H. (2019). The Use of Artificial Intelligence Methods in Jurisprudence. In *Counteraction to Organized Crime and Corruption: Proceedings of the 19th All-Ukrainian Scientific Conference on Criminology for Students, Postgraduates and Young Scientists (Kharkiv, December 2, 2019).* In A. P. Hetman, & B. M. Holovkin (Eds.) (pp. 138–139). Kharkiv: Pravo.

[16] On Access to Public Information: Law of Ukraine (2011, January). Retrieved from https://zakon.rada.gov.ua/laws/show/2939–17#Text

[17] Chaikovska, V. (2023, November). «Hallucinate»: Cambridge Dictionary Named the Word of the Year. *DW*. Retrieved from https://www.dw.com/uk/galucinuvati-kembridzskij-slovnik-viznaciv-slovo-roku/a-67406110

[18] Shevchuk, V. (2024). Issues of Using Artificial Intelligence in Law Enforcement Activities in the Context of the Russian-Ukrainian War. In *«Law Enforcement Activity» of the New Formation: Directions of Educational and Scientific Support: Proceedings of the All-Ukrainian Scientific and Pedagogical Qualification Seminar (March 4 – April 14, 2024)* (pp. 134–138). Lviv – Torun: Liha-Pres.

[19] Shevchuk, V. (2024). The Role of Artificial Intelligence Technologies in Law Enforcement and Ensuring Ukraine's Security and Defense Capability. *Legal Scientific Electronic Journal*, 6, 356–361. Retrieved from https://doi.org/10.32782/2524–0374/2024–6/88

[20] Yurtaieva, K. V. (2021). Deepfake: Criminogenic Risks on the Threshold of the Technological Singularity Era. In *Crime and Its Counteraction in the Conditions of Singularity: Trends and Innovations: Collection of Abstracts of the Scientific-Practical Conference (Kharkiv, April 16, 2021)* (pp. 173–174). Kharkiv: KNUVS.

[21] Yukhno, O. O. (2023). Genesis and Problematic Aspects of Using Modern Technologies and Artificial Intelligence in Forensics, Expert Activity, and Pre-trial Investigation. *Theory and Practice of Forensic Science and Criminalistics*, 3(25), 40–59. Retrieved from https://doi.org/10.32353/khrife.3.2021.04

[22] Yarovyi, K. (2024). Artificial Intelligence as a Tool for Combating Crime. *Legal Bulletin*, 2, 68–76. Retrieved from https://doi.org/10.32782/yuv.v2.2024.9

Валерій Петрович Кононенко
Доктор юридичних наук
Професор кафедри міжнародного права
Навчально-науковий інститут права Державного податкового університету
08205, вул. Університетська, 31, Ірпінь, Україна

Доцент кафедри міжнародних відносин, міжнародної інформації та безпеки
Харківський національний університет ім. В. Н. Каразіна
61022, майдан Свободи 4, Харків, Україна
Email: advokatkononenko@ukr.net
ORCID: https://orcid.org/0000-0002-6461-7072

Valerii P. Kononenko
Doctor of Law
Professor at the Department of International Law
Educational and Scientific Law Institute State Tax University
08205, 31 Universytetska St., Irpin, Ukraine

Associate Professor Department of International Relations
International Information and Security
V. N. Karazin Kharkiv National University
61022, 4 Svobody Sq., Kharkiv, Ukraine

Олександр Володимирович Діденко
аспірант
Державний податковий університет
08205, вул. Університетська, 31, Ірпінь, Україна
Email: didenko.oleksandr@gmail.com
*ORCID: https://orcid.org/*0009-0005-1273-7514

Oleksandr V. Didenko
Postgraduate Student
State Tax University
08205, 31 Universytetska St., Irpin, Ukraine

Рекомендоване цитування: Кононенко В. П., Діденко О. В. Використання штучного інтелекту для превентивного виявлення криміналістичних ризиків у сфері підприємництва: міждисциплінарний підхід. *Вісник Національної академії правових наук України*. 2025. Т. 32. № 3. С. 300–318.

Suggested Citation: Kononenko, V. P., & Didenko, O. V. (2025). Using Artificial Intelligence for the Preventive Detection of Forensic Risks in Entrepreneurship: an Interdisciplinary Approach. *Journal of the National Academy of Legal Sciences of Ukraine,* 32(3), 300–318.

Стаття надійшла / Submitted: 17/06/2025
Доопрацьовано / Revised: 17/07/2025
Схвалено до друку / Accepted: 29/09/2025