Львівський державний університет внутрішніх справ

Національна академія внутрішніх справ

Харківський національний університет внутрішніх справ

Одеський державний університет внутрішніх справ

Дніпровський державний університет внутрішніх справ

Рада молодих учених при Міністерстві освіти і науки України

Львівський державний університет безпеки життєдіяльності

Національний транспортний університет

Харківський національний університет радіо-електроніки

Ужгородський національний університет

Грантовий проєкт ЄС Еразмус+ (напрям Жан Моне) ELVEUCP

Co-funded by the European Union

ШТУЧНИЙ ІНТЕЛЕКТ У ПРАВОВІЙ ПРАКТИЦІ: МЕЖІ ТА МОЖЛИВОСТІ

Збірник тез міжнародного круглого столу

13 березня 2026 року

Львів-Київ-Харків-Одеса-Дніпро-Ужгород

УДК 34:[004.8+004.383.8](063)

Рекомендовано до друку та поширення через мережу Інтернет
Вченою радою ННІППД Львівського державного університету
внутрішніх справ
(протокол № 8 від 11 березня 2026 року)

Упорядник:
О. О. Барабаш, докторка юридичних наук, професорка,
завідувачка науково-дослідної лабораторії актуальних проблем
правозастосовної та правоохоронної діяльності
ННІ права та правоохоронної діяльності ЛьвДУВС

ШТУЧНИЙ ІНТЕЛЕКТ У ПРАВОВІЙ ПРАКТИЦІ: МЕЖІ ТА МОЖЛИВОСТІ : збірник тез міжнародного круглого столу (13 березня 2026 року) / упор. О. О. Барабаш. Львів : ЛьвДУВС, 2026. 396 с.

У збірнику вміщено тези доповідей учасників міжнародного круглого столу «Штучний інтелект у правовій практиці: межі та можливості», який відбувся 13 березня 2026 року у Львівському державному університеті внутрішніх справ.

Опубліковано в авторській редакції. Відповідальність за достовірність фактів, статистичних даних, точність викладеного матеріалу покладається на авторів.

This collection contains the abstracts of presentations delivered at the international roundtable discussion «Artificial Intelligence in Legal Practice: Limits and Possibilities», which took place on March 13, 2026, at Lviv State University of Internal Affairs.

Published in the authors' original version. The authors are responsible for the accuracy of the facts, statistical data, and the material presented.

УДК 34:[004.8+004.383.8](063)

ЗМІСТ

ВСТУПНЕ СЛОВО

Шановні колеги! Шановна наукова спільното!

Щиро вітаю вас із початком роботи міжнародного круглого столу «Штучний інтелект у правовій практиці: межі та можливості».

Сьогодні ми об'єднані спільною метою – осмислити роль штучного інтелекту в правовій практиці, визначити межі його застосування та окреслити перспективи розвитку в умовах сучасних викликів.

Особливо приємно відзначити активну роль Ради молодих вчених Львівського державного університету внутрішніх справ, яка є важливою платформою для формування нової генерації дослідників, розвитку міждисциплінарного наукового діалогу та впровадження інноваційних підходів у сфері права і правоохоронної діяльності.

Сьогодні молоді науковці не лише долучаються до дискусії, а й формують нову наукову повістку, де штучний інтелект розглядається крізь призму прав людини, етики та європейських стандартів.

Переконаний, що поєднання досвіду провідних фахівців і енергії молодих дослідників створює унікальне середовище для вироблення сучасних правових рішень.

Бажаю всім учасникам плідної роботи, змістовних дискусій та нових наукових ідей.

Дмитро ШВЕЦЬ
ректор,
доктор юридичних наук, професор,
заслужений працівник освіти України,
полковник поліції

Афтанасів В.М.
здобувачка вищої освіти
навчально-наукового інституту
права та правоохоронної діяльності,
співголова Наукового товариства
студентів (курсантів, слухачів),
аспірантів, докторантів і молодих вчених
(Львівський державний університет внутрішніх справ)
Барабаш О.О.
завідувач науково-дослідної лабораторії
актуальних проблем правозастосовної
та правоохоронної діяльності
навчально-наукового інституту
права та правоохоронної діяльності,
голова Ради молодих вчених,
доктор юридичних наук, професор
(Львівський державний університет внутрішніх справ)

ПРАВОВЕ РЕГУЛЮВАННЯ ЗАСТОСУВАННЯ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ У МЕДИЧНІЙ ДІАГНОСТИЦІ ТА ЛІКУВАННІ: ПРОБЛЕМАТИКА ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ ЗА МЕДИЧНІ ПОМИЛКИ

Починаючи міркування щодо правового регулювання застосування систем штучного інтелекту (далі – ШІ) у медичній діагностиці та лікуванні, доречно, щонайменше, взяти до уваги обставину, яка стає все більш очевидною у світлі трансформацій медичної практики. Так, передусім слід відзначити поступову зміну моделі клінічного мислення, в якій центральною постаттю був лікар-клініцист, носій професійного досвіду, – у напрям технологічно опосередкованого прийняття рішень. Сьогодні алгоритмічні системи аналізують результати магнітно-резонансної томографії, комп'ютерної томографії, дані гістопатологічних досліджень, електрокардіографічні показники, біомаркери плазми крові тощо [1, с. 72]. Відповідно, юридична наука, без перебільшення, стикається з потребою перегляду класичних

категорій деліктної відповідальності у сфері охорони здоров'я. При цьому виникає цілком логічне питання – чи може алгоритм, побудований на основі нейронної мережі, бути опосередкованим суб'єктом деліктної відповідальності, чи, навпаки, юридична відповідальність має залишатися виключно в площині людської діяльності.

Історично медична відповідальність у континентальній правовій традиції формувалася через доктрину професійної вини лікаря. Зокрема, ще у працях французького правника Ж. Пенне наголошувалося, що лікарська діяльність є сферою підвищеного ризику, у межах якої недбалість повинна оцінюватися з огляду на стандарт «bonus medicus», тобто поведінки розсудливого лікаря за аналогічних обставин [2]. Втім, коли ми говоримо про використання алгоритмів глибокого навчання у клінічній практиці, концепція професійної вини свідчить про певні доктринальні протиріччя. Адже у випадку, скажімо, діагностики гострої краніофаціальної травми на підставі аналізу томографічних зображень алгоритм може запропонувати висновок, який лікар, довіряючи технологічній системі, прийме як обґрунтований. І якщо цей висновок виявиться помилковим – до прикладу, алгоритм не розпізнає субдуральну гематому або перелом основи черепа, – юридична оцінка відповідальності набуває зовсім іншого виміру.

У цьому аспекті слід звернутися до національного законодавства, яке, попри певні кроки у напрямі цифровізації медицини, наразі не містить достатньо визначеної конструкції відповідальності за використання алгоритмічних систем у клінічній практиці. Закон України «Основи законодавства України про охорону здоров'я» від 19.11.1992 р. №2801-XII, зосереджуючись на правах пацієнтів та професійних обов'язках медичних працівників, фактично виходить із антропоцентричної моделі медичної допомоги [3]. Вважаємо, що у випадку застосування систем ШІ в медичній практиці, потенційну юридичну відповідальність може нести лікар, медичний заклад, розробник програмного забезпечення, виробник медичного обладнання, а інколи й постачальник даних, на яких тренувався алгоритм.

Прикметно, що у праві Європейського Союзу відповідна проблематика більш виразно нормативно окреслена. Насамперед варто згадати Регламент Європейського Парламенту та Ради (ЄС) 2017/745 про медичні вироби, який класифікує програмне забезпечення для медичної діагностики як медичний виріб і підпорядковує його як вимогам безпеки, так і клінічної ефективності [4]. Утім, більш показовим у цьому контексті є Регламент Європейського Союзу про ШІ – «AI Act», ухвалений у 2024 році. В акті системи ШІ, що застосовуються у сфері медичної діагностики або клінічних рішень, віднесені до категорії *високого ризику*, а отже підлягають обов'язковим процедурам сертифікації, аудиту алгоритмів та контролю якості даних [5]. Власне кажучи, вбачається, що подібна модель може становити інтерес для українського законодавця, особливо з огляду на євроінтеграційний вектор розвитку правової системи України.

Окремо варто зупинитися на тому, що у правовій доктрині достатньо часто висловлюються пропозиції переглянути традиційну модель відповідальності за медичні помилки. Зокрема, британський дослідник Р. Браунсворд, аналізуючи вплив технологій ШІ на медичну практику, звертає увагу, що алгоритмічні системи створюють делегування відповідальності без контролю, коли визначення конкретного винуватця шкоди є вкрай складним [6, с. 211]. У світлі наведеного автор апелює до концепції розподіленої відповідальності. Утім, висловимо певне застереження з даного приводу. Так, запропонована модель видається обґрунтованою з позицій теорії ризику, однак, може зумовити правову невизначеність для пацієнта, який у випадку шкоди хоче отримати чітку відповідь на запитання про те, хто саме має нести юридичну відповідальність за завдану шкоду.

Звертаючись до практики Європейського суду з прав людини (далі – ЄСПЛ, Суд), варто підкреслити, що у справах «Lopes de Sousa Fernandes v. Portugal» [7] та «Vasileva v. Bulgaria» [8] Суд наголошував на позитивному обов'язку держави гарантувати належне функціонування системи охорони здоров'я, в тому числі з механізмами розслідування лікарських і медичних помилок. Врешті, можна дійти висновку, що застосування алгоритмічних систем у медицині неминуче охоплює й обов'язок держави створити систему юридичної відповідальності, яка

гарантуватиме захист права людини на життя та медичну допомогу відповідно до ст. 2 Конвенції про захист прав людини і основоположних свобод [9].

Попри зазначене, станом на сьогодні вітчизняне законодавство у досліджуваній сфері тільки починає формуватися. Закон України «Про захист персональних даних» від 01.06.2010 р. №2297-VI встановлює певні вимоги щодо обробки медичної інформації [10], однак питання алгоритмічного аналізу біомедичних даних залишаються поза його регулюванням. Слід наголосити і на тому, що медичні алгоритми функціонують завдяки масивам клінічних даних – від результатів лабораторних досліджень до геномних маркерів, а отже питання правового режиму медичної інформації безпосередньо пов'язане з ефективністю та безпечністю алгоритмічної медицини.

Привертає увагу й доволі показова тенденція, що останнім часом простежується у політиці великих технологічних корпорацій щодо використання алгоритмічних систем у сфері медичних консультацій. Так, зокрема, у внутрішніх правилах використання штучних інтелектуальних сервісів корпорації Microsoft підкреслюється, що подібні системи не повинні застосовуватися для встановлення медичних діагнозів, призначення лікування або рекомендацій щодо застосування лікарських препаратів, оскільки вони *не є медичними виробами* та *не можуть замінити професійне клінічне судження лікаря*. Відповідно до положень оновленої угоди про використання сервісів Microsoft, так звані «health-bots» або інші алгоритмічні інструменти можуть виконувати лише інформаційну або освітню функцію, тоді як будь-які рішення щодо діагностики, профілактики чи лікування захворювань повинні прийматися виключно кваліфікованим медичним фахівцем [11].

Принагідно зауважимо, що така позиція зумовлена не тільки етичними міркуваннями, але й доволі прагматичними юридичними ризиками. У наукових дослідженнях, присвячених оцінці якості медичних відповідей алгоритмічних систем, було встановлено, що значна частина рекомендацій, сформульованих ШІ, потенційно може спричинити шкоду здоров'ю пацієнта, а у певних випадках навіть становити загрозу життю. За результатами дослідження, проведеного європейськими експертами з медичної інформатики, приблизно 42% відповідей алгоритмічних систем у сфері

медицини могли призвести до помірної або значної шкоди для пацієнта, а близько 22% - до тяжких або навіть летальних наслідків у разі їх некритичного застосування [12].

Втім, що прикметно і, без перебільшення, дещо парадоксально, навіть за наявності подібних обмежень та застережень, медичні працівники у різних країнах світу продовжують використовувати загальнодоступні системи ШІ у своїй повсякденній клінічній практиці. Звертаючись до сучасних досліджень у галузі медичної інформатики, можна побачити, що лікарі застосовують алгоритмічні моделі для інтерпретації лабораторних показників, попереднього аналізу результатів комп'ютерної томографії, формування диференційного діагнозу, а інколи навіть для перевірки фармакологічних взаємодій лікарських препаратів. У цьому контексті виникає доволі цікаве протиріччя: технологічні компанії прагнуть максимально дистанціюватися від юридичної відповідальності за медичні рекомендації, наголошуючи на винятково допоміжному характері алгоритмічних систем, тоді як сама медична практика вже поступово інтегрує ці інструменти у процес клінічного мислення.

У світлі цього, вбачається, що проблема юридичної відповідальності за медичні помилки, пов'язані з використанням ШІ, не може бути розв'язана лише шляхом формального проголошення застережень або обмежень у правилах використання технологічних сервісів. Врешті-решт, коли лікар, аналізуючи результати нейровізуалізації пацієнта із підозрою на внутрішньочерепну гематому чи гостру краніофаціальну травму, звертається до алгоритмічної системи для уточнення діагностичної гіпотези, виникає новий тип клінічного рішення, у якому людський інтелект та алгоритмічна аналітика фактично співіснують у межах одного процесу медичного мислення. Саме ця обставина, очевидно, й формує новий виклик для сучасного медичного права, яке наразі не виробило юридичних критеріїв оцінки подібних ситуацій.

Список використаних джерел:

1. Litjens G., Kooi T., Bejnordi B., Setio A., Ciompi F., Ghafoorian M., van der Laak J., van Ginneken B., Sánchez C. A survey on deep learning in medical image analysis. *Medical Image Analysis*.

2017. Vol. 42. P. 60-88. DOI: https://doi.org/10.1016/j.media.2017.07.005

2. Penneau J, Faute et erreur en matière de responsabilité médicale. *Revue internationale de droit comparé*. Année 1974. Vol. 26-4 . P. 948-949.

3. Основи законодавства України про охорону здоров'я: Закон України від 19.11.1992 №2801-XII. URL: https://zakon.rada.gov.ua/laws/show/2801-12#Text

4. Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices. URL: https://eur-lex.europa.eu/eli/reg/2017/745/oj/eng

5. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

6. Brownsword R. Law, Technology and Society: Reimagining the Regulatory Environment (1st ed.). *Routledge*. 2019. 361 p. DOI: https://doi.org/10.4324/9781351128186

7. Lopes de Sousa Fernandes v. Portugal. App 56080/13. Judgement 19.12.2017. URL: https://hudoc.echr.coe.int/eng?i=001-179556

8. Vasileva v. Bulgaria. App 23796/10. Judgement 17.03.2016. URL: https://hudoc.echr.coe.int/fre?i=001-161413

9. European Convention on Human Rights of 04.11.1950. URL: https://www.echr.coe.int/documents/d/echr/convention_ENG

10.Про захист персональних даних: Закон України від 01.06.2010 №2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

11.Okemwa K. Even Microsoft doesn't think AI is 'designed or intended' to substitute professionals and should only be treated as a guide. 2024. URL: https://www.windowscentral.com/software-apps/even-microsoft-doesnt-think-ai-is-designed-to-substitute-professionals

12.Corden J. A new research paper suggests that Bing / Microsoft Copilot «AI» medical advice may be capable of causing you severe harm, at least 22% of the time ... 2024. URL: https://www.windowscentral.com/microsoft/microsoft-copilot-ai-medical-advice-danger

Барабаш О.О.
завідувач науково-дослідної лабораторії
актуальних проблем правозастосовної
та правоохоронної діяльності
навчально-наукового інституту
права та правоохоронної діяльності,
голова Ради молодих вчених,
доктор юридичних наук, професор
(Львівський державний університет внутрішніх справ)

ВИКОРИСТАННЯ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПРОГНОЗУВАННЯ ПОТРЕБ У КАДРАХ МВС: ПРАВОВІ, ЕТИЧНІ ТА КІБЕРБЕЗПЕКОВІ АСПЕКТИ

Правоохоронна практика сьогодення розвивається на перетині двох епох: інструменти управління, закорінені у традиціях XX століття, співіснують із алгоритмічними системами аналізу даних, здатними прогнозувати можливі траєкторії криміногенної динаміки. Поряд із цим, питання кадрового забезпечення органів внутрішніх справ виходить за межі адміністративно-організаційної площини, що зосереджувалася на чисельності особового складу та державному замовленні на підготовку кадрів. Досліджуваний аспект безпосередньо пов'язується з використанням цифрової аналітики, великих масивів статистичних даних та алгоритмів штучного інтелекту (далі – ШІ). Прикметно, що сучасні дослідження висвітлюють досить показову тенденцію: у державах із розвиненою технологічною інфраструктурою понад 62% правоохоронних органів використовують чи тестують системи ШІ, тоді як у країнах, що перебувають на етапі інституційних змін, цей показник становить близько 28% [1].

Водночас стрімке поширення алгоритмічних інструментів у сфері публічної безпеки має доволі виразне соціально-економічне підґрунтя. Так, за оцінками міжнародних аналітичних досліджень, світовий ринок систем прогнозування злочинності та управління поліцейськими ресурсами у 2024 р. оцінювався приблизно у 590 млн доларів США, тоді як до 2030 р. очікується його зростання до

1,62 млрд доларів, що демонструє стійку тенденцію інституційного переходу правоохоронних структур до алгоритмічних моделей планування діяльності [2].

Більше того, окремі аналітичні прогнози вказують на ще більш динамічний розвиток названої галузі: за деякими оцінками, глобальний ринок ШІ у «predictive policing» (використання алгоритмів ШІ для прогнозування ймовірних місць та часу вчинення злочинів, а також для аналізу поведінкових патернів) може зрости до 29 млрд доларів США уже до 2029 р., що відображає безпрецедентний рівень інвестицій у цифровізацію систем безпеки [3].

Історично, як відомо, кадрове планування у поліції формувалося за відносно стабільною адміністративною моделлю: чисельність особового складу визначалась демографічними показниками, рівнем злочинності та фінансовими можливостями держави. Утім нині, коли криміногенне середовище все більш пов'язане з кіберзлочинністю, транснаціональними кримінальними мережами та інформаційними загрозами, традиційні методи прогнозування кадрових потреб виявляються щонайменше недостатніми. Принагідно зауважимо, що навіть у країнах Європейського Союзу використання алгоритмічних систем у поліцейській діяльності тепер розглядається як інструмент оптимізації кадрового ресурсу, оскільки аналітичні моделі дають змогу точніше прогнозувати оперативно-службове навантаження на підрозділи та відповідно планувати структуру персоналу. У наукових працях наголошується, що це поступово змінює саму філософію функціонування правоохоронних органів, оскільки аналітичні системи ШІ здатні опрацьовувати значні обсяги інформації та виявляти кореляції між подіями, які залишаються поза межами традиційних управлінських інструментів [4, с. 149].

Актуальною зазначена проблематика є і для України, адже система МВС функціонує в умовах тривалих безпекових викликів та воєнної агресії. Сьогодні правоохоронні органи змушені виконувати завдання, які ще кілька років тому були не властиві їх традиційному функціональному профілю: документування воєнних злочинів, протидія диверсійним групам, забезпечення правопорядку у прифронтових регіонах, супровід масштабних евакуаційних та гуманітарних процесів. Відповідно, питання

прогнозування кадрового потенціалу є стратегічно важливим, оскільки результативність правоохоронної діяльності залежить від здатності держави передбачати майбутню потребу у фахівцях різних напрямів – від кримінальних аналітиків і кіберслідчих до експертів у сфері цифрової криміналістики.

У цьому контексті закономірно зростає роль закладів вищої освіти зі специфічними умовами навчання, які формують кадровий резерв правоохоронної системи. Саме вони, власне кажучи, є інституційним вузлом між стратегічними потребами держави у сфері безпеки та системою професійної підготовки майбутніх правоохоронців [5, с. 53]. Однак визначення кількості курсантів, спеціалізацій підготовки та структурної моделі навчального процесу все частіше вимагає звернення до аналітичних інструментів прогнозування, які здатні враховувати не тільки поточні кадрові потреби МВС, але й довгострокові тенденції розвитку криміногенної ситуації, демографічні зміни та характер злочинності.

Одним із найбільш перспективних напрямів модернізації державного управління у сфері публічної безпеки вбачається використання систем ШІ для прогнозування кадрових потреб органів внутрішніх справ. Втім, поряд із очевидними технологічними можливостями виникає спектр правових, етичних та кібербезпекових питань. Адже алгоритмічні системи фактично змінюють саму логіку прийняття управлінських рішень у сфері кадрової політики. Тут виникає цілком обґрунтоване питання: якою мірою держава повинна покладатися на алгоритмічні прогнози у настільки важливій сфері, як формування кадрового потенціалу правоохоронних органів, і які правові гарантії мають забезпечувати баланс між технологічною ефективністю та принципами верховенства права. Очевидно, зазначені обставини і зумовлюють потребу ґрунтовного наукового аналізу можливостей використання систем ШІ для прогнозування кадрових потреб МВС України, з огляду на правові, етичні та кібербезпекові аспекти функціонування подібних технологій у сучасній правоохоронній діяльності.

Зосереджуючись на проблематиці прогнозування кадрових потреб МВС, доречно звернутися до положень Закону України «Про Національну поліцію» від 02.07.2015 р. №580-VIII [6], а

також Закону України «Про захист персональних даних» від 01.06.2010 р. №2297-VI [7], які опосередковано формують законодавче підґрунтя для використання інформаційно-аналітичних систем у сфері державного управління. Втім, наразі вітчизняне законодавство не містить спеціального акту, присвяченого регулюванню алгоритмічних систем у діяльності правоохоронних органів. Правові передумови для їх застосування вже закладені у нормах, що регламентують функціонування інформаційно-телекомунікаційних систем МВС, зокрема у відомчих положеннях щодо кримінальної аналітики та інформаційних ресурсів Національної поліції. В даному аспекті цікавим є досвід функціонування центрів кримінального аналізу (напр., Центр кримінальної аналітики Національної академії внутрішніх справ [8]), діяльність яких охоплює систематизацію великих масивів статистичних даних, що, власне кажучи, визначає підстави для подальшого використання алгоритмів машинного навчання для прогнозування оперативно-службового навантаження та відповідної потреби у кадровому ресурсі.

Утім, коли ми говоримо про застосування систем ШІ у прогнозуванні кадрових потреб правоохоронних органів, слід звернутися до зарубіжної практики, де подібні технології вже застосовуються як для аналізу злочинності, так і для управління поліцейськими ресурсами. Зокрема, у США [9] та Великій Британії [10, с. 141] системи так званого «predictive policing» дають можливість моделювати криміногенну ситуацію на основі статистичних алгоритмів, що у свою чергу дає змогу прогнозувати навантаження на поліцейські підрозділи та планувати розподіл людських ресурсів.

В той же час, апелюючи до позицій зарубіжної наукової доктрини, не можна оминути праці британських дослідників, які, аналізуючи алгоритмічні системи у кримінальній юстиції, слушно зауважують, що використання ймовірнісних моделей у діяльності правоохоронних органів зумовлює виникнення нових правових дилем, пов’язаних із прозорістю алгоритмів, можливістю їх аудиту та потенційними ризиками дискримінаційного ефекту алгоритмічних рішень [11]. Власне кажучи, погоджуючись із цією позицією лише частково, слід відмітити, що проблема алгоритмічної упередженості не є аргументом проти використання

ШІ як такого; радше йдеться про потребу в створенні правових процедур перевірки алгоритмів та забезпечення їх підзвітності державі і суспільству.

Як зазначалося раніше, системи ШІ здатні виконувати роль аналітичного інструменту стратегічного планування. До прикладу, алгоритмічні моделі можуть враховувати статистику злочинності, демографічні зміни, динаміку міграційних процесів, а також кадрову плинність у підрозділах МВС. Відтак, використовуючи методи машинного навчання, можливо спрогнозувати кількість фахівців, які будуть потрібні для забезпечення належного функціонування правоохоронної системи у середньостроковій і довгостроковій перспективі.

Втім, не можна оминути питання кібербезпекових ризиків, які виникають у процесі використання ШІ. Алгоритмічні системи оперують значними масивами персональних даних правоохоронців і кандидатів на службу, а отже, фактично стають об'єктом підвищеного ризику кіберзлочинів (наприклад, зі сторони відповідних підрозділів спецслужб рф). Тому при створенні подібних систем варто враховувати приписи Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. №2163-VIII [12] та міжнародні стандарти інформаційної безпеки. Більше того, у контексті євроінтеграційного курсу України доцільно звернутися до положень Регламенту ЄС про ШІ [13], який закріплює категоризацію алгоритмічних систем за рівнем ризику та встановлює спеціальні вимоги до систем, що використовуються у сфері правоохоронної діяльності. У відповідь на ці виклики український законодавець, на моє переконання, має ініціювати створення окремого нормативного акту, присвяченого регулюванню застосування ШІ у діяльності правоохоронних органів.

Окремо варто зупинитися і на етичному вимірі зазначеної проблеми. Алгоритмічне прогнозування кадрових потреб неминуче передбачає використання статистичних моделей, які аналізують поведінкові та соціальні параметри. Проте, як показує зарубіжний досвід, надмірна залежність від алгоритмічних рішень може призводити до, так би мовити, «технологічної детермінації» управлінських процесів, коли рішення фактично делегуються програмному забезпеченню. На противагу цьому, на моє

переконання, ШІ має розглядатися виключно як інструмент допоміжної аналітики, а остаточне управлінське рішення повинно залишатися за уповноваженими посадовими особами.

