УДК 343.9+004.8
DOI https://doi.org/10.24144/2788-6018.2026.01.3.14

ПРОБЛЕМИ ВПРОВАДЖЕННЯ В ДІЯЛЬНІСТЬ ПРАВООХОРОННИХ ОРГАНІВ ІНФОРМАЦІЙНИХ СИСТЕМ НА БАЗІ ШТУЧНОГО ІНТЕЛЕКТУ

Мациборська О.М.,
старший викладач кафедри цивільно-правових дисциплін
Волинського національного університету імені Лесі Українки
ORCID: 0009-0000-5971-6722

Мациборська О.М. Проблеми впровадження в діяльність правоохоронних органів інформаційних систем на базі штучного інтелекту.

Стаття присвячена аналізу проблем, пов'язаних із запровадженням у діяльність правоохоронних органів інформаційних систем на базі штучного інтелекту. Підкреслюються позитивні аспекти використання систем зі штучним інтелектом для вирішення службових завдань працівниками правоохоронних органів. Описуються напрямки застосування ШІ-систем у правоохоронній діяльності. Водночас окреслюється коло актуальних і потенційних проблем, пов'язаних із застосуванням інтелектуальних систем, які вже обслуговують правоохоронну сферу і можуть використовуватися в майбутньому. Наголошується, що системи на базі штучного інтелекту, розроблені для правоохоронців, мають високий ступінь ризику, загрожуючи реалізації і захисту прав людини. Припускається, що дії правоохоронців внаслідок використання ШІ-систем можуть не відповідати принципу пропорційності. Акцентується увага на питаннях якості ШІ-розробок і даних, на яких вони навчаються, і пов'язаних із цим проблем відповідальності і політики прозорості виробника, а також проблемах охорони інтелектуальної власності. Підкреслюється, що неприпустимим є використання невідповідних ШІ-систем у процесуальних діях, що може порушити право людини на захист і справедливий суд. Утверджується думка, що системи на базі штучного інтелекту, призначені для правоохоронних органів, мають бути точними і надійними, їхня інтелектуальна робота – прозорою, зрозумілою, безпечною. Звертається увага на необхідність розроблення високоякісних ШІ-систем з вузькою спеціалізацією, призначених допомагати правоохоронцям виконувати окремі завдання: оцінку ризиків, виявлення дезінформації, викриття дипфейків, створення профілю, для аналітики злочинів проти фізичних осіб тощо. Пропонується віднести до групи з високим ступенем ризику не тільки ШІ-системи для правоохоронних органів, правосуддя і прикордонних служб, а й розроблені для митних і податкових органів. Окреслюється проблема використанні інтелектуальних систем для боротьби зі злочинністю у метавсесвіті. Визначається як проблема відсутність у національному законодавстві нормативно-правових актів щодо регулювання впровадження і використання інформаційних систем на базі штучного інтелекту у правоохоронній діяльності та інших сферах життєдіяльності.

Ключові слова: правоохоронні органи, штучний інтелект, інформаційна система, метавсесвіт, ступінь ризику.

Matsyborska O.M. Problems of introducing information systems based on artificial intelligence into the activities of law enforcement agencies.

The article is devoted to the analysis of problems related to the introduction of information systems based on artificial intelligence into the activities of law enforcement agencies. The positive aspects of using artificial intelligence systems to solve official tasks by law enforcement officers are emphasized. The directions for the application of AI systems in law enforcement activities are described. At the same time, a range of current and potential problems related to the use of intelligent systems that already serve the law enforcement sphere and may be used in the future are outlined. It is emphasized that artificial intelligence systems developed for law enforcement officers have a high degree of risk, threatening the protection of human rights. It is assumed that the actions of law enforcement officers as a result of the use of AI systems may not comply with the principle of proportionality. The emphasis is on the issues of the quality of AI developments and the data on which they are trained, and the related problems of liability and transparency policy of the manufacturer, as well as the problems of intellectual property protection. It is emphasized that the use of inappropriate AI systems in procedural actions is unacceptable, as it may violate the human right to protection and a fair trial. The opinion is affirmed that artificial intelligence systems designed for law enforcement agencies must be accurate and reliable; their intellectual work must be transparent, understandable, and safe. Attention is drawn to the need to develop high-quality AI systems with narrow specialization, designed to help law enforcement agencies