Підсумовуючи викладене, доречно відмітити, що застосування систем ШІ у прогнозуванні кадрових потреб МВС України становить перспективний напрям модернізації державного управління у сфері безпеки. Сьогодні, коли правоохоронна система функціонує під тиском воєнних викликів, аналітичні можливості ШІ можуть стати вагомим інструментом стратегічного планування кадрового потенціалу, однак лише за умови, що правова держава зберігатиме контроль над технологіями, а не навпаки.

Список використаних джерел:

1. Wahab I. AI in Policing: Trends, Applications, and Challenges. 2025. URL: https://www.legalserviceindia.com/Legal-Articles/ai-in-policing-trends-applications-and-challenges/

2. Predictive Policing Technologies: Market Growth and Ethical Considerations. 2025. URL: https://www.platformexecutive.com/insight/technology-research/predictive-policing-technologies-market-growth-and-ethical-considerations/

3. Global Artificial Intelligence (AI) In Predictive Policing Market To Reach $29.93 Billion By 2029 Growth Rate Of 50.7%. 2025. URL: https://www.einpresswire.com/article/816138662/global-artificial-intelligence-ai-in-predictive-policing-market-to-reach-29-93-billion-by-2029-growth-rate-of-50-7

4. Зачек О.І, Дмитрик Ю.І., Сеник В.В. Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності. *Науковий вісник Львівського державного університету внутрішніх справ.* 2023. Серія юридична. №3. С. 148-156. DOI: https://doi.org/10.32782/2311-8040/2023-3-19

5. Актуальні проблеми державотворення та правотворення: конституційні, загальнотеоретичні та філософсько-правові аспекти: *монографія* / кол. авт.; за заг. ред. Д. Забзалюка. Львів: Растр-7, 2026. С. 51-73.

6. Про Національну поліцію: Закон України від 02.07.2015 №580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text

7. Про захист персональних даних: Закон України від 01.06.2010 №2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

8. Штучний інтелект на службі в правоохоронців: майбутнє вже зараз. *НАВС*. 2026. URL: https://www.navs.edu.ua/news/shtuchnij-intelekt-mozhlivosti-ta-zagrozi-dlya-profesijnoyi-diyalnosti-pravoohoronciv.html

9. Lau T. Predictive Policing Explained. 2020. URL: https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained

10. Lee Y., Bradford B., Posch K. The Eff ectiveness of Big Data-Driven Predictive Policing: Systematic Review. *Justice Evaluation Journal*. 2024. Vol. 7. Iss. 2. P. 127-160. DOI: https://doi.org/10.1080/24751979.2024.2371781

11. Taka E., Lawal T., Calder M., Sevegnani M., Kotsoglou K., McClory-Tiarks E., Oswald M. Mapping the Probabilistic AI Ecosystem in Criminal Justice in England and Wales. DOI: https://doi.org/10.48550/arXiv.2512.04116

12. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 №2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

13. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

Басиста І.В.
професорка кафедри права
імені академіка УАН о. Івана Луцького
д.ю.н., професорка
(Університет Короля Данила)
Членкиня Науково-консультативної ради
при Верховному Суді

ЗАСТОСОВНІСТЬ ТЕХНОЛОГІЙ ШІ У ЕКСПЕРТНИХ МЕТОДИКАХ ЗАДЛЯ ФОРМУВАННЯ ДОСТОВІРНОЇ ТА ДОПУСТИМОЇ ДОКАЗОВОЇ БАЗИ ТА КРАЙНІ ВИЯВЛЕНІ РИЗИКИ ТА ВСТАНОВЛЕНІ ОБМЕЖЕННЯ ЩОДО ТЕХНОЛОГІЇ

Умови технологічного розвитку дозволяють осучаснення чималої кількості галузей та діяльностей, але безпечний розвиток людства вимагає формуванню *збалансованої моделі взаємодії людини і технологій* і кримінальна процесуальна діяльність, звісно, не є винятком. Вже підкреслювалося [1, с. 388-405], що якщо «технічна сторона розслідувань» у криміналістичних цілях ефективно послуговується інструментами ШІ та алгоритмічними рішеннями, то із так званою «правовою» ситуація дещо складніша і це закономірно не лише для українських реалій, виходячи із вимог процесуальних законодавств щодо допустимості та достовірності доказів [1, с. 388-405]. Авторами аналізувалася судова практика США та ЄС щодо допустимості доказів, отриманих за допомогою ШІ, та зроблено спробу визначити таке поняття, як «докази згенеровані ШІ» [2]. Загалом простежується така тенденція, що закритість технології, нерозуміння отримувачем послуги та суб'єктом, який наприкінці оцінює здобуті результати (як от суддя по відношенні до результатів досудового розслідування) ланцюжка генерації ШІ «продукту», унеможливлює сприйняття такого отриманого результату, як допустимого та достовірного, зокрема і судом у доказуванні [2].

Є й інша ситуація, зокрема, якщо наявний висновок спеціаліста, експерта, який у процесі свого дослідження застосував

ту чи іншу технологію, але про відповідальність, зокрема і кримінальну, попереджена людина-спеціаліст чи експерт, то його висновок цілком може визнаватися допустимим та достовірним доказом. Звісно на національному рівні постає питання узаконення тих чи інших експертних методик із застосуванням технологій ШІ, на кшталт судових психологічних експертиз із використанням поліграфа [3] тощо. Бо направду, лише правильно обраний вектор кримінальної процесуальної та експертної діяльності здатен у їх симбіозі убезпечити від подальших порушень прав і свобод громадян у перебігу формування доказової бази із залученням технологій ШІ. Розвитку та технологізації не потрібно та не варто уникати, а слід впроваджувати ті правові механізми, які гарантуватимуть контроль технології людиною та всеохоплюючу відповідальність людини за здобуті результати. Як влучно зазначає М.В. Карчевський, «в умовах, коли значна частина людства зайнята в процесах інформатизації та комп'ютеризації, коли у цій сфері розміщуються фінансові інвестиції та отримуються істотні прибутки….» [4, с. 6], а, логічне, і вчиняються кримінальні правопорушення, «…виникає потреба у їх правовому регулюванні. Право дає змогу забезпечити баланс соціальних переваг і ризиків інформаційних технологій» [4, с. 6]. І це вірний шлях для модернізації діяльності.

При цьому, слід зауважити, що судячи із крайнього із рішень Верховного Суду, а саме у господарській справі №925/496/24, то відповіді штучного інтелекту не можуть розглядатися, як джерело достовірної науково доведеної інформації «на противагу висновкам, що були зроблені судом першої інстанції в судовому рішенні» [5]. Відповіді двох штучних інтелектів щодо підтвердження буквального трактування підпункту 6 п. 23 договору, а саме: Grok (розроблений компанією XAI) і ChatGPT (розроблений компанією OpenAI) не було оцінено судом як електронні докази [5], що є цілком очевидним, виходячи із доктринальних розумінь цих доказів та наявної слідчої і судової практики [6]. У своєму рішенні Верховний Суд виснував, що учасник не вірно використав технологію штучного інтелекту, тобто «…не як засіб сприяння здійсненню належного правосуддя, а навпаки – з метою заперечення (ставлення під сумнів, оскарження) вже зроблених судом висновків» [7]. Схожий за

підходом до оцінки, але не аналогічний висновок Суду вже мав місце у 2024 році у справі № 925/200/22 (ухвала від 08.02.2024), де йшлося про неповагу до суду, але через відсутність контекстного пояснення у самому судовому рішенні, у чому проявилася «неповага», не сприймався науковою спільнотою, як і практиками, та піддавався критиці [8, с. 78-81]. Тобто у цьому рішенні Верховний Суд, на відміну від рішення за 2024 рік, вже розтлумачив «контекст» у своєму висновку.

Про те, що ШІ здатен вводити в оману очевидно вже написано сотню разів [9]. У 2025 році тестування функції підсумування довгих статей ШІ показало недолугі результати його роботи та брехню [9]. «Дослідники OpenAI випробували метод нагляду для зменшення кількості хибних відповідей ChatGPT, але зауваження через брехню лише змушували моделі штучного інтелекту брехати вправніше» [10]. Анастасія Печенюк наводить результати дослідження фахівці Columbia Journalism Review. Було доказано, що моделі штучного інтелекту неправильно надавали джерела новин в середньому у понад 60% випадків. Рівень помилок помітно відрізнявся серед протестованих платформ. Perplexity надав неправильну інформацію в 37% випадків, тоді як ChatGPT Search – у 67%. Grok 3 продемонстрував найвищий рівень помилок– 94% [11]. У літературі описана і проблема із *«навченим обманом*» [12], тобто доведено, що технології ШІ здатні бути ефективними маніпуляторами, зокрема і щодо сприйняття людиною певних подій чи дій, але це не власна «якість розуму ШІ», а навчання ШІ брехні людиною-розробником.

Всім нам відомі випадки, коли людна довіряє ШІ кінцевий висновок і не аналізує результати «його роботи». І наслідки логічні – для прикладу, посилання адвоката на неіснуючі судові справи та введення іншої сторони чи (та) суду в оману, у кінцевому результаті слугують підставою притягнення його до встановленої відповідальності [13] і таких ситуацій у закордонній практиці десятки. Очевидно, як результат, згодом ми будемо свідками позитивних наслідків від цього, коли захисники та інші суб'єкти, у нашому випадку кримінального процесу (слідчі, детективи, прокурори, дізнавачі, оперативні працівники та ін.), пригадають про дамоклів меч репутації, високі стандарти та основний обов'язок – служіння суспільству і відповідальність

перед суспільством. Бо вже «…потім йдеться про служіння закону, юридичну практику, дотримання процедур та, власне, юридичний бізнес» [14].

Що ж стосується крайніх виявлених ризиків технології, то щодо «найнебезпечнішого» із них вельми аргументовано і влучно висловився філософ Кембриджського університету доктор Том Макклелланд і, як його цитують видання, зауважив, що «… інструменти для визначення свідомості штучного інтелекту не просто відсутні – їх може ніколи не існувати. У журналі Mind and Language цей дослідник стверджує, що це не тимчасова прогалина у науці, а глибша проблема: людство досі не має чіткого розуміння самої природи свідомості. Без цього, каже Макклелланд, будь-які спроби виявити її у машинах залишаються чистою спекуляцією» [15]. Попри це, віра в свідомий ШІ зростає. «Макклелланд розповів, що отримував листи від користувачів чат-ботів, у яких ті переконували його, що машина стала самосвідомою. Він застерігає, що емоційні зв'язки, побудовані на хибних уявленнях, можуть стати небезпечними. У світі, де машини дедалі краще імітують людську поведінку, ілюзія усвідомленості стає сильнішою – хоч і не ближчою до істини. На сьогодні, каже Макклелланд, у нас немає засобів перевірити, чи ШІ справді свідомий – і, можливо, їх ніколи не буде» [15].

Для прикладу, у сфері охорони здоров'я технології ШІ оптимізували велику кількість процесів, діагностик тощо. При цьому, ШІ, який аналізує зрізки тканин при діагностиці пухлин, вміє визначати расу, стать і вік пацієнта – тоді як лікар цього зробити не може. Саме тому точність діагностики ШІ відрізняється для різних груп пацієнтів. Дослідники Гарвардської медичної школи перевірили чотири широко вживані моделі глибокого навчання, призначені для діагностики раку. Аналіз охопив патологічні зразки тканин з 20 різними типами раку. Результати виявили системні відмінності в точності штучного інтелекту: ШІ-моделі гірше працювали в певних демографічних групах, визначених за расою, статтю та віком. Наприклад, ШІ важче розрізняв підтипи раку легені у чоловіків й афроамериканців. Точність машини також знижувалася при класифікації підтипів раку молочної залози в пацієнтів молодшого віку. Загалом такі розбіжності виявлялися приблизно в 29%

діагностичних завдань. Дослідники визначили три основні причини проблем з точністю ШІ-діагностики та виявили, що основоположна проблема насправді є значно глибшою»: в окремих випадках ШІ-моделі псували діагностику для певних груп навіть при однаковому розмірі вибірки. Наразі команда дослідників працює з медзакладами по всьому світу, вивчаючи упередженість ШІ в регіонах із різною демографією й клінічними практиками та адаптуючи FAIR-Path для ситуацій з обмеженими даними [16].

При цьому, позови щодо компаній-розробників наявні, зокрема, серед крайніх із них, то «…компанію Character.AI звинуватили у порушенні законів про захист даних. Штат Кентуккі подав судовий позов проти компанії-розробника чат-ботів Character.AI та її засновників, звинувативши їх у порушенні законодавства про безпеку дітей і захист персональних даних, пише therecord.media. Генеральний прокурор Кентуккі вимагає накладення цивільних штрафів, а також судової заборони на подальше використання Character.AI того, що в позові названо «небезпечною технологією, яка спонукає користувачів розкривати свої найінтимніші думки й емоції та маніпулює ними за допомогою часто небезпечних взаємодій і порад. Деякі чат-боти Character.AI засновані на популярних дитячих персонажах із Sesame Street, Paw Patrol, Bluey та мультфільмів Disney. Водночас, за даними позову, попри «дитячий» вигляд, деякі з цих ботів вступають у сексуалізовані розмови та «знецінюють зловживання психоактивними речовинами, самоушкодження, агресію і насильство». Character.AI також звинувачують у причетності щонайменше до двох самогубств підлітків. У поданих позовах стверджується, що діти вкоротили собі віку після тривалого спілкування з чат-ботами платформи» [17]. «Іспанська влада звернулася до прокуратури з вимогою розпочати кримінальне розслідування щодо X, Meta та TikTok. Це пов'язано зі створенням та поширенням сексуалізованих діпфейків за допомогою їхніх інструментів штучного інтелекту [18]. Про це повідомляють українські засоби публічної інформації із покликанням на Euractiv [18]. «Про ініціативу оголосив прем'єр-міністр Іспанії Педро Санчес, заявивши, що такі платформи завдають шкоди психічному здоров'ю, гідності та правам дітей. За його словами, держава не може допустити, щоб алгоритми соціальних мереж посилювали

потенційну шкоду для неповнолітніх. Найбільше уваги регуляторів досі привертала платформа X Ілона Маска та її ШІ-асистент Grok, який із кінця минулого року активно використовувався для створення та поширення згенерованих зображень, що цифровим способом «роздягали» жінок і дітей. Водночас іспанська ініціатива може стати першим розслідуванням, яке поширюється не лише на X, а й на Meta та TikTok. Паралельно з цим у Європейському Союзі зростає регуляторний тиск на технологічні платформи. Європейська комісія наприкінці січня розпочала власне провадження щодо X у межах Закону про цифрові послуги. Також Ірландська комісія з питань захисту даних відкрила розслідування діяльності Grok у контексті загального регламенту захисту даних. У Європарламенті тим часом обговорюють можливість загальноєвропейської заборони інструментів так званої ШІ–«порнофікації», а також тривають переговори щодо криміналізації створення матеріалів сексуального насильства над дітьми, згенерованих за допомогою штучного інтелекту [18]. Навіть «Управління з питань кіберпростору Китаю (CAC) опублікувало для громадського обговорення проект заходів щодо регулювання діяльності ШІ-сервісів у країні» [19], повідомило агентство Reuters і на нього покликаються українські медіа. «Запропоновані управлінням правила будуть застосовуватися до продуктів і сервісів, які використовують технології ШІ для імітації рис людської особистості, моделей мислення та стилів спілкування, а також забезпечують емоційне взаємодію з користувачами в Китаї через текст, зображення, аудіо або відео, повідомляється на сторінці CAC у соціальній мережі WeChat. Регулятор зазначив, що проект базується на всебічному, зваженому та багаторівневому підході до регулювання з диференційованим контролем залежно від рівня ризику, що забезпечує як підтримку інновацій, так і захист від зловживань. Проектом забороняється створення та розповсюдження контенту, який загрожує національній безпеці, завдає шкоди національній честі або інтересам, підриває етнічну єдність, пропагує незаконну релігійну діяльність, поширює чутки, що порушують економічний або соціальний порядок, а також містить порнографію, включає азартні ігри, насильство або підбурювання до вчинення злочину. Також забороняється випуск

контенту, який заохочує або романтизує самогубство чи самопошкодження, а також такі дії, як словесні образи чи емоційні маніпуляції, які можуть завдати шкоди фізичному або психічному здоров'ю користувачів або призвести до підриву їхньої гідності. Відповідно до документа, провайдери ШІ-сервісів повинні брати на себе відповідальність за питання безпеки протягом усього життєвого циклу продукту та створювати системи для перевірки алгоритмів, захисту даних і охорони особистої інформації. Провайдери повинні інформувати користувачів про те, що вони взаємодіють з ШІ, а не з людиною, і попереджати їх про шкоду від надмірного використання» [19].

І, насамкінець, варто зауважити, що в українських засобах публічної інформації у першій декаді лютого поточного року із покликанням на Politico було поширено інформацію про те, що «Європейський парламент вимкнув вбудовані функції штучного інтелекту на робочих пристроях депутатів і співробітників через побоювання щодо кібербезпеки й захисту даних. Про це повідомляло Politico з посиланням на внутрішній лист, розісланий працівникам інституції. На корпоративних планшетах відключили «вбудовані функції штучного інтелекту» після того, як ІТ-департамент Європарламенту заявив, що не може гарантувати безпеку даних, які обробляють ці інструменти. У листі зазначається, що частина функцій використовує хмарні сервіси для виконання завдань, які могли б оброблятися локально. Це означає, що дані можуть передаватися за межі пристрою. Працівникам також рекомендували застосовувати аналогічні запобіжні заходи на приватних пристроях, особливо якщо вони використовуються для роботи. Депутатів закликали не надавати функціям ШІ, які сканують або аналізують контент, доступ до службової пошти та внутрішніх документів, а також обережно ставитися до сторонніх застосунків. У відповіді на запит Politico Європарламент не уточнив, які саме функції були вимкнені та на яких операційних системах працюють службові пристрої. У 2023 році парламент заборонив застосунок TikTok на службових пристроях співробітників і рекомендував депутатам видалити його з особистих телефонів» [20]. Отож, тем для роздумів більш, ніж достатньо…

Список використаних джерел:

1. Басиста І.В. Використання ШІ в криміналістичних цілях та співвіднесення із допустимістю зібраних доказів: огляд сучасного стану справ: розділ у монографії «Нове століття криміналістики та судових наук: Liber Amicorum на честь академіка В. Ю. Шепітька»: монографія / [М. Шепітько, А. Гетьман, В. Журавель та ін.] ; Нац. юрид. ун-т ім. Ярослава Мудрого ; Нац. акад. прав. наук України ; Міжнар. конгрес криміналістів ; [за ред. М. В. Шепітька]. Харків : Право, 2026. С. 388–405. https://dspace.nlu.edu.ua/handle/123456789/20701

2. Орищук В. Докази, отримані за допомогою штучного інтелекту, та їх використання в суді. 2.10.2025. https://www.hsa.org.ua/blog/dokazi-otrimani-za-dopomogoiu-stucnogo-intelektu-ta-yix-vikoristannia-v-sudi

3. https://polygraph.ua/ekspertyzy/

4. Карчевський М.В. Кримінальне право в умовах цифрової трансформації. Від несанкціонованого доступу до «jailbreak» штучного інтелекту»: монографія. Університет Короля Данила; Ін-т інформації, безпеки і права Нац. акад. прав. наук України. Харків: Право, 2025. 176 с.

5. https://7eminar.ua/news/11526-comu-vs-vidxiliv-dokazi-vid-si

6. Гаврилюк Л. В., Басиста І. В., Афонін Д. С., Шевчишен А. В. та ін. Використання електронних доказів під час досудового розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку (Протокол Берклі): (наук.-практ. порадник). Київ : ДНДІ МВС України; Вид-во «Політехніка», 2024. 196 с. https://rep.dnuvs.ukr.education/handle/123456789/4178 https://www.researchgate.net/publication/385514719_Vikoristanna_elektronnih_dokaziv_pid_cas_dosudovogo_rozsliduvanna_zlociniv_proti_miru_bezpeki_ludstva_ta_miznarodnogo_pravoporadku_Protokol_Berkli_naukovo-prakticnij_poradnik?fbclid=IwY2xjawHkqitleHRuA2FlbQIxMAABHR0H3PLkRS0-pRUg4ZxJ8b3Yn35HF_1-JWpuBHLu2lMXNibFyiR2cKlgwg_aem_Un_o_sP6mw83lJaKOeeZog

7. Постанова Касаційного господарського суду Верховного Суду від 8 липня 2025 року по справі №925/496/24. https://reyestr.court.gov.ua/Review/128775966

8. Гловюк І.В. Покликання стороною провадження на результати, згенеровані ChatGPT: чи це неповага до суду? Штучний інтелект у правовій практиці: межі та можливості : збірник тез круглого столу (14 березня 2025 року) / упор. О. О. Барабаш. Львів : ЛьвДУВС, 2025. С. 78–81.

9. Надія Баловсяк Коли контент стає сміттям. Як штучний інтелект руйнує інтернет. 29.06.2025. https://www.dsnews.ua/ukr/society/koli-kontent-staye-smittyam-yak-shtuchniy-intelekt-ruynuye-internet-29062025-524517

10. Печенюк Анастасія Ситуація патова. Моделі OpenAI дуже вправно брешуть – розробники не знають, що з цим робити. 24.03.2025. https://techno.nv.ua/ukr/popscience/brehnya-chatgpt-50500121.html

11. Печенюк Анастасія Центр цифрової журналістики Columbia Journalism Review виявив серйозні проблеми з точністю генеративних моделей штучного інтелекту, які використовуються для пошуку новин. 16.03.2025. https://techno.nv.ua/ukr/popscience/shi-ta-novini-50498216.html

12. Печенюк Анастасія Дослідники виявили, що багато популярних систем штучного інтелекту вже здатні обманювати людей. Поки цю здатність вони проявляють передусім в іграх, але ситуація може змінитися. 26.05.2024. https://techno.nv.ua/ukr/popscience/brehnya-shtuchnogo-intelektu-50421250.html

13. У США покарали адвоката через використання ChatGPT для складання судового документа. 4 червня 2025. https://internetua.com/u-ssha-pokarali-advokata-cserez-vikoristannya-chatgpt-dlya-skladannya-sudovogo-dokumenta?utm_source=ukrnet_news

14. Олександр Черних. Українські адвокати мають у Британії пільгове визнання статусу, – представник НААУ в Шотландії. 14.07.2023. https://unba.org.ua/publications/print/8180-ukrains-ki-advokati-mayut-u-britanii-pil-gove-viznannya-statusu-predstavnik-naau-v-shotlandii.html

15. Британський науковець заявив, що свідомість штучного інтелекту неможливо перевірити. 9.01.2026. https://internetua.com/britanskii-naukovec-zayaviv-sxo-svidomist-shtucsnogo-intelektu-nemojlivo-pereviriti?utm_source=ukrnet_news

16. Штучний інтелект розпізнає рак, але водночас «бачить» демографію пацієнта – і це проблема. 29.12.2025. https://thepharma.media/uk/news/40603-stucnii-intelekt-rozpiznaje-rak-ale-vodnocas-bacit-demografiyu-pacijenta-i-ce-problema-29122025

17. У США влада Кентуккі подала позов проти розробника ШІ-ботів, звинувативши його у шкоді для дітей. 13.01.2026. https://sud.ua/uk/news/abroad/350792-v-ssha-vlasti-kentukki-podali-isk-protiv-razrabotchika-ii-botov-obviniv-ego-v-prichinenii-vreda-detyam

18. Іспанія вимагає кримінального розслідування щодо X, Meta та TikTok через ШІ-діпфейки. 17.02.2026. https://internetua.com/ispaniya-vimagaye-kriminalnogo-rozsliduvannya-sxodo-x-meta-ta-tiktok-cserez-shi-dipfeiki?utm_source=ukrnet_news

19. Китай представив жорсткі правила для ШІ, який «веде себе як людина». 28.12.2025. https://toneto.net/news/tehnologii/kitay-predstaviv-gorstk---pravila-dlya-sh----yakiy---vede-sebe-yak-lyudina---

20. Маймур Ірина Європарламент заблокував ШІ на пристроях працівників через побоювання щодо кібербезпеки. 12.02.2026. https://bzh.life/ua/novyny/1771353008-evroparlament-zablokuvav-shi-na-pristroyah-pratsivnikiv-cherez-poboyuvannya-shchodo-kiberbezpeki/

Бенза В.І.
студентка
навчально-наукового інституту права та психології
(Національна академія внутрішніх справ)
Козачина А.М.
старший викладач
кафедри кримінального права та кримінології,
доктор філософії
(Національна академія внутрішніх справ)

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ СТУДЕНТІВ В УМОВАХ ЦИФРОВІЗАЦІЇ ОСВІТИ

У XXI столітті цифрові технології стали невід'ємною складовою системи освіти. Від електронних журналів і дистанційних курсів до використання штучного інтелекту для оцінювання знань – освітній процес дедалі більше переходить у цифровий формат. Однак разом із цим постає серйозна проблема – забезпечення належного рівня захисту персональних даних студентів, які обробляються у великих обсягах через електронні освітні системи.

В умовах війни та кібератак на державні ресурси України питання інформаційної безпеки набуває ще більшої актуальності. За даними Державної служби спеціального зв'язку та захисту інформації України, лише у 2024 році кількість спроб несанкціонованого доступу до освітніх баз даних зросла на 37 % [1].

Крім того, сучасна молодь активно користується мобільними додатками, соціальними мережами та хмарними сервісами, у яких також можуть зберігатися навчальні або особисті дані. Це створює додаткові ризики порушення права на приватність, гарантованого ст. 32 Конституції України та міжнародними актами, зокрема Конвенцією про захист осіб у зв'язку з автоматизованою обробкою персональних даних (1981 р.) [2].