perform certain tasks: risk assessment, detection of disinformation, detection of deepfakes, profile creation, for analytics of crimes against individuals, etc. It is proposed to classify not only AI systems for law enforcement agencies, justice, and border services, but also those developed for customs and tax authorities as high-risk. The problem of using intelligent systems to combat crime in the metaverse is outlined. The problem is identified as the absence of regulatory acts in national legislation regulating the implementation and use of information systems based on artificial intelligence in law enforcement and other areas of life.

Key words: law enforcement agencies, artificial intelligence, information system, metaverse, risk level.

Постановка проблеми. Технології штучного інтелекту (ШІ) вочевидь мають значний потенціал як дієві функціональні інструменти для різнобічної підтримки діяльності правоохоронних органів. Однак при цьому надзвичайно важливо розуміти, що ШІ-інструменти покликані не замінити фахівця-правоохоронця, а максимально посилити його можливості виконання службових завдань.

Нині ШІ-розробки застосовуються у правоохоронній сфері для вирішення різних задач залежно від визначених пріоритетів. За даними Інтерполу, найбільш успішно інтелектуальні системи використовуються для автоматизації патрулювання, ідентифікації дітей, що потрапили у скрутне становище чи стали об'єктом насильства й експлуатації, а також для оснащення центрів екстреного виклику поліції [1]. Так, Європол використовує інструменти на основі ШІ для класифікації зображень в аналітичних проєктах щодо торгівлі людьми й експлуатації дітей [2]. Правоохоронці США запровадили інформаційну систему на базі статистичних моделей PredPol (технологічна модель прогностичної поліційної діяльності, розроблена 2011 року і визнана тоді одним із найкращих винаходів), яка зокрема застосовується для визначення районів з високою ймовірністю злочинів, а також пропонує окремо методи прогнозування злочинів і методи прогнозування правопорушень, методики прогнозування ідентичності жертв, правопорушників, злочинців [3]. Натомість сьогодні для України найбільш актуальним є використання ШІ-інструментів для ідентифікації зображень людей, які зникли безвісти за особливих обставин; вирішення цієї проблеми підтримується програмою ОБСЄ [2; 4].

Загалом впровадження різноманітних інструментів на базі ШІ в роботу правоохоронних органів для аналітики, обробки великих даних, автоматизації розшукової діяльності дозволить більш ефективно виконувати чимало службових завдань: напр., швидше виявляти зв'язки між подіями, підозрюваними, місцями і часом їх перебування; з більшою ймовірністю прогнозувати активність правопорушень і злочинів; вдосконалити системи перевірки автоматизованих баз даних, зменшуючи втручання людського фактору; виявляти дипфейки і дезінформацію тощо. Однак, запровадження ШІ-технологій у роботу правоохоронних органів має чимало застережень, оскільки їхнє використання зумовлює виникнення цілої низки таких проблем, які прямо суперечать функціям правоохоронних органів. У зв'язку з цим актуальним є формування чіткого усвідомлення значення тих проблем, з якими вже стикнулися правоохоронці і суспільство через застосування ШІ-систем у правоохоронній сфері, проблем, які можуть виникнути в найближчому майбутньому, прогнозування їх у далекій перспективі, а також випереджувальний пошук шляхів їх вирішення. Отже, насамперед необхідно визначити коло проблем і уточнити їхню суть.

У нашій розвідці маємо на **меті** визначити нагальні і потенційні проблеми впровадження і використання інформаційних систем на базі штучного інтелекту у правоохоронній діяльності.