Таким чином, питання захисту персональних даних студентів є не лише технічним чи адміністративним, а й правовим та етичним завданням, яке потребує системного підходу.

Відповідно до Закону України «Про захист персональних даних» персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути ідентифікована [3]. У контексті освітнього процесу це може бути: прізвище, ім'я, по батькові; ідентифікаційний код; паспортні та контактні дані; інформація про успішність, результати іспитів, поведінку; медичні довідки, соціальні пільги, адреси проживання тощо.

Заклади освіти виступають володільцями баз персональних даних, а працівники – розпорядниками. Це покладає на них обов'язок забезпечити збір, зберігання, використання та поширення інформації відповідно до вимог закону та лише з визначеною метою – реалізацією освітнього процесу [4, с. 33].

У сучасному навчальному середовищі персональні дані студентів обробляються за допомогою численних цифрових платформ:

- Системи управління навчанням (LMS) — Moodle, Canvas, Google Classroom;
- Інформаційно-аналітичні системи університетів (наприклад, ЄДЕБО);
- Електронна пошта та корпоративні хмари (Google Workspace, Microsoft 365);
- Сервіси відеоконференцій (Zoom, Teams, Meet);
- Бази обліку результатів навчання та стипендіального забезпечення.

Переваги таких технологій очевидні – оперативність, прозорість, доступність інформації. Але водночас зростає ризик витоку даних, фішингових атак, несанкціонованого копіювання інформації або її передачі третім особам без згоди студента [6, с. 71].

Захист персональних даних студентів передбачає комплекс організаційних, технічних і правових заходів. Серед основних:

- обмеження доступу до баз даних лише уповноваженим працівникам;
- використання паролів і двофакторної аутентифікації;
- резервне копіювання та шифрування інформації;
- аудит інформаційних систем;

– розроблення внутрішніх політик конфіденційності [7, с. 36].

Однак у більшості навчальних закладів України ці заходи реалізовані лише частково. Часто відсутня посада фахівця із захисту персональних даних (Data Protection Officer), а викладачі не проходять навчання з питань кібергігієни/

Порушення конфіденційності може мати не лише юридичні, а й соціальні наслідки – дискримінацію, психологічний тиск або втрату репутації. Наприклад, витік даних про академічну успішність чи дисциплінарні стягнення може стати підставою для кібербулінгу або маніпуляцій [8, с. 89].

Таким чином, цифровізація освіти потребує переосмислення етичних стандартів роботи з інформацією, особливо коли йдеться про неповнолітніх студентів і учнів.

У свою чергу, на нашу думку, в Україні залишається низка невирішених проблем:

1. Недосконаліть законодавства. Закон «Про захист персональних даних» не деталізує специфіку освітньої сфери та не враховує нові цифрові ризики – хмарні сервіси, штучний інтелект, біометричну ідентифікацію.

2. Відсутність уніфікованих стандартів. Немає єдиної політики безпеки для всіх закладів освіти, що призводить до хаотичності підходів до обробки інформації.

3. Недостатня кваліфікація персоналу. Більшість працівників не проходять навчання з питань інформаційної безпеки та не усвідомлюють юридичних наслідків порушень.

4. Технічна вразливість систем. Часто університетські платформи працюють без сертифікованих систем захисту, резервного копіювання чи шифрування.

5. Використання закордонних платформ. Передача даних на сервери за межами України без чіткої правової бази створює потенційні загрози національній безпеці.

Підсумовуючи, слід зазначити, що захист персональних даних студентів є стратегічним напрямом формування безпечного освітнього середовища. Цифровізація освіти відкриває нові можливості, проте водночас підсилює ризики кіберзагроз.

Необхідність удосконалення законодавчої бази, створення інституційної системи управління безпекою та підвищення

обізнаності учасників освітнього процесу є ключовими умовами забезпечення цифрової довіри в освітній сфері.

Список використаних джерел:

1. Державна служба спеціального зв'язку та захисту інформації України. Аналітичний звіт про кіберінциденти, 2024 р. URL: https://cip.gov.ua/ua/statics/analitichni-materiali-derzhspeczv-yazku

2. Конституція України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80

3. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

4. Бурлака В. Захист інформації у вищій школі: правові аспекти. *Право України*. 2022. № 5. С. 31-37.

5. Гуменюк І. В. Цифровізація освіти: ризики для захисту персональних даних. *Інформаційне право України*. 2022. № 3. С. 85–92.

6. Гайдай О. Інформаційна безпека в освітньому процесі. П*раво та інновації*. 2023. № 1. С. 70–78.

7. Петренко С. Проблеми правового регулювання обробки персональних даних у сфері освіти. *Юридична наука*. 2023. № 2. С. 35–40.

8. Мельник Р. Цифрова безпека у вищій освіті: виклики та перспективи. *Освітній простір*. 2024. № 4. С. 88–93.

Білий І.О.
курсант
навчально-наукового інституту поліцейської діяльності
(Національна академія внутрішніх справ)

ШТУЧНИЙ ІНТЕЛЕКТ ЧИ ЛЮДСЬКИЙ РЕСУРС

2 грудня 2020 року Кабінет Міністрів України затвердив розпорядження «Про схвалення Концепції розвитку штучного інтелекту в Україні». Цей документ розрахований до 2030 року й визначає головні напрями, цілі та принципи впровадження технологій ШІ в нашій державі. Автори Концепції переконані, що розвиток штучного інтелекту допоможе Україні стати більш конкурентоспроможною на світовій арені та сприятиме зростанню інклюзивності. У ній окреслено вісім ключових сфер державної політики щодо ШІ: освіта й людський капітал; наука та інновації; економіка й бізнес; кібербезпека; оборона та безпека; державне управління; правове регулювання й етика; правосуддя.

Штучний інтелект – це, мабуть, один із найбільших винаходів людства, який серйозно змінює наше життя: він полегшує виконання рутинних справ і пришвидшує вирішення більшості завдань. Але важливо не забувати про захист прав людини. Основним принципом регулювання ШІ має бути підтримка його розвитку та запобігання негативним наслідкам [1].

Штучний інтелект – це здатність машин імітувати людське мислення та когнітивні функції. Тобто вони збирають і аналізують зовнішні дані, а на їх основі вчаться приймати рішення й робити висновки – приблизно як людина. ШІ умовно ділять на два типи: слабкий (вузький) і сильний (повний). Слабкий ШІ – це технології, які перевершують людину в якійсь конкретній галузі. Найочевидніші приклади – голосові асистенти Alexa, Google Assistant або Siri. Сюди ж належать безпілотні авто, боти в ритейлі, системи розпізнавання облич, спам-фільтри й навіть пошуковий бот Google. Сильний ШІ дозволяє машині використовувати набуті знання й навички в різних сферах. Його будова й можливості максимально наближені до людського розуму, він здатен самостійно вчитися й виконувати завдання. Щоправда, поки що це лише теорія. Навіть щоб просто зрівнятися з мозком за

потужністю, такій системі потрібна обчислювальна здатність понад 1 екзафлопс – саме стільки, за оцінками, має людський мозок.

Хоча ШІ поступово входить у наше повсякдення, багато хто досі сприймає його як щось із фантастики — далеке й незрозуміле. Але ми щодня користуємося такими інструментами, навіть не замислюючись. Наприклад, Google Maps використовує ШІ, щоб аналізувати швидкість руху, попереджати про аварії чи ремонти. А Spotify вивчає наші вподобання й пропонує музику, яка може сподобатися.

Загалом під штучним інтелектом розуміють комплекс технологій, які виконують «інтелектуальну» роботу без участі людини. Нещодавно ШІ вийшов на новий рівень: тепер він може писати зв'язні тексти, відповідати на запитання й навіть створювати ілюстрації. За даними звіту CVL Economics за січень 2024 року, 36% керівників індустрії розваг, які використовують генеративний ШІ, помітили, що для виконання повсякденних завдань тепер потрібно менше навичок. У дослідженні взяли участь 300 керівників із шести секторів розваг. Виявилося, що 75% із них скоротили персонал через інструменти Gen AI. Найбільше від цього постраждали кіно та анімація.

Минулого року, невдовзі після запуску ChatGPT, Гільдія письменників Америки (WGA) та Гільдія кіноакторів (SAG-AFTRA) влаштували страйк через побоювання, що ШІ вплине на їхні робочі місця та безпеку. Навіть після нещодавніх переговорів з Альянсом продюсерів, члени цих гільдій усе ще стурбовані невизначеністю щодо впливу Gen AI на кіно й телебачення [2].

У звіті прогнозують, що протягом найближчих трьох років найбільше постраждають звукорежисери – так вважають 55% керівників. Понад 40% опитаних сказали, що під загрозою музичні редактори, аудіотехніки та звукорежисери, а 33% очікують, що проблеми торкнуться авторів пісень, композиторів і студійних інженерів. Ще 44% респондентів думають, що Gen AI зможе забезпечити якісний дубляж для різних мов у фільмах і телешоу. У звіті також згадується, що на початку 2024 року звільнення відбулися в таких компаніях, як Riot Games, Unity Software, Amazon MGM Studios, Pixar та Universal Music Group. У CVL Economics прогнозують, що скорочення триватимуть і далі.

Песимісти лякають: а раптом у ШІ з'явиться щось схоже на особистість, адже він думає швидше за людину й може вийти з-під контролю? Оптимісти ж вважають, що свідомості в нього ніколи не буде, тож просто треба навчитися правильно його використовувати. Незважаючи на величезний потенціал ШІ, науковці розділилися на два табори: одні вірять у його користь, інші попереджають, що він здатен знищити людство. Тут важливо знайти золоту середину й пам'ятати: штучний інтелект не відчуває, не має емоцій і не усвідомлює себе.

Список використаних джерел:

1. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. Офіційний веб-сайт Верховної Ради України «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show (дата звернення 11.03.2026)

2. Барбашин Сергій. Штучний інтелект: правове регулювання в Україні та ЕС. URL https://barbashyn.law/statti/shtuchnyj-intelekt-pravove-regulyuvannya-v-ukrayini-ta-yes/ (дата звернення 11.03.2026)

Білик В.М.
професор кафедри поліцейської діяльності,
кандидат юридичних наук, доцент
(*Національна академія внутрішніх справ*)

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ: ОРГАНІЗАЦІЙНО-ПРАВОВІ ТА ЕТИЧНІ АСПЕКТИ

Стрімкий розвиток цифрових технологій у сучасному суспільстві сприяє активному впровадженню інноваційних рішень у сфері публічного управління та правоохоронної діяльності. Одним із ключових напрямів такої трансформації є використання технологій штучного інтелекту (далі – ШІ), що відкриває нові можливості для підвищення ефективності діяльності правоохоронних органів, у тому числі Національної поліції України. У сучасних умовах забезпечення публічної безпеки та правопорядку, особливо в період воєнного стану, застосування інтелектуальних цифрових технологій набуває особливого значення.

Загалом під штучним інтелектом у науковій літературі розуміють комплекс технологій та алгоритмів, здатних імітувати інтелектуальні процеси людини, зокрема аналіз даних, прогнозування, прийняття рішень та навчання на основі отриманих результатів. Використання таких технологій у правоохоронній діяльності сприяє автоматизації значної частини аналітичних і управлінських процесів, підвищує оперативність реагування на правопорушення та сприяє більш ефективному використанню ресурсів правоохоронних органів.

У діяльності Національної поліції України перспективними напрямами застосування технологій ШІ можуть бути інформаційно-аналітичне забезпечення правоохоронної діяльності, прогнозування криміногенної ситуації, автоматизований аналіз великих масивів даних, розпізнавання облич і номерних знаків транспортних засобів, а також удосконалення систем відеоспостереження. Застосування таких технологій дозволяє

підвищити ефективність виявлення правопорушень, сприяти оперативному встановленню осіб, причетних до їх вчинення, та оптимізувати управлінські процеси в системі поліції [1].

Важливим напрямом використання ШІ є автоматизований аналіз великих масивів інформації, що надходить до інформаційно-комунікаційних систем правоохоронних органів. Такі системи можуть застосовуватися для виявлення закономірностей у кримінальній діяльності, аналізу оперативної інформації, а також формування прогнозів щодо можливого розвитку криміногенної ситуації на певних територіях. Це, у свою чергу, дозволяє більш ефективно планувати діяльність підрозділів поліції та здійснювати превентивні заходи.

Разом із тим використання технологій штучного інтелекту у правоохоронній діяльності пов'язане з низкою організаційно-правових викликів. Передусім ідеться про необхідність формування належної нормативно-правової бази, яка б регламентувала порядок застосування таких технологій, визначала межі їх використання та забезпечувала дотримання основоположних прав і свобод людини. Важливим є також забезпечення прозорості алгоритмів, що використовуються у процесі прийняття управлінських або процесуальних рішень [2].

Окрему увагу слід приділити питанням захисту персональних даних та інформаційної безпеки під час використання систем штучного інтелекту. Обробка значних обсягів інформації, у тому числі персональних даних громадян, потребує дотримання встановлених законодавством вимог щодо їх захисту та недопущення несанкціонованого доступу до відповідних інформаційних ресурсів [3].

Не менш важливими є етичні аспекти застосування технологій штучного інтелекту в діяльності правоохоронних органів. Серед основних ризиків, що обговорюються у міжнародній правовій та науковій спільноті, слід назвати можливість алгоритмічної дискримінації, упередженості автоматизованих систем, а також недостатню прозорість процесів прийняття рішень на основі алгоритмів. У зв'язку з цим використання ШІ у правоохоронній діяльності повинно ґрунтуватися на принципах законності, підзвітності, прозорості та дотримання прав людини [4].

Крім того, важливим є забезпечення належного рівня підготовки працівників поліції до використання сучасних цифрових технологій. Впровадження систем штучного інтелекту потребує розвитку цифрових компетентностей працівників правоохоронних органів, формування навичок роботи з інформаційно-аналітичними системами, а також розуміння можливостей і обмежень використання таких технологій у службовій діяльності.

У контексті інтеграції України до європейського правового простору особливого значення набуває врахування міжнародних стандартів і рекомендацій щодо використання штучного інтелекту в публічному управлінні та правоохоронній діяльності. Зокрема, важливими є положення міжнародних документів, спрямованих на забезпечення етичного та безпечного використання технологій ШІ, а також на запобігання порушенням прав людини у процесі їх застосування.

Таким чином, використання технологій штучного інтелекту в діяльності Національної поліції України має значний потенціал для підвищення ефективності правоохоронної діяльності, удосконалення інформаційно-аналітичного забезпечення та оптимізації управлінських процесів. Водночас впровадження таких технологій повинно супроводжуватися формуванням належного організаційно-правового механізму їх застосування, забезпеченням дотримання етичних стандартів та гарантій захисту прав і свобод людини.

Подальший розвиток зазначеного напряму потребує комплексного підходу, що включає удосконалення нормативно-правового регулювання, впровадження сучасних інформаційно-комунікаційних систем, підготовку кваліфікованих кадрів, а також розвиток міжнародного співробітництва у сфері використання штучного інтелекту в правоохоронній діяльності.

Список використаних джерел

1. Про схвалення Концепції розвитку штучного інтелекту в Україні: розпорядження Кабінету Міністрів України від 02.12.2020. № 1556-р. Дата оновлення: 29.12.2021. URL: https://zakon.rada.gov.ua/go/1556-2020-%D1%80 (дата звернення: 05.03.2026).

2. Європейська етична хартія щодо використання штучного інтелекту в судових системах та їхньому середовищі: Європейська комісія з питань ефективності правосуддя (CEPEJ), 3 – 4 груд. 2018. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://rm.coe.int/ru-ethical-charter-en-version-17-12-2018-mdl-06092019-2-/16809860f4 (дата звернення: 05.03.2026).

3. Про захист персональних даних: Закон України від 01.06.2010. № 2297-VI. Дата оновлення: 14.06.2025. URL: https://zakon.rada.gov.ua/go/2297-17 (дата звернення: 05.03.2026).

4. Recommendation on the Ethics of Artificial Intelligence від 23.11.2021. UNESCO. URL: https://unesdoc.unesco.org/ark:/48223/pf0000381137 (дата звернення: 05.03.2026).

Бортник Н.П.
завідувачка кафедри адміністративного
та конституційного права,
докторка юридичних наук, професорка
*(Національний кораблебудівний університет
імені адмірала Макарова)*
Єсімов С.С.
професор кафедри адміністративно-правових дисциплін,
кандидат юридичних наук, професор
(*Львівський державний університет внутрішніх справ)*

СУЧАСНІ ТЕНДЕНЦІЇ ІНФОРМАТИЗАЦІЇ ОСВІТИ

Інформаційні технології є невід'ємною частиною освітнього процесу. Процес освіти змінився, коли освіта стала переважно дистанційною. Зараз досить активно відбувається впровадження штучного інтелекту (ШІ) в різні напрями освіти. Інтенсифікуючи процес впровадження інформаційних технологій в освіту, не можна забувати про інформаційну безпеку, використовуючи тільки апробовані технології.

Розглядаючи накопичений досвід впровадження інформаційних технологій у сферу освіти, її цифровізацію, слід звернути увагу на накопичений європейський досвід. Проблемою поки залишається недостатнє ознайомлення педагогів з можливостями інформаційних технологій, але ця проблема поступово долається. Нові розробки знаходять застосування і служать на благо освіти.

У контексті інформатизації освіти слід торкнутися аспекту інформаційної відкритості. У доповіді Організації економічного співробітництва та розвитку «Погляд на освіту 2021» розрізняються три області відкритості, які мають значення для освіти (технічні та соціальні характеристики і характер ресурсів), які відстежують тенденції щодо технологічних аспектів (програмне забезпечення з відкритим вихідним кодом) [1].

Відкритість – це концепція, яка стала характеризувати системи знань і комунікації. По суті, відкритість у всіх вимірах відноситься до прозорості, яка є протилежністю секретності. Найчастіше ця прозорість розглядається з точки зору доступу до

інформації. Відкритість передбачає форму відкритого уряду, який вимагає, щоб громадяни мали доступ до офіційної інформації, щоб були представлені розумні підстави для приховування інформації від громадськості. Це основа руху за свободу інформації, яке призвело до прийняття законодавства, що стосується прав на інформацію.

Вільне поширення інформації означає, що громадськість має юридично закріплені права на доступ до інформації державних органів. Така свобода інформації розглядається як невід'ємна частина демократії, що є формою відкритого уряду, де прийняття урядових рішень на всіх рівнях є прозорим, публічні записи відкриті для громадського контролю, а особи мають права доступу до такої інформації.

З точки зору організації і інститутів відкритість стала означати певний режим роботи, що характеризується кооперативним або спільним управлінням, мотивованою вірою в те, що подібний підхід забезпечує набір принципів не тільки для громадянського суспільства, але й для державних і приватних організацій. Відкритість може бути витлумачена як доктрина, яка передбачає центральну роль науки і філософії як одного з центральних засобів досягнення раціонального суспільства, заснованого на відкритості для критики.

Освіта залежала від зміни інформаційних і комунікаційних технологій. Більш важливе питання полягає в тому, щоб зрозуміти, як нові технології, і особливо платформи та протоколи Web 2.0, сприяють повсюдному навчанню, яке руйнує простір між навчальним закладом і домом, створює нові форми суспільного виробництва, які необхідні для економіки знань.

Відкрита освіта і освіта в дусі відкритості – це взаємопов'язані проекти і одне із значних освітніх рухів, що поширилися в XXI столітті. Інформація є життєво важливим елементом «цифрової» політики і економіки, яка пов'язує простір, знання та капітал в мережевих практиках. Мережеві практики розвиваються або трансформуються в культуру знань.

Нормативне забезпечення цифровізації освітнього процесу передбачає таку побудову освітнього процесу, при якій всі учасники цієї діяльності будуть використовувати цифрові технології, розширюючи межі знання. Сучасні підходи до

формування цифрового освітнього середовища будуть спрямовані не тільки на підготовку та перепідготовку кваліфікованих кадрів, затребуваних сучасною економікою, а й на розробку цифрових рішень.

Цифрова трансформація необхідна для ефективності та результативності інформації, послуг і особистого досвіду, життєво важливих для зацікавлених сторін. Якщо говорити про напрями цифровізації – це великі платформні рішення, штучний інтелект та інформаційна безпека.

Керівники системи освіти хочуть вийти за рамки розрізнених цифрових інновацій і прийняти трансформаційне мислення, використовуючи технології як інструмент реалізації. Використання мобільних пристроїв учнями дозволяє вчителям успішно доставляти контент, забезпечувати підтримку та сприяти синхронному спільному навчанню.

Інтеграція цифрових рішень, наприклад, ігор, у викладання та навчальну діяльність дала вчителям можливість вивчати та застосовувати різні педагогічні практики.

Цифрові технології у сфері освіти означають, що буде новий підхід у галузі штучного інтелекту, наприклад, штучний інтелект, що все глибше проникає в життя, представляє математичний код, заснований на певних алгоритмах, що впливають на свідомість людей. Говорячи про тенденції, не можна оминути і штучний інтелект (ШІ).

Основними прикладами ШІ у сфері освіти є спеціальні платформи, які надають більш простий спосіб використання та отримання нових знань, тим більше що ми знаємо, що в країнах, що розвиваються, роль вчителя відіграє робот, однак у найближчому майбутньому штучний інтелект зможе самостійно змінювати існуючі коди і навіть створювати нові. Ця розробка вже знаходиться на зачатковій стадії в рамках так званої Індустрії 4.0 та Інтернету речей (IoT).

Забезпечення навчання цифровим навичкам і знайомство з новими цифровими інструментами може спонукати викладачів застосовувати різні технології на заняттях. Крім цифрової компетентності технічна підтримка впливає використання вчителями технологи.

Цифрові технології швидко прижилися у вишах. Головною перевагою месенджерів, інтегрованих у соціальні мережі, є те, що API доступний усім охочим. Широкий набір можливостей чат-бота дозволяє реалізовувати функціонал додатків, які можна порівняти з повноцінними сайтами. про ці можливості відносяться: автоматичне відправлення, обробка і отримання повідомлень; збереження інформації у базах даних; використання у повідомленнях більшості відомих форматів даних; робота всередині груп і каналів; можливість інтеграції з сторонніми сервісами, до віддаленого управління розумним будинком; створення html ігор; проведення фінансових операцій та багато іншого.

Перспективною можливістю для побудови комунікаційних процесів у закладі освіти є можливість автоматичного відправлення і обробки повідомлень.

Виші ведуть акаунти у соціальних мережах у комерційних цілях. Університетам важливо залучити якнайбільше талановитих та платоспроможних абітурієнтів.

Ефективна інтеграція інформаційних технологій на всіх рівнях освіти передбачає розвиток інфраструктури, надання цифрового контенту та вибір відповідних ресурсів, інформаційну відкритість закладів освіти, зокрема месенджерів у діяльності закладів освіти.

Список використаних джерел:

1. «Погляд на освіту 2021» – щорічна доповідь Організації економічного співробітництва та розвитку. URL. https://pon.org.ua/international/9064-pogliad-na-osvitu-2021-shchorichna-dopovid-organizacii-ekonomichnogo-spivrobitnyctva-ta-rozvytku.html

Ботнаренко І.А.
старший науковий співробітник
науково-дослідної лабораторії
з проблем протидії злочинності
навчально-наукового інституту
поліцейської діяльності,
кандидат юридичних наук
(Національна академія внутрішніх справ)
Шипп В.В.
курсант навчально-наукового інституту
поліцейської діяльності
(Національної академії внутрішніх справ)

ШТУЧНИЙ ІНТЕЛЕКТ У СУДОЧИНСТВІ ТА ДІЯЛЬНОСТІ ПОЛІЦІЇ: ІННОВАЦІЙНІ МОЖЛИВОСТІ ТА РИЗИКИ ДЛЯ ПРАВ ЛЮДИНИ

Штучний інтелект (далі – ШІ) сьогодні розглядається як одна з ключових технологій, що здатні радикально трансформувати публічне управління, судочинство та правоохоронну діяльність. Перспективи автоматизації відповідних процесів включають підвищення ефективності ухвалення рішень, оптимізацію ресурсів, оперативність аналізу даних та створення передових інструментів прогнозування ризиків і загроз. Разом із тим широке впровадження ШІ супроводжується серйозними етичними викликами, зокрема можливостями дискримінації, порушенням приватності, непрозорістю алгоритмічних рішень і ризиком зловживань у високочутливих сферах суспільного життя.

Європейський Союз, який розробив один із найамбіційніших у світі підходів до регулювання ШІ через так званий AI Act, зосереджує увагу саме на поєднанні інновацій і захисту основоположних прав людини [1]. В рамках цього регламенту вже заборонено найризикованіші застосування штучного інтелекту, як-то соціальний скоринг, непрозорі системи прогнозної поліції та автоматичне розпізнавання обличь без чітких гарантій прав та свобод, а для систем з високим ризиком накладаються посилені вимоги щодо прозорості, безпеки та контролю, вводяться суворіші

стандарти [2]. Таким чином, перспективи автоматизації у публічному секторі розглядаються ЄС як потенційно корисні за умови суворого дотримання етичних та правових стандартів, що мають бути імплементовані як на рівні розробників, так і на рівні органів влади.

ШІ дедалі активніше інтегрується в діяльність правоохоронних органів Європейського Союзу, зокрема в системи, що підтримують аналіз даних, розпізнавання обличь, прогнозну поліцію та автоматизоване виявлення загроз. За даними правових досліджень, застосування ШІ у кримінальному процесі ЄС включає використання різноманітних технологій для оптимізації розслідувань, підвищення оперативності контролю за злочинністю та аналізу великих обсягів доказів, що створює нові можливості для боротьби зі складними злочинами [3].