Стан опрацювання проблематики. Проблеми впровадження в діяльність правоохоронних органів інформаційних систем на базі штучного інтелекту ще не були предметом окремого наукового дослідження. Певні зауваження викладені експертами Інтерполу і Європолу, причому вони були висловлені свого часу як прогностичні припущення [1; 9; 10]. Відсутність наукових праць з обраної теми зумовлює актуальність нашої роботи.

Виклад основного матеріалу. Як відомо, системи на основі ШІ, призначені для правоохоронних органів, належать до систем з високим рівнем ризику, оскільки можуть бути використані так, що це обмежить права людей (приміром, під час оцінки достовірності доказів). Фахівці Інтерполу зазначають, що дії правоохоронців, які ґрунтуються на використанні систем ШІ, характеризуються значним рівнем дисбалансу сил і можуть бути причиною безпідставного стеження, арешту чи позбавлення волі, а також інших обмежень гарантованих прав людини [1]. Яскравим прикладом стало затримання у жовтні 2025 року американського підлітка внаслідок помилки функції розпізнавання системи охорони на базі штучного інтелекту, яка прийняла пакет з-під чипсів за зброю. У результаті на затримання прибуло кілька патрульних машин, поліцейські направили на дитину зброю, змусили хлопця лягти на землю, відтак поставили на коліна, вдягнули кайданки та обшукали. При цьому, незважаючи на очевидний дисбаланс між рівнем «потенційної загрози» і діями правоохо-

ронців, поліцейське управління округу Балтимор заявило, що його офіцери діяли пропорційно [5]. Водночас спрацював людський фактор: директорка школи викликала поліцію, хоча відповідний працівник, перевіривши сигнал системи, не підтвердив наявність небезпеки. Отже, проблема дисбалансу, непропорційності дій поліції може бути спричинена не тільки помилкою людини, а й помилкою машини, зумовленої недостатнім інтелектуальним розвитком системи, створеної на основі ШІ, а також, що теж важливо, надлишковим рівнем довіри людини до машини.

З огляду на це постає проблема якості інтелектуальних систем, вже визнаних готовими для використання, якості даних, на яких навчався штучний інтелект, і рівня кваліфікації тренера (аналітика даних, фахівця з машинного навчання). Якщо система штучного інтелекту є в цілому недостатньо якісною розробкою, навчається не на високоякісних або невідповідних даних, не перевірена належним чином аналітиком даних перед початком масового виробництва, продажу і використання, вона, вочевидь, є потенційно неадекватним інструментом, який становить загрозу для людини. Причому для правоохоронця така система теж не є дружньою, тому що через її неякісність/некомпетентність його дії можуть бути помилковими і навіть катастрофічними, що своєю чергою може мати для нього негативні наслідки. Отже, на нашу думку, вже зараз доцільно ставити питання компетентності інтелектуальних систем як загальної відповідності стандартам якості в трьох аспектах – технічної якості, якості навчальних даних і професійності фахівця з машинного навчання. Звісно, при цьому важливо також усвідомлювати роль людського фактора на етапі реагування на всиновок/рішення інтелектуальної системи.

Принагідно зауважимо, що 2 серпня 2025 року в ЄС набули чинності нові вимоги використання штучного інтелекту загального призначення, відповідно до яких розробники зобов'язані розкривати широкому загалу (або конкретним користувачам в разі застосування спеціалізованих інтелектуальних систем) інформацію про принципи роботи своїх ШІ-моделей, а також про дані, що були використані для їхнього навчання, та документування заходів безпеки (реагування системи на інциденти щодо безпеки в реальному часі). Натомість за порушення цих правил на інтелектуальні системи можна подавати скарги, навіть до суду. Отже, йдеться про проблему відповідальності і політику прозорості виробника, що своєю чергою може спричинити проблеми із забезпеченням захисту інтелектуальної власності, напр., щодо даних для навчання ШІ-системи. Втім, Європейський офіс з нагляду за штучним інтелектом (European AI Office) почне перевіряти нові моделі на відповідність встановленим правилам тільки із серпня 2026 року, а попередні модифікації перевірятиме з 2027 року.

Разом із тим із цих правил є винятки: відповідно до встановлених правил у ЄС заборонено розпізнавати за допомогою ШІ обличчя людей із записів відеокамер у громадських місцях, однак це дозволено правоохоронним органам у разі розслідування злочинів, пов'язаних із торгівлею людьми і тероризмом [6; 7]. Отже, результативність поліційних розслідувань і дотримання прав людини напряму залежить від якості технічного забезпечення, інтелектуального розвитку ШІ-систем, кваліфікованості аналітика даних і відповідальності виробників.

Особливо небезпечним для забезпечення і реалізації основних прав людини і, зрештою, неприпустимим є використання ШІ-систем незадовільної якості у процесуальних діях, коли під загрозою можуть опинитися право на захист і справедливий суд, а також презумпція невинуватості.

Очевидно, що готові до використання у правоохоронній діяльності ШІ-системи мають бути максимально точними, надійними, а їхня інтелектуальна діяльність – ефективною, прозорою, зрозумілою і придатною для документування заходів безпеки, які вживаються. Це дозволить уникнути грубих помилок у роботі системи і несприятливих наслідків таких помилок для правоохоронців, громадян і суспільства в цілому, а також допомагатиме збереженню довіри до правоохоронних органів, налагодженню взаєморозуміння і співпраці правоохоронних органів із громадою.

Підвищенню ефективності інтелектуальних систем сприятиме також звуження їхньої спеціалізації. Нині малі мовні моделі вже успішно конкурують із великими (LLM) саме у виконання конкретних завдань. Їхніми перевагами є те, що вони навчаються швидше і на більш сфокусованих наборах даних. Правоохоронні органи зацікавлені в розроблені окремих спеціальних ШІ-інструментів для виконання конкретних функцій: зокрема для оцінки ризиків, для роботи поліграфа і подібних приладів, здатних визначати емоційний стан людини, для виявлення дипфейків, оцінки достовірності доказів у кримінальному провадженні, прогнозування скоєння правопорушень/злочинів і рецидивізму, прогнозування ймовірності серії злочинів за процедурами профайлінгу, виявлення кримінальних схильностей на підставах оцінки особистісних рис і кримінальної поведінки в минулому особи або групи осіб (тобто на засадах екстремальної психології), для профілювання під час виявлення, розслідування або судового розгляду кримінального правопорушення, а також для аналітики злочинів проти фізичних осіб або, що сьогодні особливо актуально, злочинів проти людяності. Спеціалізація окремих ШІ-систем, їхнє спеціальне, профільне навчання та перевірка з боку фахівця-аналітика дозволить зменшити вірогідність службових помилок і загалом уникати їх.

Разом із тим проблемним є питання віднесення до групи високого ризику інтелектуальних систем, призначених для використання податковими і митними органами для адміністративних проваджень. На думку фахівців Інтерполу, такі системи (напр., аналіз ризиків на митному контролі, класифікація товарів і їхніх цін, виявлення міжкорпоративних зв'язків тощо) не є високоризиковими, бо виконують інформаційну, контрольну та інші подібні функції, а не застосовуються з метою запобігання, виявлення і розслідування кримінальних правопорушень [8; 9]. Водночас Європол пропонує розроблені для сфери безпеки і правосуддя правила застосування штучного інтелекту для використання у прикордонних службах, які стикаються і з адміністративними, і з кримінальними правопорушеннями [10]. Однак правоохоронні органи й органи правосуддя, безпеки, прикордонні служби, а також митні і податкові органи – це інституції фактично одного рівня відповідальності. Відтак, аспект визначення ризиковості потребує додаткового узгодження між регіональними і міжнародними організаціями.