Водночас широке застосування таких технологій викликає серйозні етичні й правові питання, зокрема щодо прозорості алгоритмів, гарантій непорушення фундаментальних прав людини, контролю за безпекою даних і недопущення дискримінації у процесі застосування автоматизованих рішень правоохоронцями. Саме тому Європейський Союз активно працює над розробленням нормативних актів та регуляцій, які б забезпечили баланс між ефективністю боротьби із злочинністю та дотриманням етичних стандартів при використанні ШІ поліцією, судовими та іншими органами кримінальної юстиції.

Використання штучного інтелекту в правоохоронній діяльності супроводжується низкою суттєвих етичних ризиків, серед яких особливу увагу привертають алгоритмічна упередженість, автоматизований профайлінг та потенційна дискримінація окремих соціальних груп. Системи прогнозування злочинності, розпізнавання обличь та аналізу поведінкових моделей можуть відтворювати або навіть посилювати вже наявні соціальні стереотипи, якщо алгоритми навчаються на статистичних даних, що містять історичні викривлення. У такому випадку виникає ризик непропорційного контролю щодо окремих категорій населення, що суперечить принципам рівності та недискримінації.

Європейський Союз у 2024 році ухвалив Регламент про штучний інтелект (AI Act), який визначає використання систем

біометричної ідентифікації в режимі реального часу правоохоронними органами як високоризикове та передбачає суворі обмеження щодо їх застосування, зокрема обов'язковість правових підстав, пропорційності та судового контролю [1]. Такий підхід демонструє прагнення забезпечити баланс між потребами публічної безпеки та захистом фундаментальних прав людини, закріплених у праві Європейського Союзу.

Отже, перспективи впровадження штучного інтелекту в діяльність поліції безпосередньо пов'язані з необхідністю формування чітких процедур аудиту алгоритмів, запровадження механізмів прозорості прийняття рішень та гарантування права особи на оскарження автоматизованих рішень. Без належних правових і етичних запобіжників автоматизація правоохоронної діяльності може призвести до системних порушень прав людини та підриву довіри до державних інституцій.

В Україні інтеграція технологій ШІ у правозастосуванні, зокрема в судочинстві та правоохоронній діяльності, розглядається як перспективний напрям модернізації правової системи, що має потенціал суттєво підвищити її ефективність. Використання ШІ під час аналізу нормативних актів, автоматизації рутинних процесів, прогнозування результатів розгляду справ та підтримки процедур ухвалення рішень може знизити навантаження на суддів і правоохоронців, пришвидшити доступ до правосуддя та зменшити рівень суб'єктивних помилок [4].

Водночас українські дослідники звертають увагу на важливість чітких правових і етичних обмежень при впровадженні ШІ у правозастосовну практику. Це включає забезпечення прозорості алгоритмів, гарантування контролю людини над критичними рішеннями, захисту персональних даних, недопущення алгоритмічної дискримінації та створення механізмів відповідальності за помилки автоматизованих систем. Без врахування цих аспектів використання ШІ може призвести до порушення принципів справедливості й рівності перед законом, що підриває довіру до інститутів правосуддя та правоохоронних органів. Таким чином, українська перспектива застосування ШІ в правозастосуванні вимагає поєднання інноваційних можливостей із суворими етичними й правовими запобіжниками, що гарантують дотримання фундаментальних прав людини.

Список використаних джерел:

1. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*. 2024. L 1689. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (дата звернення: 25.02.2026).

2. Europe sets benchmark for rest of the world with landmark AI laws/ Reuters. 21.05.2024. URL: https://www.reuters.com/world/europe/eu-countries-back-landmark-artificial-intelligence-rules-2024-05-21/ (дата звернення: 25.02.2026).

3. Chernychenko I. Artificial intelligence in criminal procedure: current legal regulations in the EU. *Visegrad Journal on Human Rights*. 2025. DOI: https://doi.org/10.61345/1339-7915.2025.3.1 (дата звернення: 25.02.2026).

4. Gutsalyuk M., Klymenko-Panchenko O. Implementation of artificial intelligence in judicial activities: international and Ukrainian experience. *Air and Space Law Journal*. 2025. Vol. 2. Pp. 167–175. URL: https://doi.org/10.18372/2307-9061.75.20230 (дата звернення: 25.02.2026).

Братель С.Г.
завідувач кафедри поліцейської діяльності,
кандидат юридичних наук, професор
(*Національна академія внутрішніх справ*)
Білик І.В.
курсант
навчально-наукового інституту
поліцейської діяльності
(Національна академія внутрішніх справ)

ШТУЧНИЙ ІНТЕЛЕКТ У ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ: ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ТА ГАРАНТІЇ ДОТРИМАННЯ ПРАВ ЛЮДИНИ

Сучасні тенденції розвитку інформаційно-комунікаційних технологій та цифровізація суспільних процесів зумовлюють трансформацію підходів до організації публічного управління та діяльності правоохоронних органів. Одним із ключових інноваційних інструментів, що активно впроваджується у різні сфери державного управління, є технології штучного інтелекту (далі – ШІ). У сучасних умовах забезпечення публічної безпеки та правопорядку використання таких технологій може стати важливим чинником підвищення ефективності діяльності правоохоронних органів, зокрема Національної поліції України (далі НПУ).

Штучний інтелект у широкому розумінні розглядається як сукупність алгоритмічних і програмних рішень, здатних виконувати завдання, що традиційно потребують інтелектуальної діяльності людини, зокрема аналізу інформації, прийняття рішень, розпізнавання образів, прогнозування та навчання на основі накопичених даних. У правоохоронній діяльності використання таких технологій відкриває нові можливості для оптимізації управлінських процесів, підвищення ефективності аналітичної роботи та удосконалення механізмів реагування на правопорушення.

Одним із перспективних напрямів застосування ШІ у діяльності НПУ є інформаційно-аналітичне забезпечення правоохоронної діяльності. Сучасні системи ШІ здатні здійснювати обробку великих масивів даних, що надходять із різних інформаційних джерел, зокрема баз даних правоохоронних органів, систем відеоспостереження, інформаційно-телекомунікаційних мереж тощо. Аналіз таких даних дозволяє виявляти закономірності у кримінальній діяльності, прогнозувати можливі правопорушення та формувати ефективні превентивні заходи [1].

Важливим напрямом використання ШІ є застосування технологій автоматизованого розпізнавання обличчя та номерних знаків транспортних засобів. Такі системи активно використовуються у багатьох країнах світу для підвищення ефективності розшуку осіб, причетних до вчинення правопорушень, а також для встановлення місцезнаходження викрадених транспортних засобів. У контексті діяльності НПУ використання подібних технологій може сприяти оперативному реагуванню на правопорушення та підвищенню рівня безпеки.

Окрім цього, технології штучного інтелекту можуть застосовуватися для вдосконалення систем відеоаналітики у громадських місцях, автоматизованого аналізу кримінальної статистики, а також підтримки прийняття управлінських рішень у сфері забезпечення правопорядку. Використання алгоритмів машинного навчання дозволяє здійснювати прогнозування криміногенної ситуації на певних територіях, що створює передумови для більш ефективного планування діяльності підрозділів поліції та раціонального розподілу ресурсів.

Разом із тим впровадження технологій штучного інтелекту у правоохоронну діяльність пов’язане з необхідністю забезпечення належних гарантій дотримання прав і свобод людини. У міжнародній правовій практиці неодноразово наголошується на тому, що використання алгоритмічних систем у діяльності органів публічної влади повинно відповідати принципам законності, пропорційності, підзвітності та прозорості [2].

Одним із ключових викликів у цій сфері є ризик виникнення алгоритмічної упередженості, що може призвести до дискримінаційних рішень або неправомірного обмеження прав

громадян. Алгоритми штучного інтелекту формуються на основі аналізу великих масивів даних, які можуть містити певні соціальні або статистичні перекоси. У зв'язку з цим важливим є забезпечення належного контролю за розробкою та використанням таких систем, а також проведення регулярного аудиту алгоритмів з метою запобігання їх можливій упередженості [3].

Не менш важливим аспектом є захист персональних даних під час використання технологій штучного інтелекту. Обробка значних обсягів інформації, що може містити персональні дані громадян, потребує суворого дотримання законодавства у сфері захисту інформації та приватності. У цьому контексті необхідним є забезпечення належного рівня інформаційної безпеки, запобігання несанкціонованому доступу до інформаційних систем та визначення чітких правил обробки персональних даних [4].

Значну роль у забезпеченні належного використання ШІ у діяльності правоохоронних органів відіграє формування відповідної нормативно-правової бази. Зокрема, необхідним є визначення правових підстав застосування алгоритмічних систем у діяльності поліції, встановлення процедур контролю за їх використанням, а також визначення відповідальності за можливі порушення прав людини, пов'язані з використанням таких технологій. У цьому контексті важливим є врахування міжнародних стандартів та рекомендацій щодо етичного використання штучного інтелекту. Зокрема, міжнародні організації наголошують на необхідності забезпечення так званого «людського контролю» над алгоритмічними рішеннями, тобто збереження за людиною остаточного права прийняття рішень, що можуть впливати на права та свободи громадян.

Крім того, ефективне впровадження технологій ШІ у діяльність НПУ потребує належної підготовки персоналу. Працівники поліції повинні володіти відповідними цифровими компетентностями, розуміти принципи функціонування алгоритмічних систем та усвідомлювати потенційні ризики їх використання. Розвиток професійних компетентностей у сфері цифрових технологій є важливою передумовою ефективної інтеграції інноваційних рішень у правоохоронну діяльність.

Отже, використання технологій ШІ у діяльності НПУ має значний потенціал для підвищення ефективності забезпечення

публічної безпеки та правопорядку. Водночас впровадження таких технологій повинно здійснюватися з урахуванням необхідності забезпечення належних гарантій дотримання прав і свобод людини, прозорості алгоритмічних рішень та ефективного контролю за їх використанням.

Подальший розвиток цього напряму потребує комплексного підходу, що включає удосконалення нормативно-правового регулювання, розвиток сучасної інформаційно-технологічної інфраструктури, підвищення рівня цифрових компетентностей працівників поліції та врахування міжнародного досвіду використання ШІ у правоохоронній діяльності.

Список використаних джерел

1. Про схвалення Концепції розвитку штучного інтелекту в Україні: розпорядження Кабінету Міністрів України від 02.12.2020. № 1556-р. Дата оновлення: 29.12.2021. URL: https://zakon.rada.gov.ua/go/1556-2020-%D1%80 (дата звернення: 05.03.2026).

2. Recommendation on the Ethics of Artificial Intelligence. 23.11.2021. UNESCO. Paris. URL: https://unesdoc.unesco.org/ark:/48223/pf0000381137 (дата звернення: 05.03.2026).

3. European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment: EUROPEAN COMMISSION FOR THE EFFICIENCY OF JUSTICE (CEPEJ). Strasbourg. 3 – 4 December. 2018. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.europarl.europa.eu/cmsdata/196205/COUNCIL%20OF%20EUROPE%20-%20European%20Ethical%20Charter%20on%20the%20use%20of%20AI%20in%20judicial%20systems.pdf (дата звернення: 05.03.2026).

4. Про захист персональних даних: Закон України від 01.06.2010. № 2297-VI. Дата оновлення: 14.06.2025. URL: https://zakon.rada.gov.ua/go/2297-17 (дата звернення: 05.03.2026).

Бурдоносова М.А.
доцент кафедри теорії та публічного права,
кандидат юридичних наук, доцент
(Національний транспортний університ)

ПРАВОВА НАУКА В ЕПОХУ ШТУЧНОГО ІНТЕЛЕКТУ: МІЖ ІННОВАЦІЯМИ ТА ГАРАНТІЯМИ ПРАВ ЛЮДИНИ

Стрімкий розвиток штучного інтелекту змінює не лише технологічний ландшафт, а й саму природу правового регулювання. Алгоритмічні системи дедалі активніше впливають на процеси прийняття рішень у сфері правосуддя, державного управління, безпеки та освіти. У цьому контексті питання балансу між технологічною ефективністю та гарантіями прав людини набуває принципового значення.

Штучний інтелект формує нову конфігурацію владних відносин - так звану алгоритмічну владу, яка діє через аналіз даних, прогнозування поведінки та автоматизоване прийняття рішень. Водночас фундаментальні права людини, зокрема право на повагу до приватного життя, гарантоване Європейська конвенція з прав людини [1], залишаються базовими орієнтирами правового порядку. Використання біометричних технологій, систем розпізнавання облич і масивів персональних даних створює ризики надмірного втручання у приватну сферу особи.

У власних дослідженнях авторка звертала увагу на те, що впровадження ШІ у правову сферу має подвійний характер: з одного боку, воно відкриває значні перспективи для оптимізації юридичної діяльності та підвищення якості правової освіти, а з іншого - породжує нові виклики, пов’язані з відповідальністю, етичними стандартами та трансформацією професійної ролі юриста [4]. Зокрема, у роботі, присвяченій розвитку юридичної науки під впливом ШІ, наголошується на необхідності формування нової моделі юридичної освіти, що поєднує цифрову компетентність із глибоким розумінням прав людини та принципів верховенства права [4].

Окрему увагу в наукових публікаціях приділено ризикам і небезпекам використання штучного інтелекту, особливо в умовах воєнного стану та підвищеної інформаційної вразливості суспільства [5]. Серед ключових загроз визначено можливість маніпулювання даними, кіберризики, втрату контролю над автоматизованими системами та посилення інформаційних асиметрій. У цьому аспекті особливої ваги набуває питання правового регулювання та запровадження ефективних механізмів контролю за використанням високоризикових технологій.

Алгоритмічна дискримінація залишається одним із найбільш дискусійних питань. Оскільки алгоритми навчаються на історичних даних, вони можуть відтворювати соціальні упередження та нерівності. Це ставить під загрозу принцип рівності та недискримінації як фундамент сучасного правопорядку. Проблема ускладнюється тим, що алгоритмічні рішення часто є непрозорими для кінцевого користувача, що обмежує можливості ефективного захисту прав.

У сфері правосуддя використання автоматизованих систем має здійснюватися з дотриманням гарантій справедливого суду та належної правової процедури. Принцип human-in-the-loop повинен забезпечувати збереження вирішальної ролі людини у прийнятті рішень, що впливають на права та свободи особи. Штучний інтелект може виконувати аналітичну функцію, проте не може підміняти собою суддівську дискрецію чи моральну відповідальність.

Міжнародний досвід демонструє прагнення до формування людиноцентричної моделі регулювання. Так, у Європейському Союзі прийнято Artificial Intelligence Act [2], що встановлює класифікацію систем за рівнем ризику. Етичні орієнтири закріплені в рекомендаціях UNESCO [3], а також у нормативних ініціативах Council of Europe, спрямованих на захист прав людини в цифрову епоху.

Для України важливо поєднати процеси цифровізації з дотриманням європейських стандартів прав людини. Формування національної стратегії регулювання ШІ повинно спиратися на принципи пропорційності, прозорості, підзвітності та поваги до людської гідності. Необхідним є також розвиток міждисциплінарних досліджень, які дозволять комплексно

оцінювати соціальні та правові наслідки впровадження інтелектуальних систем.

Отже, баланс між технологіями та правом є не компромісом, а умовою сталого розвитку. Штучний інтелект має функціонувати в межах чітко визначених правових рамок, а його впровадження повинно супроводжуватися системною оцінкою впливу на права людини. Лише за таких умов цифрова трансформація сприятиме зміцненню, а не послабленню демократичних інститутів.

Список використаних джерел:

1. Європейська конвенція з прав людини. Convention for the Protection of Human Rights and Fundamental Freedoms : Конвенція Ради Європи від 04.11.1950 р. Rome, 1950. URL: https://www.echr.coe.int/documents/convention_eng.pdf (дата звернення: 10.02.2026).

2. Artificial Intelligence Act. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union. 2024. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (дата звернення: 12.02.2026).

3. UNESCO. Recommendation on the Ethics of Artificial Intelligence. Paris : UNESCO, 2021. URL: https://unesdoc.unesco.org/ark:/48223/pf0000380455 (дата звернення: 11.02.2026).

4. Burdonosova M. A. Artificial Intelligence in the Legal Sphere: Challenges and Prospects for Legal Education / *The Impact of Artificial Intelligence on the Development of Legal Science* (August 25-29, 2025, Riga, the Republic of Latvia): International scientific conference. Riga: Baltija Publishing, 2025. Pp. 9-13. DOI: https://doi.org/10.30525/978-9934-26-598-3-2

5. Бурдоносова М. А. Виклики та небезпеки використання штучного інтелекту // Інформаційна грамотність в умовах воєнного стану: обробка, захист та презентація даних : матеріали всеукраїнського науково-педагогічного підвищення кваліфікації, 2 грудня - 12 січня 2025 року. Львів-Торунь : Liha-Pres, 2025. С. 27-31.

Ваньчак М.В.
аспірантка кафедри конституційного права
(*Національний університет*
«*Одеська юридична академія*»)

ДОКТРИНА ПРАВОВОЇ ВИЗНАЧЕНОСТІ ПРОТИ ТЕХНОЛОГІЧНОГО ДЕТЕРМІНІЗМУ: КОНСТИТУЦІЙНІ МЕЖІ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СУДОЧИНСТВІ

У конституційному дискурсі фундаментальні засади держави виступають не просто декларативними положеннями, а базовими нормами, що визначають вектор розвитку всієї правової системи. Особливе значення мають конституційні принципи судочинства, вичерпний перелік яких закріплено у статті 129 Конституції України. Зокрема, мова йде про такі принципи, як: рівність усіх учасників судового процесу перед законом і судом, змагальність сторін та свобода в наданні ними суду своїх доказів, гласність судового процесу, а також мотивованість і обов'язковість судового рішення тощо [1].

Сьогодні цифровізація правосуддя та використання штучного інтелекту ставлять під загрозу класичні конституційні принципи.

«Одним з основоположних аспектів верховенства права є принцип правової визначеності, який передбачає дотримання принципу res judicata[1]»[2]. У контексті інтеграції штучного інтелекту, юридична визначеність передбачає, що учасник процесу може передбачити наслідки своїх дій та очікувати стабільної судової практики. Проте використання алгоритмів, схильних до «галюцинацій» (винайдення неіснуючих норм або прецедентів), прямо загрожує передбачуваності правозастосування.

[1] Res judicata – вирішена справа (res judicata pro veritate habetur! – судове рішення слід визначати за істину) означає остаточність рішення суду, яке набрало чинності і не може бути переглянуте. Принцип res judicata визнано на міжнародному рівні та зафіксовано, в тому числі, у п.1 ст.44 Конвенції про захист прав людини і основоположних свобод. Принцип остаточності рішення є складовою частиною верховенства права.

Відповідно до Постанови Касаційного цивільного суду у складі Верховного Суду від 26.10.2022 у справі № 463/3226/16-ц «рішення суду як найважливіший акт правосуддя покликане забезпечити захист гарантованих Конституцією України прав і свобод людини та здійснення проголошеного Основним Законом України принципу верховенства права»[3]. Обов'язок суду забезпечити «повне і всебічне з'ясування обставин» унеможливлює використання інструментів штучного інтелекту (як-от Perplexity), які лише узагальнюють публічну інформацію, замість ретельного дослідження доказів у засіданні. Законність вимагає інтелектуального контролю людини, а не автоматичного схвалення машинного висновку.

Наразі в Україні немає інструкції чи то закону, який би регулював використання штучного інтелекту у судочинстві, окрім статті 16 Кодексу суддівської етики, де зазначено, що суддя може використовувати штучний інтелект при таких умовах: - не відобразиться на незалежності та неупередженості судді; - не буде задіяно у оцінці доказів і в процесі винесення рішень; - не буде порушувати діюче законодавство [4].

У судовій практиці уже зафіксовані випадки, коли при підготовці рішення суддя або працівники апарату суду використовують генеративні моделі штучного інтелекту.

Розглядаючи вітчизняну практику, варто звернути увагу на постанову Новозаводського районного суду міста Чернігова від 17.10.2025 у справі №751/8289/25, у третьому абзаці мотивувальної частини якої міститься фраза: «Ось перевірений і відредагований варіант вашого тексту з виправленням граматичних, стилістичних і пунктуаційних помилок» [5]. Цей факт свідчить про механічне копіювання результатів роботи сервісу ChatGPT без належної редакційної перевірки. У відповідь на журналістський запит щодо використання технологій штучного інтелекту , суддя обмежився посиланням на статтю 16 Кодексу суддівської етики, констатувавши відсутність нормативно-правових актів, які б чітко регламентували межі допустимого застосування штучного інтелекту під час підготовки судових рішень.

Для порівняння, у Великій Британії суддя вперше офіційно підтвердив використання чат-бота Copilot від Microsoft для аналізу

матеріалів у податковому трибуналі. Технологія застосовувалася виключно як допоміжний інструмент для структурування аргументів. При цьому суддя наголосив на особистій професійній відповідальності, зазначивши: «Я приймаю рішення і несу відповідальність за цей матеріал» [6].

Водночас у США зафіксовано випадки помилкового оприлюднення проєктів рішень, підготовлених помічниками суддів за допомогою ChatGPT та Perplexity. Через виявлені «галюцинації» системи та грубі юридичні помилки голова юридичного комітету Сенату США ініціював офіційне розслідування. Наслідком цих інцидентів стало впровадження письмової політики використання штучного інтелекту в суді Нью-Джерсі, а в Міссісіпі суддя був змушений анулювати постанову, визнавши її результатом неналежного «людського нагляду».

Резюмуючи міжнародний досвід, представники Сенату підкреслили, що кожен суддя та судова влада як інституція зобов'язані гарантувати, що використання генеративного штучного інтелекту не порушує процесуальних прав сторін і не створює перешкод для справедливого правосуддя [7]. Така позиція повністю корелюється з українською конституційною доктриною. Згідно з практикою Касаційного цивільного суду у складі Верховного Суду та принципами, закладеними у статті 129 Конституції України, судочинство є функцією, яку держава делегує конкретній особі – судді. Отже, запровадження штучного інтелекту не може розглядатися як автоматизація прийняття рішень; це лише інструментарій, де кінцевим гарантом законності залишається людина.

Ці випадки доводять, що делегування аналітичної роботи алгоритмам без належного людського контролю є прямою загрозою принципу законності, але і ігнорувати технологічний прогрес також не можна. Штучний інтелект не може замінити суддю, про те він може в деякій мірі бути інструментом у здійсненні судочинства. Тому головним завданням сучасної правової системи є розробка чітких етичних та процесуальних стандартів застосування ШІ, які б відповідали Конституції України.

Список використаних джерел:

1. Конституція України : Закон України від 28 черв. 1996 р. № 254к/96-ВР. URL: https://surl.lu/ambsru (дата звернення: 17.02.2026).

2. Зловживання учасниками процесу принципом остаточності судового рішення — res judicata, що є складовою частиною верховенства права. Верховний Суд : офіційний вебпортал. URL: https://surl.li/zznvpl (дата звернення: 17.02.2026).

3. Постанова Касаційного цивільного суду у складі Верховного Суду від 26 жовтня 2022 року у справі № 463/3226/16-ц. URL: https://surl.lt/mtkjfc (дата звернення: 17.02.2026).

4. Кодекс суддівської етики: затверджений V з'їздом суддів України 24 жовтня 2002 року URL: https://surl.li/oymwdl (дата звернення: 20.02.2026).

5. Постанова Новозаводського районного суду міста Чернігова від 17 жовтня 2025 року у справі № 751/8289/25. URL: https://surl.li/nwxplr (дата звернення: 20.02.2026).

6. Godfrey T. A.I. AM THE LAW Judge admits using AI in court judgment to make sense of complicated tax arguments 'in UK first'. The Sun. 2025. Sept. 21. URL: https://surl.lu/ttnbqr (дата звернення: 20.02.2026).

7. Двоє федеральних суддів США зізналися, що під час підготовки судових рішень використовувався ШІ. Судово-юридична газета. 24 жовт. 2024. URL: https://surl.li/qipquv (дата звернення: 17.02.2026).

Вишневська І.А.
доцент кафедри
кримінально-правових дисциплін
навчально-наукового інституту
права та правоохоронної діяльності,
доктор філософії
*(Львівський державний університет
внутрішніх справ)*

ЦИФРОВІЗАЦІЯ ПРОЦЕСУ КРИМІНАЛЬНО-ПРАВОВОЇ КВАЛІФІКАЦІЇ У ПРОЄКТІ КК УКРАЇНИ

1. Протягом останніх десятиліть серед науковців та практиків неодноразово піддаються дискусії питання правил здійснення кваліфікації та алгоритму кваліфікації, в той же час потенційне прийняття проєкту КК суттєво змінює підходи до не лише до алгоритму, а й до кінцевої формули кваліфікації, що потребує не лише проведення численних тренінгів для його правозастосувачів, а й розробки нового технологічного рішення, яке здатне оптимізувати процес.

2. У практичній діяльності слідчого чи прокурора, який одночасно здійснює процесуальне керівництво, проблема полягає не у відсутності знань щодо правил кваліфікації, а у дефіциті часу для проходження повного інтелектуального маршруту кримінально-правової оцінки кожного діяння. Так, середні показники навантаження у правоохоронних органах свідчать про те, що на одного слідчого органів Національної поліції припадає близько 300 кримінальних проваджень в обласних центрах [1], а на одного прокурора окружної прокуратури — 250–300 проваджень (наприклад, у 2024 році в Полтавській окружній прокуратурі таке навантаження становило 260 проваджень на одного прокурора [2]). За таких умов здійснення повної та всебічної кримінально-правової кваліфікації у кожному окремому випадку стає об’єктивно ускладненим. Основний ризик у цій ситуації полягає не у неправильному застосуванні норми кримінального закону, а у пропуску або неперевірці окремих юридично значущих елементів складу кримінального правопорушення.

3. Кожне кримінальне правопорушення характеризується значною кількістю фактичних обставин, лише частина з яких має кримінально-правове значення. В умовах обмеженого часу правозастосувач змушений приймати рішення, спираючись на наявний обсяг інформації, що підвищує ймовірність неповної перевірки окремих ознак складу. У зв'язку з цим актуалізується питання використання цифрових інструментів, які могли б виконувати функцію допоміжного механізму контролю повноти кримінально-правової кваліфікації.

Окремого значення зазначене питання набуває у зв'язку з підготовкою та можливим запровадженням нового Кримінального кодексу України [3]. Хоча у Прикінцевих положеннях проєкту КК передбачено, що він набирає чинності з 1 січня року, який настане через три повних календарних роки з дня його офіційного опублікування, але не раніше року припинення або скасування воєнного стану, не можна виключати ймовірності скорочення цього строку. Історія прийняття чинного КК України 2001 року свідчить про можливість дострокового набрання чинності кримінальним законом унаслідок політичних рішень.

У разі, якщо новий КК набере чинності раніше, ніж це передбачено задумом його авторів, традиційні форми підготовки правозастосувачів можуть виявитися недостатніми. Натомість цифровий інструмент, який інтегрує логіку кримінального закону безпосередньо у робочий процес, здатний забезпечити швидшу адаптацію практиків до нової нормативної моделі.

4. Метою діджиталізації кримінального кодексу у цьому контексті є створення допоміжного інструменту для правозастосувача, який дозволяє окреслити коло норм, потенційно релевантних для кваліфікації конкретного діяння, виявити прогалини у процесі кваліфікації та доказування, а також раціональніше розподіляти власні часові ресурси. При цьому цифровий інструмент не виконує функцію автоматичного визначення статті кримінального закону, а слугує своєрідним контрольним списком юридичного мислення.

Станом на сьогодні розроблена програма має вигляд демонстраційного прототипу та побудована у форматі анкети. Вона охоплює основні елементи складу кримінального правопорушення, зокрема дані про суб'єкта, об'єкт, об'єктивну та

суб'єктивну сторони, потерпілого, співучасть, стадію вчинення кримінального правопорушення, а також обставини, що виключають кримінальну відповідальність або впливають на ступінь тяжкості злочину.

Програма працює з типовими фабулами та відтворює логіку кримінально-правової кваліфікації у цифровому форматі. Користувач послідовно рухається від загального опису події до конкретних статей Особливої частини КК. При цьому система не дозволяє перейти до наступного етапу аналізу без оцінки всіх обов'язкових ознак складу кримінального правопорушення. Лише після підтвердження складу програма переходить до аналізу кваліфікуючих ознак, стадій та співучасті.

У результаті користувач отримує сформовану формулу кваліфікації, визначення ступеня тяжкості кримінального правопорушення та можливі варіанти санкцій. Водночас програма не замінює правозастосувача і не ухвалює рішення замість нього, а лише забезпечує структуровану перевірку юридично значущих елементів.

5. Діджиталізація у сфері кримінального права не спрямована на заміну слідчого, прокурора чи судді і не покладає на цифрові інструменти функцію ухвалення рішень. Її призначення полягає у полегшенні роботи правозастосувача в умовах надмірного навантаження, мінімізації помилок, пов'язаних із пропуском окремих юридично значущих елементів, а також у можливості виявлення таких помилок на ранньому етапі.

У зв'язку із цим можливо стверджувати, що діджиталізація у процесі кримінально-правової кваліфікації є додатковим інструментом підтримки правозастосувача, а не обов'язковою складовою застосування нового Кримінального кодексу. Водночас у ситуації постійного дефіциту часу та значного навантаження такі інструменти можуть сприяти збереженню якості кримінально-правової кваліфікації та забезпеченню її повноти.

Список використаних джерел:

1. Нацполіція: у мегаполісах у середньому один слідчий поліції розслідує 300 кримінальних проваджень. 24 трав. 2019. URL: https://www.kmu.gov.ua/news/nacpoliciya-u-megapolisah-u-

serednomu-odin-slidchij-policiyi-rozsliduye-300-kriminalnih-provadzhen

2. Мурдза Я. На одного прокурора Полтавщини припадає 260 справ. Zmist. 19 серп. 2024. URL: https://zmist.pl.ua/news/odyn-prokuror-poltavshhyny-v-serednomu-rozsliduye-260-sprav-yak-zrostalo-navantazhennya

3. Проєкт Кримінального кодексу України: станом на 22 лютого 2026 р. URL: https://newcriminalcode.org.ua/criminal-code

Глинська Н.В.
завідувачка відділу дослідження проблем
кримінального процесу та судоустрою
науково-дослідного інституту вивчення проблем
злочинності імені академіка В.В. Сташиса
доктор юридичних наук, професор
(Національна академія правових наук України)

АСИМЕТРІЯ У ЦИФРОВОМУ ДОКАЗУВАННІ: РИЗИКИ ДЛЯ СПРАВЕДЛИВОГО СУДОВОГО РОЗГЛЯДУ

З огляду технічну складність та специфіку оцінки достовірності цифрових доказів у суді об’єктивною є потреба залучення особи зі спеціальними технічними знаннями та навичками. Більш оперативною та компромісною формою «спеціальної допомоги» у кримінальній процедурі є залучення спеціаліста (ст. 71, 360 КПК). Ба більше, як ми вже раніше наголошували, з урахуванням, з одного боку, стрімкого зростання спектру цифрової інформації, що потрапляє в царину кримінального процесуального доказування, та відповідно рівня складності питань її достовірності, та з іншого боку – явно недостатнього рівня сучасної цифрової компетентності правників, питання щодо участі спеціаліста під час дослідження цифрового доказу в суді стає не рекомендацією, *а правилом* [1]. Як влучно зазначає І. Каланча, принципово важливим є участь спеціаліста під час дослідження цифрового доказу в суді, на ключовому етапі, від якості якого залежить «технічна» обґрунтованість використання відповідної інформації для встановлення обставин справи. Роль для суду спеціаліста (у сфері ІТ) під час судового розгляду кримінального провадження важко переоцінити, адже це дозволяє унеможливити формалізований підхід до оцінки цифрових об'єктів – натомість сприяє вивченню глибших контекстуальних обставин щодо достовірності та автентичності та цілісності даних. Це особливо важливо в умовах, коли сторони надають різні тлумачення одного й того ж цифрового об'єкта – наприклад, щодо правдивості вмісту чатів або відповідності скриншот первинному

джерелу. У зв'язку з високим рівнем технічної складності доказів електронної форми залучення спеціаліста не повинно сприйматись як виняток. Це – необхідний компонент, що дозволяє суду ухвалити об'єктивне, зважене рішення на основі комплексного розуміння як юридичних, так і технічних обставин справи [2, с. 263].

Системне тлумачення статтей 71, 321 та 360 КПК з урахуванням принципів рівності та змагальності свідчить, що спеціаліст може бути залучений як за клопотанням однієї зі сторін, так і за ініціативою суду; питання щодо компетентності та неупередженості залученого до дослідження цифрового доказу фахівця в суді має бути узгоджено сторонами. Як показує аналіз практики, дослідження судом питання щодо правдивості цифрового доказу сторони обвинувачення, часто ініціюється саме стороною захисту, яка нерідко надає суду інформацію, що підтверджує наявність розумних сумнівів щодо достовірності, справжності, автентичності, цілісності цифрової інформації, на яку спирається протилежна сторона. В цьому контексті непоодинокими є випадки, коли суд надає перевагу (пріоритет) залученню спеціалісту з боку сторони обвинувачення (зокрема, співробітників того ж органу, що здійснює досудове розслідування у цьому кримінальному провадженні), що на оцінку сторони захисту є порушенням принципу рівності та створює достатні підстави для сумніву щодо неупередженості залученого фахівця, а в окремих кейсах й самого суду.

Спробуємо в міжнародно-правових та національних координатах принципів рівності та змагальності сформулювати основні вектори оцінки такої «технічної асиметрії» між повноваженнями сторони обвинувачення та сторони захисту у сфері цифрового доказування з точки зору потенційного впливу на справедливість судового розгляду .

Нагадаємо, що принцип цифрової рівності, який ми раніше виокремлювали у контексті сучасного концепту ЦКП [3, с. 63-64], не зводиться до абсолютної ідентичність прав сторін, адже законодавець наділяє учасників кримінального провадження рівними правами і рівними обов'язками (але не однаковими) щодо

участі у кримінальному процесі та відстоюванні своєї позиції [1]. Втім будь-яка асиметрія для сторони захисту має бути компенсована у спосіб наділення її ефективними інструментами.

Рівність сторін є одним із невід'ємних елементів поняття справедливого судового розгляду. Вона вимагає, аби кожна сторона бачила, що їй надано розумні можливості представити свій інтерес за умов, які не ставлять її у несприятливе становище, порівняно із супротивником (див. рішення ЄСПЛ у справах «Оджалан проти Туреччини» (Öcalan v. Turkey) [ВП], § 140; «Фуше проти Франції» (Foucher v. France), § 34; «Булут проти Австрії» (Bulut v. Austria); «Фаіг Маммадов проти Азербайджану» (Faig Mammadov v. Azerbaijan), § 19). Право на змагальне провадження означає, в принципі, можливість для сторін *знати і коментувати усі складові наданої доказової бази й усі зауваження, надані для того, щоб вплинути на рішення суду* («Брандштеттер проти Австрії» (Brandstetter v. Austria), § 67). Воно тісно пов'язане з принципом рівності сторін і, до речі, ЄСПЛ іноді вирішував про

[1] Конституційний Суд України наголошує, що рівність учасників кримінального провадження перед законом означає наділення їх рівними правами і рівними обов'язками щодо участі у кримінальному процесі та відстоюванні своєї позиції. При цьому поняття «рівні права», «рівні обов'язки» не можна ототожнювати з поняттями «однакові права», «однакові обов'язки». Права чи обов'язки можуть бути різними і залежать від статусу та ролі учасника кримінального провадження (прокурора, потерпілого, слідчого, обвинуваченого, захисника, цивільного позивача, цивільного відповідача тощо). Таким чином, рівність прав та обов'язків полягає в тому, що кожен із учасників кримінального провадження наділений правами і має обов'язками, визначеними законодавством для його процесуального становища (абзаци другий, третій підпункту 3.2 пункту 3 мотивувальної частини рішення Конституційного Суду України (Велика палата) від 17 березня 2020 року № 5-р/2020) [4]; процесуальні права та обов'язки учасників кримінального провадження *різняться*, що зумовлено різними процесуальними функціями, які мають бути реалізовані цими учасниками у перебігу кримінального провадження (абзаци другий, третій підпункту 3.2 пункту 3 мотивувальної частини рішення Конституційного Суду України (Велика палата) від 17 березня 2020 року № 5-р/2020) [4]

порушення статті 6 § 1 саме внаслідок сукупного розгляду цих двох понять.

Натомість відсутність у законодавстві певних кримінальних процесуальних правил може становити загрозу для рівності сторін, оскільки їхня мета – захистити обвинуваченого від будь-яких зловживань представників державної влади, і від недоліків або недостатньої чіткості таких правил найбільше ризикує постраждати саме сторона захисту («Коеме та інші проти Бельгії» (Coëme and Others v. Belgium), § 102)[5, с.37].

*Стандарт неупередженості спеціаліста як гарантія змагальності та рівності сторін***.** Зауважимо, що в практиці ЄСПЛ, неодноразово поставало питання залучення та участі експертів (спеціалістів). ЄСПЛ в своїх рішеннях неодноразово повторював, що пункт 1 статті 6 Конвенції гарантує право на справедливий розгляд справи *незалежним і неупередженим* судом і чітко не вимагає, щоб експерт, заслуханий цим самим судом, відповідав *таким же вимогам* (див. «Sara Lind Eggertsdóttir v. Iceland», no. 31930/04, § 47, 5 липня 2007 року, та «Letinčić v. Croatia», no. 7183/11, § 51, 3 травня 2016 року).

Однак висновок експерта, якого призначив компетентний суд для з'ясування питань, що виникають у справі, ймовірно, матиме суттєве значення для оцінки цим судом відповідних питань. У своїй практиці ЄСПЛ визнавав, що відсутність неупередженості призначеного судом експерта за певних обставин може призвести до порушення принципу рівності сторін, притаманного поняттю справедливого суду (див. «Bönisch v. Austria», 6 травня 1985 року, §§ 30–35, Series A no. 92, та «Brandstetter v. Austria», 28 серпня 1991 року, § 33, Series A no. 211). Зокрема, варто враховувати такі фактори, як *процесуальну позицію / статус експерта та його роль у відповідному провадженні* (див. «Sara Lind Eggertsdóttir v. Iceland» цит. вище, § 47, та «Letinčić v. Croatia», § 51). У той же час *сам факт, що відповідні експерти найняті однією із сторін, не є достатнім для того, щоб зробити провадження несправедливим*. ЄСПЛ пояснив, що, хоча цей факт може викликати побоювання щодо нейтральності експертів, таке побоювання, яке має певне значення, не є вирішальним. Проте *вирішальною є позиція, яку займають експерти протягом усього провадження, спосіб, у який вони*

виконують свої функції, і спосіб, у який судді оцінювали експертну думку. Під час визначення процесуальної позиції експертів та їх ролі у провадженні ЄСПЛ враховує той факт, що *думка, надана будь-яким призначеним судом експертом, може мати велике значення в оцінюванні судом питань в межах компетенції експерт*а («Шулєпова проти Росії» (Shulepova v. Russia), § 62, «Полетан та Азіровік проти колишньої Югославської Республіки Македонія» (Poletan and Azirovik v. the former Yugoslav Republic of Macedonia), § 94).

ЄСПЛ і в низці інших рішень нагадував, що позиція, яку займають експерти під час провадження, спосіб, у який вони здійснюють свої функції, і те, як судді оцінюють їхні висновки, є важливими факторами, які варто враховувати при оцінці того, *чи було дотримано принцип рівності сторін* (див. «Sara Lind Eggertsdóttir v. Iceland», § 47; «Letinčić v. Croatia», § 51). З огляду на це, ЄСПЛ встановив, що Конвенція не забороняє національним судам покладатися на експертні висновки, складені спеціалізованими органами, при вирішенні спорів, які вони розглядають, якщо цього вимагає характер спірних питань, що розглядаються. Однак це передбачає *дотримання вимоги нейтральності з боку призначеного експерта*, аби судовий розгляд був змагальним, і щоб заявник був прирівняний до свого опонента, зокрема держави, згідно з принципом рівності сторін (див. «Letinčić v. Croatia», згадане вище, § 61).

ЄСПЛ встановив, що якщо обвинувальний висновок засновується на висновку експерта, який був призначений під час досудового розслідування державним прокурором, призначення судом першої інстанції тієї ж особи експертом тягне за собою *ризик порушення принципу рівності сторін, який, проте, може бути компенсований конкретними процесуальними гарантіями* («Дж.М. та інші проти Австрії» (J.M. and Others v. Austria), § 121).

При цьому правила щодо допустимості доказів не повинні позбавляти сторону захисту можливості *ефективно оскаржити висновки експерта, зокрема, шляхом надання або отримання альтернативних висновків та звітів*. За певних обставин відмова у прийнятті альтернативної експертизи у якості доказів може розглядатися як порушення статті 6 § 1 («Стойменов проти колишньої Югославської Республіки Македонія» (Stoimenov v. the

former Yugoslav Republic of Macedonia), § 38; «Матиціна проти Росії» (Matytsina v. Russia), § 169), *оскільки може бути складно оскаржити висновок експерта без допомоги іншого експерта у відповідній сфері* («Ходорковський та Лєбєдєв проти Росії» (Khodorkovskiy and Lebedev v. Russia), § 187). [5, с. 39-40]

Тож, у разі наявності розумних побоювань щодо нейтральності спеціаліста, необхідним є з'ясувати *чи був компенсований цей ризик порушення принципу рівності сторін конкретними процесуальними гарантіями* та проаналізувати, *яку позицію займав спеціаліст протягом усього провадження, спосіб, у який він виконував свої функції, і спосіб, у який головуючий у судовому засіданні оцінював думку спеціаліста, а також чи була забезпечена стороні захисту можливість ефективно оскаржити висновки експерта, зокрема, шляхом надання або отримання альтернативних висновків* .

З урахуванням викладеного можна виділити такі *критерії оцінки з точки зору справедливості правової ситуації, у якій суд надав перевагу залученню спеціаліста з боку сторони обвинувачення.*

- *Спосіб, у який спеціаліст здійснював свої функції.* Акцентуємо увагу на те, що ставити запитання та отримувати на них відповіді є одним з основних механізмів реалізації стороною захисту свого права до доступ до матеріалів справи, зокрема цифрового доказу. При цьому законодавець не регламентував послідовність і зміст поставлення стороною захисту запитань, оскільки це напряму залежить від особливостей правової ситуації у конкретному кримінальному провадженні, а отже, цілком очевидно та логічно, що це віднесено на розсуд сторони захисту та по суті є складовою її тактики захисту. З огляду на викладене належний спосіб здійснення спеціалістом свої функцій під час дослідження цифрового доказу в суді передбачає його процесуальну, що у кореляції із гіпотетичною ситуацією процесуальної асиметрії, може мати вияв, зокрема у повноті відповідей на поставлені питання захисту, їх конкретність, нерозмитість тощо). Навпаки *негативними індикаторами* належної поведінки спеціаліста під час судового розгляду може бути уникнення ним відповідей на поставлені питання, надавання загальних, неконкретних відповіді на запитання сторони захисту.

➢ *Створення судом умови для реалізації стороною захисту своїх прав на дослідження цифрового доказу в суді.* Відмітимо, що основоположним критерієм, що визначає допустиму межу ініціативної (дискреційної) діяльності суду у змагальному процесі, є *кореляція відповідних дій суду із метою створення необхідних умов для реалізації сторонами їхніх процесуальних прав та виконання процесуальних обов'язків, нейтралізації нерівності у можливостях формування доказової бази сторони обвинувачення і сторони захисту (favor defensionis).* У контексті ж ролі головуючого у судоговорінні під час дослідження доказів, то системний аналіз норм статей § 3 Глави 28 КПК України, що є дотичними й для процедури судово-контрольних проваджень, дозволяє стверджувати про кореляцію меж нормативного уповноваження головуючого на певну ініціативність й активність із *роллю суду у змагальному процесі* — створювати необхідні умови для реалізації сторонами їхніх процесуальних прав та виконання процесуальних обов'язків, а також *нормативним обов'язком ухвалити законне, обґрунтоване та вмотивоване рішення (ст. 370 КПК України).* Так, зокрема, відповідно до ч. 2 ст. 360 КПК України головуючий у судовому засіданні наділений правом ставити спеціалістові запитання в будь-який час дослідження доказів.

З огляду на окреслені перед судом завдання метою активної участі суду під час такого етапу судоговоріння, як постановка питань спеціалісту, має бути, зокрема, сприяння стороні захисту у реалізації своїх прав, втім аж ніяк не перешкоджання в цьому. Навпаки, зміна, відхилення питань захисника, судом не лише перешкоджає реалізації стороною захисту можливості поставити питання спеціалісту, а й фактично унеможливлює ознайомлення стороною захисту з наведеним джерелом доказової інформації, отримання та з'ясуванні дійсного змісту фактичних даних, що містяться у даному джерелі, оцінку джерела на предмет допустимості, перевірку фактичних даних, їх оцінку захисником на предмет належності, достовірності та (у сукупності з іншими доказами) достатності. Наведене свідчить про фактичну відмову стороні захисту у доступі до матеріалів кримінального провадження під час досудового розслідування, що загалом

підриває справедливість у конкретному кримінальному провадженні.

➢ *Чи демонстрував суд нейтральність під час дослідження цифрового доказу з участі спеціаліста?*

Цей вектор тісно пов'язаний з попереднім та за негативної відповіді створює розумні сумніви щодо неупередженості суду як невід'ємної компоненти справедливого судового розгляду. Виходячи з нормативних меж судової активності під час дослідження доказів під час судового розгляду може й має право ставити свої питання спеціалісту питання (з метою виконання свого обов'язку щодо ухвалення законного та обґрунтованого рішення), втім *не вправі доповнювати питання, поставлені спеціалісту сторонами, змінювати їх або іншим чином впливати на їх формування чи взагалі перешкоджати стороні захисту у постановці питань спеціалісту* в контексті обраної тактики захисту*, тим самим змінюючи межі та предмет судового розгляду*.

Цей твердження має безпосереднє значення для не лише для забезпечення рівності сторін щодо участі дослідженні цифрового доказу в суді, а для оцінки відповідності поведінки суду стандарту безсторонності суду в рамках застосованого ЄСПЛ об'єктивного підходу за критерієм особистого характеру. На підтвердження тези про те, що суд у справі не був безстороннім, може свідчити сукупність певних індикаторів, як то : залучення спеціаліста, який був учасником кримінального провадження на боці сторони обвинувачення, що не було жодним чином компенсовано конкретними процесуальними гарантіями; зняття та зміна питань сторони захисту, що істотно порушило право на захист адже позбавило останню можливості.

Список використаних джерел:

1. Н. Глинська, Д. Клепка. Основні аспекти стратегії унормування інституту цифрових доказів у кримінальному процесуальному законодавстві. Питання боротьби зі злочинністю, 2023. URL: https://www.researchgate.net/publication/390302140_Basic_aspects_of_the_normalization_strategy_institute_of_digital_evidence_in_Criminal_Procedure_Law.

2. Каланча І. Докази електронної форми у кримінальному процесі України: теорія та практика : дис. … д-ра юрид. наук : 12.00.09 / І. Каланча. – Київ, 2025. – 617 с.

3. Концептуальні основи цифровізації кримінального провадження України : монографія / за заг. ред. Н. В. Глинської; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. – Харків : Право, 2024. – 452 с.

4. Рішення Конституційного Суду України (Велика палата) від 17 березня 2020 року № 5-р/2020. URL: https://zakon.rada.gov.ua/laws/show/v005p710-20#Text;

5. Посібник зі статті 6 Європейської конвенції з прав людини Право на справедливий суд (кримінальний аспект). Оновлено 31 серпня 2024 року. URL: https://ks.echr.coe.int/documents/d/echr-ks/guide_art_6_criminal_ukr.

Гловюк І.В.
професорка кафедри
кримінального процесу та криміналістики
докторка юридичних наук, професорка,
заслужена юристка України
(Одеський державний університет внутрішніх справ)

ЧИ Є ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ СУДОМ ПІДСТАВОЮ ДЛЯ СКАСУВАННЯ СУДОВОГО РІШЕННЯ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ?

Натепер в Україні немає правил (політик тощо) використання ШІ при здійсненні правосуддя, хоча декі норми, які торкаються цих питань, існують. Йдеться про ст. 16 Кодексу суддівської етики, яка регламентує: використання суддею технологій штучного інтелекту є допустимим, якщо це не впливає на незалежність та неупередженість судді, не стосується оцінки доказів і процесу ухвалення рішень та не порушує вимог законодавства.

Деякі положення щодо відповідального використання ШІ є у Рекомендаціях з відповідального використання штучного інтелекту для правників, зокрема, що із дотриманням цих умов (ст. 16 Кодексу суддівської етики) ШІ може використовуватись як асистент під час правничих досліджень, аналізу й упорядкування матеріалів, здійснення перекладів, аналізу та уніфікації судової практики, задля оформлення проєктів судових документів, для аналізу різного роду даних, розпізнавання типових підходів тощо. Звісно, фінальне рішення завжди залишатися за суддею, але використання ШІ підвищує ефективність роботи судді, а також зменшує ризик технічних помилок, хоча й вимагає уважної перевірки отриманих результатів роботи ШІ [1]. Юридичної сили ці рекомендації не мають, утім, важливо, що вимагається уважна перевірка результатів діяльності ШІ.

Слід звернути увагу, що Guidelines for the use of AI systems in courts and tribunals (Published in 2025 by the United Nations Educational, Scientific and Cultural Organization) прописують:

«Уникайте надмірної залежності від систем штучного інтелекту при прийнятті важливих рішень. Судді та магістрати не повинні повністю покладатися на системи штучного інтелекту при прийнятті рішень по суті справи або при вирішенні процедурних питань, які можуть вплинути на права людини; натомість, використовуйте результати роботи інструментів штучного інтелекту для доповнення юридичного аналізу, проведеного за допомогою інших методів та джерел інформації. Судове рішення – це не просто результат, а рішення, прийняте в ході процесу» [2]. Як видається, цим підкреслено специфіку меж використання ШІ судами у контексті правозастосування як допоміжного інструменту.

Схожий підхід викладено у 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), оскільки вказано про те, що використання інструментів ШІ може підтримувати повноваження суддів щодо прийняття рішень або незалежність судової влади, але не повинно замінювати їх: остаточне прийняття рішень має залишатися діяльністю, що здійснюється людьми (п. 61 преамбули) [3]. У цьому ж акті системи ШІ, призначені для використання судовими органами або від їхнього імені для надання допомоги судовим органам у дослідженні та тлумаченні фактів і законів, а також у застосуванні законів до конкретного набору фактів, або для використання аналогічним чином в альтернативному вирішенні спорів, визнані системами ШІ високого ризику.