Складною проблемою, яка дещо випереджає час, є боротьба зі злочинністю у метавсесвіті. Думки про тяжкість одного і того самого злочину (напр., зґвалтування) і покарання за нього в реальному світі та метавсесвіті суттєво розходяться, оскільки концепція метавсесвіту ще остаточно не сформована. Незважаючи на це, Інтерпол 2023 року заявив, що організація планує боротися зі злочинністю у метавсесвіті, а для цього ініціює віртуальні розробки і відповідні навчальні проєкти. Інтерпол створив власний простір віртуальної реальності, де користувачі можуть проходити навчання і відвідувати зустрічі. У такий спосіб правоохоронні органи можуть навчитися прогнозувати злочини в метавсесвіті і контролювати його [11]. Отже, у новітній час правоохоронні органи стикнулися із проблемою опанування метавсесвіту як модерного потенційно небезпечного середовища для модифікацій кіберзлочинності і водночас – нового поля для поліційної діяльності, інструменти якого необхідно швидко освоювати.

У зв'язку із запровадженням систем штучного інтелекту поглиблюється проблема наукової підготовки працівників правоохоронних органів. Якщо раніше наукова підготовка стосувалася окремої спеціалізації фахівців правоохоронної сфери (приміром, спеціалістів із судової експертизи та судово-медичної експертизи, фахівців із оперативно-технічного забезпечення і вибухотехнічної служби, криміналістів тощо), то з початком тотальної автоматизації службових процесів і процедур у правоохоронній сфері збільшилися вимоги до теоретичної і практичної наукової підготовки правоохоронних кадрів загалом (на тлі стрімкого розвитку і поширення інформаційно-комунікаційних технологій в епоху інформаційного суспільства). Правоохоронець 2000-х років уже мав бути обізнаним в автоматизованих системах обробки даних, автоматизованих інформаційно-пошукових системах, автоматизованих інформаційно-довідкових системах, автоматизованих інформаційно-розпізнавальних системах, згодом – системах підтримки ухвалення рішень та експертних системах. Сучасні правоохоронці мають швидко опановувати теоретичні і практичні наукові засади роботи з інтелектуальними системами і використання технологій метавсесвіту. Нагадаємо, що новітні наукові підвалини правоохоронної діяльності закладалися на початку 2010-х років. Так, Національний інститут юстиції США і Гарвардський університет 2011 року опублікували концептуальну працю «Поліційна наука: рух до нової парадигми» (Police Science: Toward a New Paradigm, 2011), в якій обґрунтовувалося радикальне збільшення наукового елементу у підготовці правоохоронців, наголошувалося на необхідності тісної співпраці поліції і наукових інституцій, визначалися пріоритети політики доказування як основи поліційної діяльності. При цьому, на думку авторів концепції, збільшення наукової складової в роботі правоохоронців покликане допомагати вирішувати службові завдання, гарантувати громадську підтримку, аргументувати легітимність дій поліції, а також сприяти забезпеченню належного фінансування [12].

Проблемним залишається питання темпів розроблення національних, регіональних і міжнародних нормативних та інструктивних документів у сфері розроблення і використання штучного інтелекту, причому з високим ступенем проактивності. На сьогодні головними документами, які регулюють використання інтелектуальних систем у діяльності правоохоронних органів, є розроблений Інтерполом Інструментарій для відповідального впровадження інновацій у сфері штучного інтелекту у правоохоронних органах (AI Toolkit, 2022) та укладені Європолом Принципи підзвітності для штучного інтелекту у сфері внутрішньої безпеки (AP4AI, 2022) [1; 10]. Обидва документи ґрунтуються на концепції відповідального запровадження і використання ШІ у правоохоронних органах, а також у сфері безпеки, правосуддя і прикордонних службах. Основними принципами застосування інтелектуальних систем визначено законність, відповідальність, людиноцентризм, соціальна керованість щодо наявних і майбутніх можливостей ШІ у секторі безпеки і правосуддя [1; 10]. Очевидно, що на основі цих документів та іншого світового досвіду час створювати і розвивати власну національну нормативно-правову базу.