У судовій практиці України вже мала місце ситуація, коли суд апеляційної інстанції скасував вирок, у мотивувальній частині згадавши про використання ШІ судом першої інстанції. Зокрема, суд зазначив: колегія суддів звертає увагу на зміст вироку, який обтяжений довільним трактуванням загальних понять, тверджень, наведенням теоретичних аспектів права, згенерованих штучним інтелектом "ChatGPT", що ставить під сумнів суддівський розсуд та судове тлумачення окремих питань, беручи до уваги суть пред`явленого обвинувачення. Також судом першої інстанції у

вироку наведено узагальнені поняття та теоретичні міркування щодо об`єктивної та суб`єктивної сторін інкримінованих ОСОБА_7 правопорушень, однак вони не відображають фактичні обставини кримінального провадження та не містять прив`язки до даного кримінального провадження. Вирок у такому вигляді без встановлення судом фактичних обставин кримінального провадження - в будь-якому разі не може бути законним [4]. У підсумку суд зробив висновок, що при ухваленні вироку судом першої інстанції допущено порушення вимог ст. ст. 91, 94 370, 374 КПК України, тобто такі істотні порушення вимог КПК України унеможливили прийняття законного та обґрунтованого рішення, а тому оскаржуваний вирок суду першої інстанції не можна визнати законним, обґрунтованим, вмотивованим [4].

Аналізуючи і вирок [5], і вищепроцитовану ухвалу, спробуємо викласти власне бачення проблеми використанні ШІ у тексті вироку суду.

Наявність підстав для скасування вироку: куди «віднести» використання ШІ? КПК України регламентує, що підставою для скасування або зміни судового рішення при розгляді справи в суді апеляційної інстанції є: 1) неповнота судового розгляду; 2) невідповідність висновків суду, викладених у судовому рішенні, фактичним обставинам кримінального провадження; 3) істотне порушення вимог кримінального процесуального закону; 4) неправильне застосування закону України про кримінальну відповідальність.

В ухвалі суду апеляційної інстанції зазначено ключове щодо оцінки вироку: «Вирок у такому вигляді без встановлення судом фактичних обставин кримінального провадження - в будь-якому разі не може бути законним» [4]. Утім, неповнота судового розгляду та істотне порушення вимог кримінального процесуального закону – є відмінними за змістом підставами. І якщо «у вироку наведено узагальнені поняття та теоретичні міркування щодо об`єктивної та суб`єктивної сторін інкримінованих ОСОБА_7 правопорушень, однак вони не відображають фактичні обставини кримінального провадження та не містять прив`язки до даного кримінального провадження», то виникає питання, чому не констатовано таку підставу скасування вироку, як неповнота судового розгляду (до речі, в ухвалі вказано,

що «Судом першої інстанції достатніх, переконливих та пов`язаних між собою доказів на обґрунтування своїх висновків на наведено» [4] або невідповідність висновків суду, викладених у судовому рішенні, фактичним обставинам кримінального провадження (адже, судячи з ухвали, міркування вироку не відображали фактичні обставини кримінального провадження, тому висновки ніяк не можуть бути кваліфіковані як такі, що відповідають фактичним обставинам кримінального провадження).

Безумовна складність перегляду вироку у цій ситуації для апеляційного суду полягає у тому, що відсутні правила щодо меж використання ШІ при здійсненні правосуддя. Кодекс суддівської етики містить такі правила у ст. 16, але ці положення спрямовані на встановлення етичних стандартів, пов'язаних зі статусом судді (що вказано у преамбулі), а не процесуальну регламентацію / заборони використанні ШІ у кримінальних провадженнях. Висновок КРЄС № 26 (2023) «Рухаючись вперед: використання асистивних технологій у судочинстві» [6], на який суд послався, дає рекомендації, вказує на загальні принципи, що стосуються технології в судових системах, та одночасно визначає виклики, у тому числі щодо справедливого судового розгляду. Але і вони не надають відповіді на питання, яка має бути процесуальна реакція, як у вищеописаній ситуації.

Деталізація мотивування при критиці потенційного застосування ШІ. З аналізу тексту ухвали складно зрозуміти, як суд ідентифікував підстави скасування. Судячи з ухвали, саме використання ШІ стало істотним порушенням, хоча згадувалися і інші недоліки вироку. Що ж до істотності порушень, то вони не відносяться до того переліку, що передбачений ч. 2 ст. 412 КПК України. А отже, при встановленні під час апеляційного розгляду інших істотних порушень, крім передбачених у ч. 2 ст. 412 КПК, судам слід враховувати, чи такі порушення перешкодили або могли перешкодити ухваленню законного та обґрунтованого судового рішення суду першої інстанції. Порушення кримінального процесуального закону, які не вплинули та не могли вплинути на винесення законного та обґрунтованого судового рішення, не є підставами для скасування судового рішення (п. 19 Листа ВССУ Про деякі питання порядку здійснення

судового провадження з перегляду судових рішень у суді апеляційної інстанції відповідно до Кримінального процесуального кодексу України від 21.11.2012 № 10-1717/0/4-12). Отже, з урахуванням доводів ухвали, які стосуються різних підстав скасування вироку, для точного розуміння того, чому суд визнав використання ШІ у тому контексті, як це мало місце у вироку, істотним порушенням КПК України, дещо бракує більш розлогої аргументації. Формулювання «Вирок у такому вигляді без встановлення судом фактичних обставин кримінального провадження - в будь-якому разі не може бути законним. Використання технологій повинно, перш за все, поважати природу судового процесу (пункт 90 висновку КРЄС № 26 (2023) від 1 грудня 2023 року "Рухаючись вперед: використання асистивних технологій у судочинстві"). Штучний інтелект може бути корисним та допоміжним інструментом у сфері правосуддя, але не може замінити роль суддів (рішення Верховного Суду від 08 лютого 2024 року у справі 925/200/22)» [4] - є цілком логічними та доречними, однак недостатніми з урахуванням чутливості та новизни питання. Більше того, розлога аргументація була б дуже доречною, зважаючи на те, що це перша ухвала суду апеляційної інстанції у контексті використання ШІ у вироку.

Чи є використання ШІ для підготовки тексту вироку саме по собі істотним порушенням КПК України? Аналіз ст. 412 КПК України, як видається, не дає підстав для таких безкомпромісних тверджень. Оцінювати дотримання ст. 16 Кодексу суддівської етики суд апеляційної інстанції повноважень не має (вона, до речі, і не згадується). «Вирок у такому вигляді без встановлення судом фактичних обставин кримінального провадження - в будь-якому разі не може бути законним» [4] - важливе формулювання, яке, тим не менш, потребує пояснення, які саме частини вироку є незаконними, в чому полягають порушення КПК України, і як визначено їх істотність.

Отже, розуміючи складність теми та контраверсійність сприйняття використання ШІ у ситуації, коли це прямо не було визнано у вироку, дозволимо собі підвести підсумки розумів та викласти авторське бачення відповідей на поставлені в тезах питання. За чинної нормативної регламентації саме по собі використання ШІ для підготовки тексту вироку не є істотним

порушенням КПК України (за відсутності інших істотних порушень, що можуть полягати у недотриманні вимог КПК України щодо форми та змісту вироку). Утім, використання ШІ у разі галюцинацій або інших недоліків може свідчити про наявність іншої підстави або підстави скасування вироку за ст. 409 КПК України, зокрема, неповноти судового розгляду, невідповідності висновків суду, викладених у судовому рішенні, фактичним обставинам кримінального провадження. У ситуаціях, коли суди мають обгрунтоване припущення про використання ШІ і цим аргументують скасування вироку, мотивування має бути розлогим з тим, щоб було точно ідентифіковано, про яку підставу скасування вироку йдеться та як використання ШІ вплинуло на її появу.

Фінансується Європейським Союзом. Проте висловлені погляди та думки належать лише автору (-ам) і не обов'язково відображають погляди Європейського Союзу чи Європейського виконавчого агентства з питань освіти та культури (EACEA). Ні Європейський Союз, ні Європейське виконавче агентство з питань освіти та культури (EACEA) не можуть нести за них відповідальність.

Список використаних джерел:

1. Рекомендаціях з відповідального використання штучного інтелекту для правників. URL: https://storage.thedigital.gov.ua/files/2/72/fcf6c498e0a9f57e7a8521ff9833372d.pdf

2. Guidelines for the use of AI systems in courts and tribunals (Published in 2025 by the United Nations Educational, Scientific and Cultural Organization). URL: https://unesdoc.unesco.org/ark:/48223/pf0000396582

3. 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) (Text with

EEA relevance). URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

4. Ухвала Київського апеляційного суду від 30 липня 2025 року, справа № 11-кп/824/1818/2025. URL: https://reyestr.court.gov.ua/Review/129699665

5. Вирок Дніпровського районного суду міста Києва від 06 червня 2024 року. URL: https://reyestr.court.gov.ua/Review/119559177

6. Висновок КРЄС № 26 (2023): Рухаючись вперед: використання асистивних технологій у судочинстві. URL: https://hcj.gov.ua/sites/default/files/field/vysnovok_kryes_no_26_neofi ciynyy_pereklad.pdf

Глушкова Д.В.
доцент кафедри правоохоронної діяльності
навчально-наукового інституту № 5,
доктор філософії
*(Харківський національний університет
внутрішніх справ)*

КІБЕРБЕЗПЕКА ТА ШТУЧНИЙ ІНТЕЛЕКТ. ПРАВОВІ МЕХАНІЗМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ДОБУ АЛГОРИТМІВ

Стрімкий розвиток цифрових технологій та впровадження систем штучного інтелекту у різні сфери суспільного життя зумовили суттєві трансформації у підходах до обробки, зберігання та захисту персональних даних. Алгоритмічні системи дедалі активніше використовуються в публічному управлінні, правоохоронній діяльності, медицині, банківській сфері, соціальних сервісах та судочинстві. Водночас це породжує нові кібербезпекові та правові виклики, пов'язані з ризиками несанкціонованого доступу до даних, дискримінаційного алгоритмічного аналізу, втрати контролю особи над власною інформацією та складністю визначення юридичної відповідальності за порушення прав суб'єктів персональних даних.

Особливість штучного інтелекту полягає в його здатності обробляти значні масиви даних, у тому числі персональних і чутливих, із застосуванням методів машинного навчання. Саме великі набори даних є базою для функціонування сучасних алгоритмів, що об'єктивно підвищує цінність персональної інформації та одночасно рівень загроз її безпеці. Фактично персональні дані перетворюються на ключовий ресурс цифрової економіки, що потребує адекватного правового захисту [1].

На практиці використання штучного інтелекту вже призводило до резонансних порушень права на приватність. Так, у низці європейських держав були зафіксовані випадки застосування алгоритмів автоматизованого оцінювання соціальних ризиків, які на основі персональних даних громадян формували профілі «потенційно неблагонадійних осіб». Подібні системи нерідко

використовували непрозорі критерії аналізу, що унеможливлювало перевірку правильності рішень та створювало ризики дискримінації. У відповідь на це регуляторні органи Європейського Союзу неодноразово наголошували на неприпустимості автоматизованого ухвалення рішень без належного людського контролю.

Кібербезпековий аспект захисту персональних даних у системах штучного інтелекту полягає не лише у технічному захисті інформації, а й у правовому регулюванні процесів доступу, обробки та використання даних. Кібератаки, витоки інформації та зломи баз даних демонструють, що навіть високорозвинені технологічні системи залишаються вразливими. За даними відкритих аналітичних звітів, значна частина масштабних витоків персональних даних у світі була пов'язана саме з використанням автоматизованих систем аналізу інформації, які не мали належних механізмів захисту та аудиту [2].

Правові механізми захисту персональних даних у добу алгоритмів мають ґрунтуватися на поєднанні загальних принципів захисту прав людини та спеціальних норм цифрового права. Ключовими серед них є принцип законності обробки даних, мінімізації даних, цільового використання, прозорості алгоритмів та відповідальності суб'єктів, які впроваджують системи штучного інтелекту. Важливим правовим інструментом залишається інформована згода особи на обробку її персональних даних, однак у випадку складних алгоритмічних систем цей механізм часто має формальний характер, що потребує його переосмислення.

В умовах воєнних і гібридних загроз питання захисту персональних даних набуває додаткового значення. Масове використання цифрових сервісів, реєстрів та електронних платформ підвищує ризики несанкціонованого доступу до персональної інформації громадян, що може бути використано для тиску, шантажу або інформаційних операцій. У таких умовах штучний інтелект одночасно виступає і як інструмент захисту, і як потенційне джерело загроз, що вимагає особливо зваженого правового регулювання [3].

Таким чином, захист персональних даних у системах штучного інтелекту потребує комплексного підходу, який поєднує кібербезпекові заходи, правові механізми контролю та етичні

стандарти використання алгоритмів. Ефективне правове регулювання у цій сфері має бути спрямоване не на обмеження технологічного розвитку, а на забезпечення балансу між інноваціями та фундаментальними правами людини. У перспективі це сприятиме підвищенню довіри до цифрових технологій та формуванню безпечного правового середовища в умовах алгоритмічної трансформації суспільства.

Окремої уваги заслуговує проблема відповідальності за порушення кібербезпеки персональних даних у системах штучного інтелекту. На практиці складно визначити, хто саме несе юридичну відповідальність у разі завдання шкоди: розробник алгоритму, власник системи, оператор даних чи користувач. Відсутність чітких відповідей на ці питання створює прогалини у правозастосуванні та ускладнює захист прав потерпілих осіб. Саме тому в європейській правовій доктрині активно обговорюється ідея запровадження спеціального режиму відповідальності для високоризикових систем штучного інтелекту.

Список використаних джерел:

1. Права людини та штучний інтелект : аналітичний огляд [Електронний ресурс]. – Українська Гельсінська спілка з прав людини, 2024. – Режим доступу: https://www.helsinki.org.ua/wp-content/uploads/2024/05/Preview_AI_human_right_A4-1.pdf (дата звернення 16.02.2026)

2. Захист персональних даних та штучний інтелект [Електронний ресурс]. – BCA Education. – Режим доступу: https://www.bca.education/zahyst-pd-ai/ (дата звернення 16.02.2026)

3. Захист персональних даних в умовах воєнного стану [Електронний ресурс]. – Офіс Уповноваженого Верховної Ради України з прав людини. – Режим доступу: https://ombudsman.gov.ua/storage/app/media/Воєнний%20стан/Захист%20персональних%20даних/Захист%20персональних%20даних%20в%20умовах%20воєнного%20стану.pdf (дата звернення 17.02.2026)

Горпинюк О.П.
доцент кафедри кримінально-правових дисциплін
навчально-наукового інституту
права та правоохоронної діяльності,
кандидат юридичних наук, доцент
*(Львівський державний університет
внутрішніх справ)*

ПРАВОВІ ПІДСТАВИ ВИКОРИСТАННЯ БІОМЕТРИЧНИХ ДАНИХ (ТЕХНОЛОГІЙ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ) В ПРАВОЗАСТОСУВАННІ ЯК УМОВА ДОТРИМАННЯ ПРАВА НА ПРИВАТНІСТЬ[1]

Коли ми говоримо про штучний інтелект (далі – ШІ) у правозастосуванні, зокрема у кримінальних провадженнях значний інтерес становить питання використання біометричних даних, таких як відбитки пальців чи використання технологій розпізнавання обличчя. Сучасні правоохоронні органи все частіше застосовують алгоритми штучного інтелекту при роботі з біометрією. Існують автоматизовані системи дактилоскопічної ідентифікації (AFIS), що за допомогою ШІ швидко порівнюють відбитки пальців підозрюваних із базами даних[1, с.4]. Активно розвиваються технології розпізнавання обличчя: камери відеоспостереження у поєднанні з нейромережами дозволяють у режимі реального часу виявляти розшукуваних осіб у натовпі або ідентифікувати людей на відеозаписах[2, с.279]. Подібні рішення приймаються і щодо голосових даних: програмне забезпечення з елементами ШІ здатне зіставляти зразки голосу (аудіозаписи розмов) з еталонними записами, допомагаючи визначити особу

[1]«Фінансується Європейським Союзом. Проте висловлені погляди та думки належать лише автору і не обов'язково відображають погляди Європейського Союзу чи Європейського виконавчого агентства з питань освіти та культури (EACEA). Ні Європейський Союз, ні Європейське виконавче агентство з питань освіти та культури (EACEA) не можуть нести за них відповідальність».

мовця. Також з'являються спеціалізовані алгоритми для менш традиційних біометричних характеристик – наприклад, ідентифікація людини за манерою ходи на відео [3, с. 17].

Водночас, чинне на сьогодні, вітчизняне законодавство недостатньо врегульовує питання про алгоритмічні висновки, згенеровані ШІ та можливі варіанти їх використання у вигляді доказів або експертних висновків у кримінальних провадженнях чи під час судового розгляду справ, а це, своєю чергою, породжує певну правову невизначеність. Крім того існує серйозна небезпека втручання у приватність особи, шляхом неправомірного використання її біометричних даних. Зокрема, незаконне використання профілю обличчя несе серйозні ризики та може бути використано для фінансового шахрайства під час ідентифікації профілю у банківських додатках, незаконно отримане зображення обличчя може бути основою для створення відео чи аудіо (діпфейків), що часто використовується для таких посягань як шахрайство чи вимагання. Використання систем розпізнавання обличчя у громадських місцях для забезпечення правопорядку також несе певні ризики у випадку витоку персональних даних та використання у незаконних цілях (наприклад, відстежування політиків, громадських діячів з метою вт ручання у їхню діяльність).

Потрібно зробити акцент на тому, що моделі ШІ можуть мати похибки та схильність до хибних спрацьовувань[2, с.280]. Тому в цьому аспекті необхідна система перевірки точності роботи ШІ. Зокрема у літературі звертають увагу на основних ризиках використання технології розпізнавання обличчя під час війни[4]. З-поміж них: 1) помилкова ідентифікація (можливі помилки при ідентифікації обличчя, зокрема система Clearview в Україні під час війни використовується для ідентифікації загиблих російських солдатів); 2) неконтрольоване використання (йдеться про використання технологій в особистих інтересах, порушуючи права інших людей); 3) інтеграція в системи зі зброєю (використання технології під час війни можуть стимулювати подальшу розробку нового автоматизованого озброєння, що застосовує алгоритм для виявлення та ураження цілей).

Загалом слушним в контексті викладеного видається думка про необхідність належного нормативного регулювання, що

усуває відповідні ризики та дієвого судового контролю, що має слугувати своєрідною гарантією від порушень[2, с.281]. Щодо законодавчої складової, то внесення змін до вітчизняного законодавства, враховуючи існуючі зобов'язання на шляху України до вступу в ЄС необхідно враховувати прийняті на сьогодні у цій сфері два міжнародні нормативні акти. Йдеться про Регламент (ЄС) 2024/1689 Європейського Парламенту та Ради від 13 червня 2024, який ще називають Закон про штучний інтелект [5] (далі – Закон про ШІ). Стаття 5 відповідного Закону про ШІ визначає основні правила використання систем дистанційної біометричної ідентифікації в режимі реального часу в загальнодоступних місцях з метою забезпечення правопорядку. Біометричні дані, зокрема системи дистанційної біометричної ідентифікації відповідно до зазначеного закону належать до систем ШІ високого ризику (додаток ІІІ). При законодавчому регулюванні слід також брати до уваги Рамкову Конвенцію Ради Європи зі штучного інтелекту, прав людини, демократії та верховенства права від 17 травня 2024 року[6]. Важливо відзначити, що якщо перший документ встановлює положення більш загального характеру, а саме принципи, пов'язані з діяльністю ШІ (зокрема, людська гідність та індивідуальна автономія), то Закон про ШІ містить конкретні положення про використання біометричних даних. Стаття 5 зазначеного закону передбачає заборону використання систем дистанційної біометричної ідентифікації в режимі реального часу в загальнодоступних місцях з метою забезпечення правопорядку за винятком, коли це строго необхідне для досягнення таких цілей: пошук жертв викрадення, торгівлі людьми, сексуальної експлуатації людей, пошук зниклих безвісти; запобігання конкретній, істотній та безпосередній загрозі життю або фізичній безпеці фізичних осіб або реальній та існуючій, або реальній та передбачуваній загрозі терористичного нападу; локалізації або ідентифікації особи, підозрюваної у вчиненні кримінального правопорушення, з метою проведення кримінального розслідування або судового переслідування або виконання кримінального покарання за конкретні правопорушення і за які в державі-члені передбачено покарання у виді позбавлення волі або арешт на строк не менше чотирьох років. Закон про ШІ містить

перелік таких правопорушень, до яких належать: тероризм, торгівля людьми, сексуальна експлуатація дітей та дитяча порнографія, незаконний обіг наркотичних засобів або психотропних речовин, незаконна торгівля зброєю, боєприпасами або вибуховими речовинами, вбивство, тяжке тілесне ушкодження, незаконна торгівля людськими органами або тканинами, незаконна торгівля ядерними або радіоактивними матеріалами, викрадення, незаконне утримання або захоплення заручників, злочини, що підпадають під юрисдикцію Міжнародного кримінального суду, незаконне захоплення літаків або суден, згвалтування, екологічні злочини, організовані або збройні пограбування, саботаж, участь у злочинній організації, причетній до одного або кількох із перелічених вище злочинів (додаток ІІ).

Зважаючи на євроінтеограційні процеси України опиратися слід на практику Європейського суду з прав людини (далі – ЄСПЛ). На часі також вивчення практики Суду справедливості ЄС(СЄС) з відповідного питання. На сьогоднішній день ЄСПЛ поки ще не сформулював чітких правових позицій щодо використання штучного інтелекту та впливу такого використання на права гарантовані Європейською конвенцією про захист прав людини і основоположних свобод (1950р.) (далі – ЄКПЛ). Проте існує доволі широка практика ЄСПЛ щодо умов правомірності обмеження права на приватність особи шляхом автоматизованої обробки та зберігання біометричних даних, встановлення правил використання таких даних. Ключовим рішенням ЄСПЛ у частині закріплення стандартів поводження з біометричними даними як умова дотримання положень ст.8 ЄКПЛ є справа «S. and MARPER v. THE UNITED KINGDOM» (Application no.30562/04*), 04.*12.2008.

Основним питанням у цій справі було те, чи обгрунтованим слід вважати зберігання відбитків пальців та ДНК-інформації (клітинних зразків) у випадках із конкретними заявниками, які підозрювалися, але не були засуджені за певні кримінальні правопорушення. ЄСПЛ констатував у цій справі відсутність справеливого балансу між конкуруючими суспільними та приватними інтересами, а зберігання біометричних даних заявників становило непропорційне втручання у їхнє приватне життя та не було необхідним у демократичному суспільстві

(відсутність граничних строків зберігання, категоризації правопорушень, за вчинення яких дозволялось зберігання даних, а також осіб, дані яких зберігають, відсутність незалежного нагляду за процесом зберігання та будь-яких гарантій для заявників від зловживань). Примітно, що ЄСПЛ наголосив, що захист, який надається статтею 8, був би неприйнятним чином послаблений, якби використання сучасних наукових методів у системі кримінальної юстиції дозволялося за будь-якої ціни та без обережного збалансування їхніх потенційних переваг з важливими інтересами приватного життя. Будь-яка держава, яка претендувала на роль піонера у розвитку нових технологій, мала особливу відповідальність за знаходження такого правильного балансу[7].

Зокрема у цьому контексті доволі цікавою є справа CASE OF GAUGHRAN V. THE UNITED KINGDOM (Application no. 45245/15), 13 February 2020[8]. Справа стосувалась вирішення питання про правомірність зберігання біометричних даних органами поліції. За обставинами цієї справи фотографію заявника було зроблено під час його арешту для безстрокового зберігання в місцевій поліцейській базі даних. Фотографія зберігалася в автономній базі даних, доступ до якої мали лише уповноважені працівники поліції, які не мали можливості зіставляти фотографії ані за допомогою технології розпізнавання облич, ані іншим способом. Однак як згодом було встановлено, хоча відповідна база даних не мала програмного забезпечення для розпізнавання чи картографування облич, однак фотографії з цієї бази могли бути завантажені до Національної поліцейської бази даних, яка таке програмне забезпечення мала. Як встановив ЄСПЛ у цій справі Національна поліцейська база даних (PND) створена для сприяння обміну оперативною інформацією дозволяє уповноваженому користувачеві (зазвичай поліцейському) здійснювати пошук серед збережених у PND фотографій, зроблених під час тримання під вартою, шляхом їх порівняння із зображенням, яке він тимчасово завантажує зі своєї локальної бази даних. У зазначеному рішенні ЄСПЛ встановив, що невибірковий характер повноважень щодо зберігання ДНК-профілю, відбитків пальців і фотографії заявника як особи, засудженої за правопорушення, навіть якщо воно є погашеним, без урахування тяжкості правопорушення чи необхідності безстрокового зберігання та за відсутності будь-якої

реальної можливості перегляду, не забезпечив справедливого балансу між конкуруючими суспільними та приватними інтересами. Держава має дещо ширшу межу розсуду щодо зберігання відбитків пальців і фотографій, однак ця розширена межа не є достатньою для висновку про пропорційність зберігання таких даних за обставин цієї справи, які включають відсутність будь-яких належних гарантій, зокрема відсутність реальної процедури перегляду (п. 96).

Важливий також висновок, на якому наголошує ЄСПЛ у цьому рішенні про те, що серед договірних держав на сьогодні відсутній консенсус щодо зберігання біометричних даних і у цьому випадку межа розсуду держав може бути відрізнятися. Проте у цій справі ЄСПЛ звузив межу розсуду доступну державі-відповідачу щодо конкретного виду біометричних даних, а саме зберігання ДНК-профілів (п.84), враховуючи стрімкий технологічний розвиток та технології розпізнавання обличчя. ЄСПЛ слушно зазначив, що стосовно відбитків пальців і фотографій строки зберігання, які закінчуються у момент смерті або невдовзі після неї, можуть вважатися співмірними з безстроковим зберіганням; водночас він усвідомлює можливість стрімкого технологічного розвитку в цій сфері, зокрема щодо технологій розпізнавання та картографування облич (п.80).

Знаковим рішенням у контексті правових позицій ЄСПЛ щодо використання технологій розпізнавання обличчя в реальному часі належить відзначити справу «GLUKHIN v. RUSSIA» (Application no.30562/04), 04.07.2023[9]. За обставинами справи заявника, який провів в 2019 році, в метро м. Москви, одиничний мирний пікет, було затримано за вчинення адміністративного правопорушення поліцією, яка використала систему відеоспостереження з функцією розпізнавання обличчя, порівнявши його фото з соцмереж із записами з камер. У цьому рішенні ЄСПЛ дійшов висновку, що обробка персональних даних заявника в межах провадження щодо адміністративного правопорушення, включно з використанням технології розпізнавання облич – по-перше, для його ідентифікації за фотографіями та відео, опублікованими в Telegram, і, по-друге, для встановлення його місцезнаходження та затримання під час поїздки в московському метро – становила втручання у його право

на повагу до приватного життя у розумінні пункту 1 статті 8 ЄКПЛ (п. 73). При цьому національне законодавство дозволяло обробку біометричних персональних даних у зв'язку з розслідуванням і переслідуванням будь-якого правопорушення, незалежно від його характеру та тяжкості (п.87). Своєю чергою використання технології розпізнавання облич для ідентифікації заявника за фотографіями та відео, опублікованими в Telegram, а тим більше використання технології розпізнавання облич у режимі реального часу для встановлення його місцезнаходження та затримання під час поїздки в московському метро, не відповідало «нагальній суспільній потребі» (п. 89) при звинуваченні в адміністративному правопорушенні та не могло вважатися необхідним у демократичному суспільстві (п. 90).

Відповідне рішення важливе також з огляду на те, що в ньому ЄСПЛ посилається на Керівні принципи щодо розпізнавання облич(2021) [10], ухвалені Консультативним комітетом Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних [11], виконання якої для України обов'язкове починаючи ще з 2011 року. У Керівних принципах наголошується на обов'язку держав-сторін Конвенції встановити правову базу, застосовну до обробки біометричних даних за допомогою розпізнавання обличчя. Ця правова база повинна визначати для кожного окремого випадку використання технологій: детальне пояснення конкретного способу використання та передбачуваної мети; мінімальну надійність і точність використовуваного алгоритму; строки зберігання використаних фотографій; можливість проведення аудиту за цими критеріями; простежуваність процесу; заходи безпеки (гарантії захисту) [10, с. 7].

Таким чином можна зробити висновки, що стрімкий розвиток технологій штучного інтелекту дедалі частіше проникає до різних сфер суспільного життя та суттєво впливає на правозастосування. Незважаючи істотні переваги використання технологій розпізнавання обличчя для боротьби зі терористичною та організованою злочинністю на сьогодні вітчизняне законодавство ще недостатньо чітко та грунтовно регулює питання про алгоритмічні висновки, згенеровані ШІ та можливі варіанти їх використання у правозастосуванні, зокрема у кримінальних

провадженнях. Проте євроінтеграційні вимоги, які стоять перед Україною передбачають її обов'язок вивчати та в перспективі гармонізувати національне законодавство із існуючими нормативними актами Ради Європи та Європейського Союзу у цій сфері. Зокрема йдеться про уже згадуваний Закон про ШІ, Конвенцію Ради Європи зі штучного інтелекту, прав людини, демократії та верховенства права, Керівні принципи щодо розпізнавання облич, ухвалені Консультативним комітетом Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних. Запорукою успішної інтеграції України у європейський правовий простір є також вивчення практики ЄСПЛ та Суду справедливості ЄС (СЄС). Адже відповідні міжнародні судові інституції встановлюють європейські стандарти захисту прав людини, без знання відповідної судової практики неможливе розуміння ефективного застосування європейських правових норм у реальному житті.

На сьогоднішній день ЄСПЛ перебуває на шляху формування правових позицій щодо використання штучного інтелекту та впливу такого використання на права гарантовані ЄКПЛ. Вивчення практики ЄСПЛ з питань правомірного використання біометричних даних, а саме технологій розпізнавання обличчя в правоохоронній діяльності дозволяє зробити наступні висновки.

У аналізованих категоріях справ, що переважно розглядаються крізь призму ст.8 ЄКПЛ, ЄСПЛ наголошує на умовах, за яких зберігання персональних даних буде пропорційне, зважаючи на інтереси суспільства та приватні інтереси осіб. Зокрема до умов правомірності зберігання біометричних даних в базах даних відносяться випадки, коли: 1) зберігання стосується тільки засуджених осіб за кримінальні правопорушення за які передбачено покарання у виді позбавлення волі, тобто у джержавах-відповідачах встановлений режим зберігання враховує мінімальний ступінь тяжкості правопорушення; 2) існує граничний строк зберігання таких даних, що встановлений законодавством; 3) наявність та функціонування певних гарантій для особи, дані якої зберігаються безстроково (наприклад, надання заявникові права клопотати про видалення даних щодо нього, якщо їх подальше зберігання більше не є необхідним з огляду на характер

правопорушення, вік особи, тривалість часу, що минула, та її нинішню особистість).

Що стосується правових висновків з питань використання правоохоронними органами саме технологій розпізнавання обличчя, то ЄСПЛ звузив межу розсуду доступну державі-відповідачу щодо конкретного виду біометричних даних, а саме зберігання ДНК-профілів, враховуючи стрімкий технологічний розвиток та технології розпізнавання обличчя і ризик для приватності, який це може мати. Для обробки таких біометричних даних вимагаються чіткі строки для зберігання та гарантії для осіб, права яких обмежуються.

Список використаних джерел:

1. Басиста І.В., Удовенко Ж.В., Кулинич М.А. Огляд тенденцій щодо штучного інтелекту та його перспектив для процесуальних рішень під час кримінального провадження. *Науковий вісник Ужгородського національного університету.* Серія: Право. 2024. Вип. 81(3). С. 19-38. DOI: https://doi.org/10.24144/2307-3322.2024.81.3.3.

2. Машталяр О.М. Штучний інтелект і біометричні дані в кримінальному процесі України: допустимість, ризики, судовий контроль. *Науковий вісник Ужгородського Національного Університету*. 2025. *Серія ПРАВО. Випуск 92. Частина 3. С.*276-283

4. Хахановський В.Г., Чашницька Т.Г. Ідентифікація особи за ходою, зафіксованою в матеріалах відеозапису. Криміналістичний вісник. 2020. № 1(33). С. 72–79. DOI: https://doi.org/10.37025/1992-4437/2020-33-1-72.

5. Ліманте А., Москвитин Ю. Технологія розпізнавання обличчя: ризики застосування у воєнний час. *Юридична газета. Коментарі. 13 вересня 2024. URL*.: https://yur-gazeta.com/dumka-eksperta/tehnologiya-rozpiznavannya-oblichchya-riziki-zastosuvannya-u-voenniy-chas.html#:~:text

6. 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) No168/2013, (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). URL.: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689 [in English].

7. Конвенція Ради Європи зі штучного інтелекту, прав людини, демократії та верховенства права 133-тє Засідання Комітету міністрів (Страсбург, 17 травня 2024 року) *URL*.: https://vkksu.gov.ua/sites/default/files/rye_ramkova_konvenciya_zi_shtuchnogo_intelektu_prav_lyudyny_demokratiyi_ta_verh._prava.pdf

8. «S. and MARPER v. THE UNITED KINGDOM» *(Application no.30562/04), 04.*12.2008. *URL*.: https://hudoc.echr.coe.int/fre?i=001-117816

9. CASE OF GAUGHRAN V. THE UNITED KINGDOM *(Application no. 45245/15)* 13.02.2020. *URL*.: https://hudoc.echr.coe.int/ukr?i=001-200817

10. «GLUKHIN v. RUSSIA» *(Application no.30562/04),* 04.07.2023 *URL*.: https://hudoc.echr.coe.int/?i=001-225655

11. Guidelines on facial recognition (2021) dopted by the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108) URL.: https://edoc.coe.int/fr/intelligence-artificielle/9753-guidelines-on-facial-recognition.html

12. Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних (ETS № 108) від 28 січня 1981 року**.** URL.: https://zakon.rada.gov.ua/laws/show/994_326#Text

Грезіна О.М.
доцент кафедри кримінального аналізу
та інформаційних технологій,
доктор філософії
(Одеський державний університет внутрішніх справ)

ВИКОРИСТАННЯ ІНСТРУМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ В КРИМІНАЛЬНОМУ АНАЛІЗІ

Стрімкий розвиток технологій штучного інтелекту (ШІ) суттєво трансформує методологічні підходи до виявлення, розслідування та попередження злочинів. Кримінальний аналіз, як системна діяльність із збору, обробки та інтерпретації інформації про злочинні прояви, дедалі активніше інтегрує алгоритмічні інструменти для підвищення ефективності оперативно-розшукової та слідчої роботи [1]. Застосування методів машинного навчання, обробки природної мови та комп'ютерного зору відкриває принципово нові можливості для аналізу великих масивів кримінальних даних, прогнозування злочинної поведінки та ідентифікації прихованих зв'язків між суб'єктами злочинної діяльності.

Серед ключових напрямів впровадження ШІ в кримінальному аналізі особливе місце займають системи предиктивної аналітики. Зазначені системи ґрунтуються на алгоритмах глибокого навчання (deep learning) та дозволяють на підставі статистичних закономірностей минулих злочинів формувати прогнози щодо ймовірних місць і часу вчинення нових правопорушень. Дослідження, проведені в межах розробки систем прогностичного поліціювання, демонструють, що використання алгоритмів кластеризації та регресійного аналізу забезпечує високий рівень точності прогнозування. Водночас, наголошуються на необхідності критичного осмислення ризиків алгоритмічної упередженості, що може призводити до дискримінації певних соціальних груп при прийнятті рішень правоохоронними органами.

Окремим і надзвичайно перспективним напрямом є застосування технологій обробки природної мови (NLP) для аналізу текстових масивів у кримінальному судочинстві.

Автоматизована обробка матеріалів кримінальних проваджень, протоколів допитів, оперативних зведень та відкритих джерел інформації дозволяє виявляти приховані закономірності, виокремлювати ключові сутності та встановлювати зв'язки між суб'єктами злочинної діяльності значно швидше, ніж це можливо в ручному режимі. Великі мовні моделі (LLM) вже сьогодні успішно застосовуються для автоматичного реферування матеріалів справ, класифікації злочинів за видами та генерації аналітичних звітів, що суттєво скорочує часові витрати аналітиків і слідчих на рутинні операції з обробки інформації.

Технології розпізнавання обличчя та комп'ютерного зору становлять ще один вагомий сегмент застосування ШІ в правоохоронній діяльності. Системи відеоспостереження, інтегровані з алгоритмами біометричної ідентифікації, дозволяють здійснювати автоматичний пошук підозрюваних осіб у базах даних в режимі реального часу [2]. Проте, активне впровадження зазначених технологій супроводжується дискусіями щодо їх відповідності стандартам захисту персональних даних та основоположних прав людини. Зокрема, Загальний регламент захисту даних (GDPR) Європейського Союзу та національне законодавство низки держав встановлюють суттєві обмеження щодо умов і порядку використання біометричних даних у правоохоронних цілях, що потребує вироблення збалансованих правових механізмів регулювання.

Важливим аспектом інтеграції ШІ в кримінальний аналіз є питання допустимості та доказової цінності результатів, отриманих за допомогою алгоритмічних систем. У більшості правових систем результати автоматизованого аналізу наразі розглядаються лише як орієнтуюча інформація, що потребує верифікації уповноваженими фахівцями та не може самостійно слугувати підставою для процесуальних рішень. Водночас, серед наукової спільноти формується нова доктрина ««пояснюваного штучного інтелекту» (Explainable AI, XAI) [3], яка вимагає від алгоритмічних систем забезпечення прозорості логіки прийнятих рішень», що є критично важливим для дотримання принципів верховенства права та права особи на справедливий суд.

Науковці зазначають, що «ключовими напрямами вдосконалення методології боротьби з кіберзлочинністю є

використання систем штучного інтелекту для виявлення кіберзагроз, розвиток цифрової криміналістики, впровадження прогностичної аналітики на основі машинного навчання, розширення міжнародної співпраці та підвищення кваліфікації правоохоронців у сфері інформаційних технологій» [4]

Таким чином, впровадження інструментів штучного інтелекту в кримінальний аналіз є об'єктивною тенденцією, зумовленою потребами сучасного правоохоронного середовища. Ефективне використання ШІ-технологій потребує комплексного підходу, що поєднує вдосконалення технічних рішень, розроблення відповідної нормативно-правової бази та підвищення цифрової компетентності фахівців у сфері кримінального судочинства. Перспективами подальших досліджень є розробка методологічних стандартів використання ШІ-інструментів у кримінальному аналізі, визначення критеріїв допустимості алгоритмічних доказів у кримінальному процесі та формування єдиних підходів до забезпечення кібербезпеки правоохоронних баз даних.

Список використаних джерел

1. Muhati E., Rawat D. Data-Driven Network Anomaly Detection with Cyber Attack and Defense Visualization. *Journal of Cybersecurity and Privacy*. 2024. Vol. 4, No. 2. P. 241–263. DOI: 10.3390/jcp4020012.

2. Simmler M., Canova G. Facial recognition technology in law enforcement: Regulating data analysis of another kind. *Computer Law & Security Review*. 2025. Vol. 56.Art. 106092. DOI: 10.1016/j.clsr.2024.106092.

3. Коростін О. О. Explainable AI: нові підходи до інтерпретованості глибоких нейронних мереж. *Вісник Херсонського національного технічного університету*. 2025. Т. 2, № 1(92). DOI: 10.35546/kntu2078-4481.2025.1.2.14. URL: https://journals.kntu.kherson.ua/index.php/visnyk_kntu/article/view/861

4. Форос Г.В., Калугін В.Ю., Грезіна О.М. Методологія кримінального аналізу в умовах зростання кіберзагроз. Юридичний науковий електронний журнал. № 11/2025.С. 356-359. https://doi.org/10.32782/2524-0374/2025-11/74

Гуцуляк Ю.В.
доцент кафедри кримінального процесу
та криміналістики факультету № 1,
доктор філософії
(Львівський державний університет внутрішніх справ)

ПРО ПИТАННЯ АКТУАЛЬНОСТІ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ARTIFICIAL INTELLIGENCE В КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Розвиток технологій здатних автономно виконувати складні комплекси завдань, викликає постійний запит на такий продукт для впровадження у все ширше коло правовідносин та сфер господарювання. Технології здатні вирішувати завдання за аналогією з свідомістю людини, з високими аналітичними показниками, умовно прийнято називати Artificial Intelligence (AI) або ж Штучний Інтелект (ШІ)[1].

Технології штучного інтелекту за останні кілька десятиліть активно впроваджуються в різноманітні сфери людської діяльності, з метою автоматизації процесів, підвищення ефективності виконання завдань, підтримання високого рівня точності виконання завдань (продуктивності), оптимізації часу для виконання поставлених завдань, та навіть з метою оптимізації прийняття рішень управлінського рівня.

Необхідність запровадження новітніх технологій такого кшталту має декілька причин. По перше, це цифрова трансформація діяльності людства; по друге, гіперзростання об'єму інформації; по третє, пряма залежність часу необхідного для опрацювання та прийняття рішення від наявного об'єму інформації. Перелік названих нами передумов для впровадження сучасних технологій обробки та аналізу інформації, не є вичерпний і може корелюватись в залежності від специфіки галузі в якій він застосовується.

Зростання числа кримінальних правопорушень як у сфері цифрового обміну інформацією, так і за допомогою цифрових

[1] В межах доповіді не аналізується зміст поняття ШІ, автором умовно запропоновано поняття «технологія».

технологій, вимагає адекватної протидії від держави таким суспільно-небезпечним діянням.

Сфера кримінальної юстиції все активніше включається в процес використання потенціалу машинного навчання. Як слушно підкреслено дослідниками, це стало реакцією на виклики з стрімкого розвитку науки й техніки, питання впровадження штучного інтелекту в професійну діяльність представників держави сфери кримінальної юстиції. За таких умов особливої актуальності набувають проблеми активізації розроблення та впровадження інноваційних підходів у криміналістиці, новітніх технологій і криміналістичних засобів, а також їх активне застосування в слідчій (детективній), судовій та експертній діяльності у сфері протидії злочинності. Серед таких засобів найбільш перспективним у сучасних умовах глобальних загроз і воєнних викликів є використання технологій штучного інтелекту [1, с. 84].

Також, наводяться причини співрозмірної реакції запиту на ШІ, зростання зацікавленості представників так званого «кримінального середовища» сферою інформаційних технологій, що передбачає використання відповідних наукових досягнень у протиправній діяльності, а також наявністю позитивного досвіду застосування ШІ в протидії злочинності в ряді зарубіжних держав [5, с.298]. Вплив воєнного стану на криміногенну ситуацію в державі, а також колапс традиційної доказової бази, дефіцит оперативних ресурсів, обмежений людський фактор та необхідність швидкої обробки великих обсягів інформації – теж виокремлюються як першопричини, що визначають необхідність впровадження надбань технологій ШІ в кримінальне провадження [6, с. 357].

Тому серед головних пріоритетів, які визначені в Комплексному стратегічному плані реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 року [2], йдеться про широке використання під час здійснення досудового розслідування, а також для обробки даних та аналітичної діяльності органів правопорядку і прокуратури штучного інтелекту, блокчейну, хмарних обчислень та інших інноваційних рішень.

Слід виокремити реалії війни, які з військової сфери, зміни ситуації в Україні мають вплив на запити криміналістики, кримінального процесу, кримінального права, тощо. Як слушно зазначає В.М. Шевчук, однією з найважливіших тенденцій у зв'язку з такими реаліями є інтеграція знань, створення та впровадження інноваційних розробок, широке використання цифрових технологій та штучного інтелекту, спрямованих на вирішення завдань протидії злочинності та формування доказової бази [3, с. 203]. Серед таких засобів найбільш перспективним у сучасних умовах глобальних загроз і воєнних викликів, з огляду на окремі дослідження, є використання технологій штучного інтелекту [4, с. 84].

Безумовним підґрунтям необхідності впровадження технологій штучного інтелекту у кримінальному провадженні є зростання обсягу інформацію, необхідної для опрацювання, аналізу та систематизації. Інформації, яка потенційно може бути фактичними даними у конкретному кримінальному провадженні. Швидкість опрацювання таких даних, точність їх опрацювання це забезпечення виконання завдань кримінального провадження (ст.2 КПК України) та дотримання засад кримінального провадження, зокрема засади розумних строків (ст.28 КПК України). Адже однією з ключових переваг технологій ШІ є можливість швидкого пошуку закономірностей та кореляцій у даних, що сприяє встановленню послідовності подій та можливого кола осіб, які свідків вчинення кримінального правопорушення, так і співучасників його вчинення.

Водночас, скористатись сучасним необхідним інструментарієм, яким є технології ШІ, в кримінальному провадженні, можливо винятково з врахуванням і дотриманням засад кримінального провадження, захисту персональних даних, прозорості алгоритмів та недопущення дискримінаційних рішень на основі результатів застосування.

ШІ, як технологія, на наше переконання, є інструментарієм, а не заміни людського розсуду.

Отже, актуальність застосування ШІ у кримінальному процесі це не лише підвищення ефективності й швидкості розслідування, а й можливість модернізації інструментарію правосуддя.

Список використаних джерел:

1. Шевчук В. Перспективні напрями використання технологій штучного інтелекту в розслідуванні кримінальних правопорушень. Інноваційні методи та цифрові технології в криміналістиці й судовій експертизі: монографія / В.Ю. Шепітько, Г.К. Авдєєва, В.М. Шевчук та ін.Харків: Право, 2024. С. 83–106. URL: https://ivpz.kh.ua/wp-content/uploads/ 2025/01/Монорафія-Криміналістів-2024.pdf (дата звернення: 20.07.2025)

2. Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2017 року: Указ Президента України № 273/2023 від 11 травня 2023 року. URL: https://zakon.rada.gov.ua/laws/show/273/2023#Text

3. Shevchuk V. Development trends in criminalistics in the era of digitalization. Modern Knowledge: Research and Discoveries: Proceedings of the 1st International Scientific and Practical Conference (Vancouver, Canada, May 19-20, 2023). P. 198-219. DOI 10.51582/interconf.19-20.05.2023.019

4. Шевчук В. Перспективні напрями використання технологій штучного інтелекту в розслідуванні кримінальних правопорушень. Інноваційні методи та цифрові технології в криміналістиці й судовій експертизі: монографія / В.Ю. Шепітько, Г.К. Авдєєва, В.М. Шевчук та ін. Харків: Право, 2024. С. 83–106. URL: https://ivpz.kh.ua/wp-content/uploads/ 2025/01/Монорафія-Криміналістів-2024.pdf (дата звернення: 20.07.2025).

5. Курман О.В. Переваги та проблемні питання використання штучного інтелекту при дослідженні цифрових сліді. *Науковий вісник Ужгородського Національного Університету*. 2025. Серія ПРАВО. Випуск 90: частина 4. С. 297-302.

6. Шкелебей В.А., Галаган В.І., Удовенко Ж.В. Проблеми законодавчого врегулювання використання штучного інтелекту під час досудового розслідування в умовах воєнного стану. *Науковий вісник Ужгородського Національного Університету*. 2025. Серія ПРАВО. Випуск 90: частина 4. С. 355-361.

Денисюк О.В.
здобувачка ступеня магістра
(Одеський державний університет внутрішніх справ).
Науковий керівник – **Середницька І.А.**
доцент кафедри цивільно-правових дисциплін
інституту права та безпеки
(Одеський державний університет внутрішніх справ)

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ПРОЦЕДУРАХ АЛЬТЕРНАТИВНОГО ВИРІШЕННЯ СПОРІВ

Сучасний етап розвитку правової системи характеризується активним упровадженням цифрових технологій, зокрема штучного інтелекту, у механізми правового регулювання та вирішення конфліктів. Одним із найбільш динамічних напрямів є застосування інтелектуальних систем у процедурах альтернативного вирішення спорів, що традиційно розглядаються як гнучкі, менш формалізовані та економічно доступні способи врегулювання правових конфліктів без звернення до суду. Однак, незважаючи на позитивні можливості, широке використання штучного інтелекту супроводжується низкою юридичних, етичних та технологічних проблем, які потребують комплексного дослідження.

Насамперед, залишається невизначеним питання меж автономності інтелектуальних систем та допустимості їх участі у прийнятті рішень, що впливають на права та обов'язки сторін. Неврегульованим є питання відповідальності за помилки алгоритмів, а також критеріїв оцінки об'єктивності, прозорості та неупередженості результатів, згенерованих на основі автоматизованої обробки даних. Законодавство не містить однозначних положень щодо захисту персональних даних та забезпечення конфіденційності учасників таких процедур, що створює значні ризики порушення їхніх прав. Крім того, відсутні національні стандарти сертифікації технологічних рішень, що застосовуються у процесі альтернативного вирішення спорів.

Таким чином, проблема полягає у необхідності формування науково обґрунтованої концепції правового регулювання використання штучного інтелекту у процедурах альтернативного вирішення спорів, здатної забезпечити баланс між цифровими інноваціями та конституційними гарантіями захисту прав людини.

Подальший розвиток досліджуваного питання потребує глибшого аналізу можливостей та ризиків використання штучного інтелекту у процедурах альтернативного вирішення спорів з урахуванням доктринальних напрацювань та практичних потреб. Насамперед важливо зазначити, що альтернативні процедури вирішення спорів – медіація, переговори, арбітраж та інші позасудові інструменти врегулювання конфліктів – мають суттєвий потенціал для використання штучного інтелекту як інструмента забезпечення ефективності й швидкості процедур, що базуються на багатофакторному аналізі даних і моделюванні можливих результатів спору. Саме альтернативні способи урегулювання спорів нині формують новий напрям модернізації правосуддя, який потребує розширення технологічної складової та впровадження інновацій для зміцнення довіри громадян до системи вирішення конфліктів [1, с. 32]. У цьому контексті штучний інтелект може виконувати функції аналітичної підтримки, забезпечуючи як сторони спору, так і посередника об’єктивними та структурованими даними, що сприяють прийняттю взаємоприйнятного рішення.

Проте, разом з беззаперечними перевагами, використання штучного інтелекту у процедурних механізмах альтернативного вирішення спорів потребує врахування низки ризиків. Одним із найпроблемніших аспектів є питання відповідальності за результати діяльності інтелектуальних систем. Сучасні технології, що використовуються в автоматизованих платформах переговорів або онлайн-медіації, здатні не лише обробляти дані, а й пропонувати варіанти вирішення спору. У ситуаціях, коли такі рішення обумовлюють істотні правові наслідки для сторін, постає питання юридичної відповідальності за помилки алгоритмічних моделей. З огляду на це у літературі наголошують на необхідності оптимізації механізмів правової охорони цифрових продуктів та алгоритмів, зважаючи на складність визначення правового титулу створених результатів і меж відповідальності розробників [2]. У

правовій науці ще не існує однозначного підходу до вирішення питання, чи повинен результат, згенерований штучним інтелектом, вважатися юридично значущим актом та хто має бути його належним суб'єктом – людина чи програма.