Висновки. Таким чином, головними проблемами впровадження систем на базі штучного інтелекту в діяльність правоохоронних органів є такі: високий ступінь ризику використання ШІ-систем

щодо дотримання прав людини, проблема компетентності інтелектуальних систем (технічна якість ШІ-розробки, якість використаних для її навчання даних, якість передбачених заходів безпеки, кваліфікація фахівця з машинного навчання), необхідність розроблення високоякісних інтелектуальних систем вузької спеціалізації для вирішення правоохоронцями конкретних службових задач, потреба перегляду на міжнародному рівні класифікації ШІ-систем для сфери безпеки і правосуддя, прикордонних служб, митних і податкових органів за ступенем ризику, необхідність активного опанування правоохоронцями інструментарію метавсесвіту для прогнозування злочинів у цій новій машинній реальності і реагування на них, збільшення наукової складової в підготовці і перепідготовці правоохоронців у контексті розвитку цифрової цивілізації, розроблення на принципах проактивності національних нормативно-правових актів та інструктивних документів щодо відповідального впровадження і використання систем на базі ШІ і гармонізація їх із відповідними актами міжнародного і регіонального значення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Artificial intelligence Toolkit / Interpol. URL: https://www.interpol.int/How-we-work/Innovation/Artificial-Intelligence-Toolkit (дата звернення: 02.12.2025).
2. Штучний інтелект у службі безпеки та правопорядку / Панченко Євгеній, перший заступник начальника Департаменту міжнародного поліцейського співробітництва Національної поліції України. 10.11.2025. URL: https://www.facebook.com/panch.evg/posts/ (дата звернення: 02.12.2025).
3. Прогностичні алгоритми у поліційній діяльності / imena.ua. 15.01.2018. URL: https://www.imena.ua/blog/nerds-and-cops-predpol/ (дата звернення: 02.12.2025).
4. Україна використовує штучний інтелект для пошуку зниклих безвісти людей / Омбудсман України. 16.11.2023. URL: https://ombudsman.gov.ua/news_details/dmitro-lubinec-shtuchnij-intelekt-vikoristovuyut-dlya-poshuku-zniklih-bezvisti-lyudej (дата звернення: 02.12.2025).
5. McMahon L., Rahman-Jones I. Armed police handcuff teen after AI mistakes crisp packet for gun in US / BBC. 24.10.2025. URL: https://www.bbc.com/news/articles/cgjdlx92lylo (дата звернення: 02.12.2025).
6. У ЄС набули чинності вимоги до прозорості штучного інтелекту / Укрінфо. 02.08.2025. URL: https://www.ukrinform.ua/rubric-world/4021454-u-es-nabuli-cinnosti-vimogi-do-prozorosti-stucnogo-intelektu.html (дата звернення: 02.12.2025).
7. Artificial intelligence Act / EC. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206 (дата звернення: 02.12.2025).
8. Shaping Europe's digital future: AI Act / EC. URL: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (дата звернення: 02.12.2025).
9. Accountability Principles for Artificial Intelligence (AP4AI) in the Internal Security Domain AP4AI Framework Blueprint / Europol. 22.02.2022. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/Accountability_Principles_for_Artificial_Intelligence_AP4AI_in_the_Internet_Security_Domain.pdf (дата звернення: 02.12.2025).
10. Toolkit for Responsible AI Innovation in Law Enforcement: README file / Interpol. URL: https://www.interpol.int/How-we-work/Innovation/Artificial-Intelligence-Toolkit (дата звернення: 02.12.2025).
11. Cieslak M., Gerken T. Interpol working out how to police the metaverse / BBC. 04.02.2023. URL: https://www.bbc.com/news/technology-64501726 (дата звернення: 02.12.2025).
12. Weisburd D., Neyroud P. Police Science: Toward a New Paradigm / Haward Kennedi School; National Institute of Justice. URL: https://www.hks.harvard.edu/sites/default/files/centers/wiener/programs/pcj/files/Police%2BScience-TowardaNewParadigm.pdf (дата звернення: 02.12.2025).

Дата першого надходження рукопису до видання: 5.12.2025
Дата прийняття до друку рукопису після рецензування: 26.01.2026
Дата публікації: 2.02.2026