Це співвідноситься з більш широкою дискусією про правовий статус штучного інтелекту, проаналізованою у наукових роботах. Дослідники стверджують, що відсутність чітко визначеного правового статусу штучного інтелекту створює нормативний вакуум, який унеможливлює ефективне правозастосування у ситуаціях, коли автономні алгоритмічні рішення можуть завдати шкоди фізичним чи юридичним особам [3]. Низка правових систем і міжнародних ініціатив намагаються вирішити цю проблему, пропонуючи концепції електронної правосуб'єктності або функціональної правової відповідальності штучного інтелекту. Проте більшість учених наголошує, що надання штучному інтелекту статусу самостійного суб'єкта права є передчасним. Такий підхід може спричинити ризик розмивання межі між відповідальністю людини та технічного механізму, що потенційно призведе до уникнення відповідальності з боку реальних суб'єктів, які здійснюють контроль над системою [3].

Не менш важливим є питання інформаційної етики й впливу штучного інтелекту на міжособистісну комунікацію у процесі врегулювання спорів. Адже альтернативні процедури вирішення конфліктів, особливо медіація, значною мірою ґрунтуються на емоційному сприйнятті, довірі, психологічному залученні сторін. Впровадження технологій штучного інтелекту має неоднозначний вплив на культуру спілкування, оскільки сприяє стандартизації мовлення і зниженню автентичності комунікації між людьми [4, с.160]. Перенесення міжособистісної взаємодії в алгоритмічне середовище може призвести до втрати гуманістичного складника, що є ключовим елементом успішного врегулювання спору. Отже, впровадження інтелектуальних систем у медіаційні процедури потребує чіткої регламентації щодо меж і умов використання алгоритмічних рекомендацій з метою недопущення домінування машинних рішень над волею сторін.

Суттєвою перешкодою для широкого впровадження штучного інтелекту у сферу альтернативного вирішення спорів є відсутність єдиного законодавчого підходу. Наразі ані національні,

ані міжнародні правові стандарти не містять комплексних регуляцій, які б забезпечували гарантії прозорості, відповідальності та безпеки використання штучного інтелекту у таких процедурах. Окрім того, мінливість технологічного розвитку призводить до постійного відставання правового регулювання від реальних суспільних потреб. Усе це створює значні ризики: можливість алгоритмічної дискримінації, витік конфіденційної інформації, маніпулювання результатами обговорень та спотворення принципу рівності сторін. Тому нагальною потребою є розроблення державної політики, спрямованої на створення правової моделі регулювання штучного інтелекту, яка включала б поєднання правових, етичних та технологічних засобів гарантування безпеки.

У науковій літературі дедалі ширше обговорюється концепція «гібридної моделі відповідальності», яка передбачає спільну участь людини та штучного інтелекту у прийнятті процесуальних рішень. У межах такого підходу ролі між сторонами чітко розмежовуються: штучний інтелект забезпечує аналітичну підтримку і оптимізацію інформаційних процесів, але остаточне рішення залишається виключною прерогативою людини. Таким чином, алгоритми виступають інструментом підсилення, а не підміною професійного розсуду. Ця модель уможливлює одночасне використання технологічних переваг та дотримання стандартів справедливості.

Разом із тим необхідною передумовою такого підходу є впровадження стандартів алгоритмічної прозорості, зрозумілості та аудитності систем, що застосовуються у процедурі альтернативного вирішення спорів. Без цього неможливо гарантувати ані об’єктивність результатів, ані відновлення довіри до правового процесу. Необхідність удосконалення правового регулювання у цьому напрямі підтверджує зростання міжнародної уваги до проблем відповідальності штучного інтелекту, використання етичних кодексів цифрової поведінки та стандартизації безпеки даних.

Отже, використання штучного інтелекту у процедурах альтернативного вирішення спорів є перспективним напрямом модернізації механізмів вирішення правових конфліктів, здатним забезпечити ефективність, швидкість та доступність процедур.

Водночас упровадження таких технологій неможливе без чіткого правового регулювання меж автономності систем, визначення механізмів відповідальності, гарантій прозорості та захисту прав людини. Перспективною є модель розвитку, за якою штучний інтелект виступає допоміжним інструментом підтримки комунікації та аналітики, а остаточне рішення залишається за людиною. Саме такий підхід забезпечує баланс між технологічними можливостями інновацій і фундаментальними принципами справедливості, неупередженості та верховенства права.

Список використаних джерел:

1. Слюсаренко К. Р. Альтернативні методи врегулювання спорів: пошук нових напрямів юриспруденції. *Право і суспільство*. 2024. № 1, т. 2. С. 28-33.

2. Кірін Р.С., Гутий Б.В., Дніпров О.С. Оптимізація правових механізмів захисту інтелектуальної власності у сфері штучного інтелекту та цифрових технологій. *Український політико-правовий дискурс*.2025. №9. URL: https://doi.org/10.5281/zenodo.15081410

3. Мохначук С. В., Ломака І. І. Визначення правового статусу штучного інтелекту в контексті порушення прав людини. Український політико-правовий дискурс. 2025. № 14. URL: https://doi.org/10.5281/zenodo.16869109

4. Парфенюк І. Вплив технологій штучного інтелекту на міжособистісні комунікації: сучасність і майбутнє. *Питання культурології.* 2025. № 45. С. 150-163.

Деревягін О.О.
професор кафедри ОРД та РЗ ННІ № 2,
кандидат юридичних наук,
старший науковий співробітник
(Харківський національний університет внутрішніх справ)

ІНТЕГРАЦІЯ МЕТОДІВ ПОВЕДІНКОВОЇ БІОМЕТРІЇ ТА НЕЙРОМЕРЕЖЕВОЇ СТИЛОМЕТРІЇ В ОПЕРАТИВНО-РОЗШУКОВУ ПРАКТИКУ ІДЕНТИФІКАЦІЇ КІБЕРЗЛОВМИСНИКІВ

Стрімка еволюція цифрового середовища та масове використання кіберзлочинцями засобів анонімізації мережевого трафіку (VPN, проксі-сервери, децентралізовані мережі) призвели до критичного зниження ефективності традиційних методів ідентифікації за базовими ідентифікаторами (IP- чи MAC-адресами). За таких умов на перший план виходять сучасні інструменти розвідки на основі відкритих джерел (OSINT) та глибокого апаратного профілювання. Практика показує, що навіть приховуючи своє реальне місцезнаходження, зловмисник неминуче передає серверам унікальні цифрові сліди свого обладнання: від обсягу оперативної пам'яті та специфічної роздільної здатності дисплея до індивідуальних мікродефектів рендерингу графіки відеокартою (WebGL та Canvas-відбитки). Збір цих унікальних даних пристрою дозволяє формувати стійкий багатовимірний маркер об'єкта, що робить можливою його деанонімізацію без необхідності прямого технічного проникнення.

В умовах поточних українських реалій, що супроводжуються безпрецедентним рівнем кіберзагроз з боку ворожих хакерських угруповань та координаторів інформаційно-психологічних операцій, вдосконалення цього інструментарію є стратегічним пріоритетом [1, с. 307]. Перед правоохоронними органами постає гостра необхідність впровадження комплексних аналітичних підходів. Синтез методів перехресного аналізу відкритих даних, фіксації апаратних метаданих пристрою та інструментів нейромережевої стилометрії (лінгвістичного аналізу текстових масивів) відкриває нові вектори для встановлення особи

правопорушника [2, с. 88]. Таке поєднання технологій здатне забезпечити оперативні підрозділи надійною орієнтувальною інформацією, а органи досудового розслідування – належною доказовою базою, нівелюючи спроби зловмисників застосувати штучну обфускацію своїх цифрових слідів. Варто зазначити, що проблематика використання новітніх ідентифікаційних систем набула широкого розповсюдження у вітчизняних наукових дослідженнях, зокрема у ґрунтовних працях В.П. Захарова та В.І. Рудешка, присвячених застосуванню біометричних технологій у діяльності правоохоронних органів [3].

У сучасній практиці оперативно-розшукової діяльності (далі – ОРД) процес деанонімізації цільового об'єкта все частіше базується на перехресному аналізі відкритих даних (OSINT) та глибокому апаратному профілюванні. Головна перевага цього підходу полягає в тому, що браузер або мобільний додаток зловмисника, навіть за умови використання захищених з'єднань (Tor, VPN), неминуче передає серверам розширену технічну інформацію, яка є критично необхідною для коректного відображення вебконтенту.

Ідентифікація (офізичення) особи в такому випадку здійснюється не через змінні мережеві адреси, а через фіксацію унікальної комбінації апаратних характеристик самого пристрою. До таких маркерів, що формують цифровий відбиток, належать: обсяг вбудованої оперативної пам'яті пристрою, кількість доступних потоків або ядер процесора; унікальна роздільна здатність дисплея (включно зі специфічним системним масштабуванням інтерфейсу, що часто використовується на нестандартних моніторах) та глибина кольору; параметри рендерингу графіки відеокартою (WebGL та Canvas-відбитки). Ці технології промальовують приховані тестові зображення у фоновому режимі, фіксуючи мікроскопічні, унікальні для кожного фізичного кремнієвого чіпа відхилення у згладжуванні шрифтів та пікселів, формуючи математично унікальний хеш пристрою.

З точки зору тактики ОРД, отримання такого масиву даних не обов'язково потребує застосування складних засобів негласного зняття інформації (троянських програм чи шпигунського програмного забезпечення). Шляхом створення легендованих веб-ресурсів або застосування інструментів генерування посилань-

«пасток» (tracking links) у межах проведення оперативних комбінацій (наприклад, під час спілкування з об'єктом під вигаданим профілем), оперативні підрозділи можуть негласно зібрати цей апаратний відбиток. Навіть якщо фігурант регулярно змінює IP-адресу, застосовує ланцюжки проксі-серверів та очищає файли cookie, ймовірність збігу складної конфігурації оперативної пам'яті, роздільної здатності та мікродефектів рендерингу в іншого користувача є мінімальною.

Наступним логічним етапом деанонімізації є глибинна інтеграція отриманого апаратного профілю з інструментарієм нейромережевої стилометрії. Встановлення суто технічного зв'язку між різними мережевими сесіями доводить лише те, що активність велася з одного фізичного пристрою (чи його клону), проте це не ідентифікує особу, яка безпосередньо перебувала за клавіатурою. Саме тут алгоритми обчислювальної лінгвістики (Natural Language Processing, NLP) виступають вирішальним фактором деанонімізації. Завдяки автоматизованому парсингу великих текстових масивів оперативний працівник отримує змогу здійснити перехресне порівняння тіньової та легальної активності фігуранта.

На практиці це виглядає як зіставлення масивів дописів із закритих хакерських форумів (Darknet) або повідомлень з анонімних Telegram-каналів із публічними коментарями, блоговими записами чи відкритим листуванням у соціальних мережах, попередньо зібраними в процесі OSINT-розвідки. На цьому етапі нейромережа перетворює «сирий» текст на багатовимірний математичний вектор, аналізуючи сотні прихованих параметрів: стійких, повторюваних послідовностей літер (біграми, триграми) або слів, які автор використовує рефлекторно та підсвідомо; специфіку побудови складних речень, частоту використання дієприслівникових зворотів чи вставних конструкцій; індивідуальні відхилення від мовної норми тощо. Це можуть бути систематичні специфічні друкарські помилки, нетипове використання пробілів перед розділовими знаками, використання авторських неологізмів, регіонального сленгу або характерного суржику, які неможливо контролювати свідомо впродовж тривалого часу.

Синергетичне об'єднання апаратного вектору (який беззаперечно доводить, який саме унікальний пристрій використовувався для виходу в мережу) та лінгвістичного вектору (який підтверджує, як саме ця особа несвідомо мислить, формулює думки та фізично вводить текст) дозволяє з максимальною вірогідністю зв'язати розрізнені анонімні акаунти з однією конкретною фізичною особою. Якщо ізольований апаратний відбиток зловмисник може пояснити в суді «випадковим використанням комп'ютера сторонньою особою», а стилометричну схожість текстів – «копіюванням його авторського стилю», то одночасний збіг обох векторів повністю руйнує подібну лінію захисту.

Такий синтез передових технологій формує не просто оперативну гіпотезу, а міцну, науково обґрунтовану орієнтувальну основу для подальшої легалізації здобутих даних у межах кримінального провадження. Отримані результати стають вагомим фактичним підґрунтям для складання ініціативних рапортів, клопотань до слідчого судді на проведення обшуків, вилучення електронних носіїв інформації та подальшого призначення комплексних комп'ютерно-технічних і судово-лінгвістичних (авторознавчих) експертиз. Саме висновки цих експертиз, проведені на базі зібраних оперативним шляхом цифрових слідів, набувають статусу належних та допустимих доказів у суді.

Для ефективної імплементації зазначених методів у практичну діяльність необхідна реалізація комплексу нормативно-правових, технічних та методичних заходів, які концептуально узгоджуються із завданнями Комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 роки [4]. Насамперед, у контексті визначеного Стратегічним планом пріоритетного переходу до проактивної моделі діяльності, керованої аналітикою (Intelligence-Led Policing), критично необхідним є прискорення прийняття законопроєкту «Про кримінальну розвідку» [5]. Цей нормативний акт має остаточно замінити морально застарілий Закон України «Про оперативно-розшукову діяльність», чітко регламентувати процедуру збору цифрових поведінкових даних та легалізувати використання алгоритмів штучного інтелекту без зайвої бюрократизації. Водночас, на виконання стратегічних завдань із

посилення технологічних та аналітичних спроможностей сектору безпеки, технічне забезпечення потребує впровадження у діяльність підрозділів кримінальної поліції та експертних установ вітчизняних програмно-апаратних комплексів автоматизованого стилометричного аналізу, адаптованих до специфіки українського мовного середовища (зокрема суржику та регіонального сленгу). Паралельно має формуватися методичне підґрунтя шляхом створення єдиного класифікатора цифрових поведінкових маркерів та розробки рекомендацій щодо фіксації апаратних відбитків під час негласних слідчих (розшукових) дій, що дозволить уніфікувати слідчу і судову практику відповідно до європейських стандартів кримінального аналізу.

Список використаних джерел:

1. Бакицький, Т.Д. Інструменти штучного інтелекту у сфері кібербезпеки. *Актуальні питання розвитку сектору безпеки і оборони (зарубіжний досвід)* : зб. тез доп. учасників XXVI Міжнар. наук.-практ. конф. іноземн. мовами для здобувачів освіти (м. Вінниця, 4 квіт. 2025 р.) / МВС України, Харків. нац. ун-т внут. справ, Каф. мов. підготов. Вінниця : ХНУВС, 2025. С. 307-308.

2. Behavioral Biometry as a Cyber Security Tool / M. Chyzhevska, N. Romanovska, A. Ramskyi, V. Venger, M. Obushnyi. *CEUR Workshop Proceedings*. 2022. Vol. 3188, Iss. 2 : CPITS-II-2021: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2021, Kyiv, Ukraine. P. 88–97.

3. Біометричні технології в XXI столітті та їх використання правоохоронними органами: посібник. 2-ге вид., доп. / В.П. Захаров, В.І. Рудешко. Львів: ЛьвДУВС, 2015. 492 с.

4. Про Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 роки : Указ Президента України від 11.05.2023 № 273/2023. URL: https://www.president.gov.ua/documents/2732023-46733 (дата звернення: 25.02.2026).

5. Нові підходи до безпеки: в НАВС обговорили законопроєкт «Про кримінальну розвідку». *НАВС: офіційний веб-портал*. URL: https://www.navs.edu.ua/news/novi-pidhodi-do-bezpeki-v-navs-obgovorili-zakonoproyekt-pro-kriminalnu-rozvidku.html (дата звернення: 25.02.2026).

Долинська М.С.
професор кафедри господарсько-правових дисциплін
навчально-наукового інституту
права та правоохоронної діяльності,
доктор юридичних наук, професор
(*Львівський державний університет внутрішніх справ*)

ДЕЯКІ АСПЕКТИ ВИКОРИСТАННЯ ІНСТРУМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ ПРИ ВИКЛАДАННІ НАВЧАЛЬНИХ ДИСЦИПЛІН У ЛЬВІВСЬКОМУ ДЕРЖАВНОМУ УНІВЕРСИТЕТІ ВНУТРІШНІХ СПРАВ

Набуття якісної юридичної вищої освіти, в тому числі у Львівському державному університеті внутрішніх справ, надає можливість у майбутньому отримати достойну професію та високооплачувану заробітну плату.

Органи поліції сучасної України потребують працівників, які б володіли широкими знаннями у правничій діяльності але й відповідали високим етичним та моральним людським якостям. Підготовка у закладах вищої освіти системи МВС України повинна дати не лише ґрунтовні знання та вміння, але й сформувати здатність випускників до саморозвитку, а також вміння адаптуватися до нових соціальних та інформаційних, технічних та технологічних вимог, та особливо до самоосвіти [1, с. 243].

В Україні і до сьогодні юридичні навчальні заклади зі специфічними умовами навчання здійснюють підготовку кадрів - правників різних видів юридичної діяльності, в тому числі для правоохоронних органів. Випускники вказаних закладів вищої працюють не лише в органах МВС, але й в судових та нотаріальних органах, прокуратурі, займаються адвокатською діяльністю [2, с. 33].

Загальновідомо, що інструменти штучного інтелекту активно застосовуються в закладах вищої освіти, в тому у Львівському державному університеті внутрішніх справ, як науково-педагогічними працівниками, так і особливо здобувачами вищої освіти.

Варто пригадати, що світовий досвід діджитилізації набув поширення і в Україні, цьому сприяло прийняття відповідного законодавства, зв тому числі Закону України «Про інформацію» від 02.10.1992 року [3].

Ми погоджуємося з науковцями, що цифрові технології використо-вуються з метою автоматизації та оптимізації, а також призводять до покращення різних процесів та сфер діяльності [4, с. 89], в тому числі в освіті, юридичній практиці, зокрема, судовій та нотаріальній.

Україна приєдналася до Рекомендацій Організації економічного співробітництва і розвитку з питань штучного інтелекту (Organisation for Economic Co-operation and Development, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449). Поширенню інструментів штучного інтелекту сприяло прийняття 2 грудня 2020 року розпорядження Кабінету Міністрів України № 1556-р, яким схвалено Концепцію розвитку штучного інтелекту в Україні [5]. Варто зауважити, що у тексті нормативно-правового акту не передбачено визначення поняття штучного інтелекту.

З точки зору теми дослідження вважаємо за доцільне виокремити розпорядження Кабінету Міністрів України № 320-р від 13 квітня 2024 р., яким схвалено Концепцію Державної цільової науково-технічної програми з використання технологій штучного інтелекту в пріоритетних галузях економіки на період до 2026 року [6]. У акті надано поняття штучного інтелекту, як «організованої сукупності інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань».

Наступним значущим актом щодо штучного інтелекту є розпорядженням Кабінету Міністрів України № 457-р від 9 травня 2025 р. [7], яким затверджено План заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025-2026 роки. Зокрема, у плані на Міністерство освіти і науки України,

Національну академію педагогічних наук та Міністерство цифрової трансформації України покладено обов'язок розробити методичні рекомендації щодо використання технологій штучного інтелекту у сфері вищої освіти.

Ми погоджуємося з науковцями, що майбутнє освіти нерозривно пов'язане з розвитком інформаційно-комунікаційних технологій та інтелектуальних машин. Перспективи штучного інтелекту відкривають нові можливості у викладанні та навчанні у ЗВО з потужним потенціалом для зміни навіть самої системи управління ЗВО. За даними індустрії електронного навчання впродовж найближчих трьох років інструменти управління навчанням будуть оснащені можливостями штучного інтелекту [8, с. 171, 172].

Автором дослідження проведено опитування у листопаді-грудні 2025 року, які серед іншого стосувалися питань застосування штучного інтелекту в сфері освіти. У опитуванні взяли участь 82 респонденти-здобувачі вищої освіти Львівського державного університету внутрішніх справ.

Респондентів було запевнено щодо дотримання етичних норм при проведенні анкетування (American Sociological Association's, 1997) [9, с 25].

На запитання, що найбільше мотивує осіб, використовувати ШІ 43,9 % (36) опитаних респондентів стверджують що цьому сприяла недостатність часу на опрацювання матеріалу, а 28% (23 особи) вважають, що таким мотивом є брак інформації по обраній тематиці. Лише 9,8 % (8) опитаних респондентів стверджують що використанню ШІ сприяє відсутність у особи бажання до самостійної праці над виконанням поставленого завдання.

Переважна більшість респондентів - 58,5% (48) на запитання, які можуть бути рекомендації щодо використання ШІ здобувачами вищої освіти? - вказала використати як спрямування у напрямку дослідження. 17% (14) вважають, що інструменти ШІ варто застосовувати при недостатності часу на опрацювання матеріалу. На противагу - 14,% (12) вважають, що варто застосовувати ШІ при відсутності бажання до самостійної праці над виконанням завдання.

На запитання щодо категорій викладачів, які більше використовують ШІ при викладанні навчальних дисциплін,

більшість респондентів - 65,9% (54) вважають, що такими є педагоги віку 30-40 років, не залежно від статі. 6,1% - (5) респондентів вважають, що такими є педагоги віку 45-60 років, не залежно від статі. Перевагу чоловікам педагогам надають 3,7% (3), та жінкам – 2,4% (2).

Як позитивне слід відзначити, що 89% (73) здобувачів вищої освіти стверджують, що лише за потреби використовують ШІ при підготовці до практичних та семінарських занять. Ні одна особа з респондентів не заявила про те, що вона не користується інструментами ШІ при підготовці до занять. 2 респонденти (2,4%) стверджують, що користуються ШІ при підготовці до кожного заняття, такаж кількість респондентів використовує ШІ - при приготуванні до другого та третього заняття.

Праці науковців, опитування здобувачів вищої освіти ЛьвДУВС, свідчать, що застосування інструментів ШІ в науці є незаперечною дійсністю [10, с. 40].

Як правильно зауважує Корнєєва С.Р. багато технологій штучного інтелекту засновані на тому, що задіюють великі масиви даних, в які входить також і особиста інформація, та найбільш конфіденційна. Технології штучного інтелекту можуть використовуватися для збору і аналізу величезної кількості особистої інформації для різних цілей [11, с. 394].

Має рацію О. Кармаза, що норми права в частині використання штучного інтелекту повинні відповідати принципу юридичної визначеності та принципу верховенства права, закріпленим в Конституції України [12, с. 17].

Таким чином, здобувачі вищої освіти навчального закладу та науково-педагогічні працівники ЛьвДУВС при потребі - у своїй науковій та практичній діяльності користуються інструментами ШІ. При цьому вони повинні дотримуватися принципів доброчесності та конфіденційності.

Список використаних джерел:

1. Романюк В. В. Вплив специфічних умов навчання у ВНЗ МВС України на здійснення підготовки поліцейських. *Підготовка охоронців правопорядку в Харкові (1917–2017 рр.)* : зб. наук. ст. і тез доп. на наук.-практ. конф. до 100-річчя підготовки охоронців правопорядку в Харкові (м. Харків, 25 листоп. 2017 р.) /

МВС України, Харків. нац. ун-т внутр. справ. Харків, 2017. URL: siy96og6OUhRIBmn4NV5iH2M93hWdMgW.pdf.

2. Долинська М. С. Проблеми юридичної освіти у закладах вищої освіти зі специфічними умовами навчання. *Право і суспільство*. 2020. № 2. Ч. 1. С.32-37.

3. Про інформацію: Закон України від 02.10. 1992 року № 2657-XII. *Відомості Верховної Ради України (ВВР),* 1992, № 48, ст.650.

4. Долинська М. До питання впровадження в Україні засадничих принципів системи е-нотаріату. *Науковий вісник ЛьвДУВС. Серія юридична.* 2023. № 4. С. 89-98. DOI https://doi.org/10.32782/2311-8040/2023-4-11.

5. Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядження Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text

6. Про схвалення Концепції Державної цільової науково-технічної програми з використання технологій штучного інтелекту в пріоритетних галузях економіки на період до 2026 року: Розпорядження Кабінету Міністрів України 13 квітня 2024 р. № 320-р. URL: https://zakon.rada.gov.ua/laws/show/320-2024-%D1%80#Text

7. Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025-2026 роки: Розпорядження Кабінету Міністрів України 9 травня 2025 р. № 457-р. URL: https://zakon.rada.gov.ua/laws/show/457-2025-%D1%80#Text

8. Гуревич Р. С., Коношевський Л. Л., Коношевський О. Л., Воєвода А. Л., Люльчак С. Ю. Інтеграція штучного інтелекту в сферу освіти: проблеми, виклики, загрози, перспективи. Сучасні інформаційні технології та інноваційні методики навчання в підготовці фахівців: методологія, теорія, досвід, проблеми. 2024.. Випуск 72. С. 171-186.

9. Dolynska, M. (2025). Notarial registration of inheritance of real estate in independent Ukraine: Socio-legal dimension. *Social and Legal Studios*, 8(3), 23-33. https://doi.org/10.32518/sals3.2025.23

10. Долинська Марія. Окремі питання застосування штучного інтелекту при викладанні навчальної дисципліни

«Нотаріальний процес» у закладах вищої освіти зі специфічними умовами навчання. AI-асистент на базі ChatGPT: практичний кейс: матеріали всеукраїнського науково-педагогічного підвищення кваліфікації, 1 грудня – 11 січня 2026 року. – Львів – Торунь : Liha-Pres, 2026. С. 36-40.

11. Корнєєва С.Р. Вплив застосування технологій штучного інтелекту на реалізацію та захист прав людини. Електронне наукове видання «Аналітично-порівняльне правознавство 2021. № 4 (71). С. 392-394.

12. Кармаза Олександра. Використання видів (форм) штучного інтелекту в нотаріальному процесі України: проблеми та шляхи вирішення. *Підприємництва, господарство і право*. 2021.№ 3. С.13-18.

Єсімов С.С.,
професор кафедри адміністративно-правових дисциплін
навчально-наукового інституту права
та правоохоронної діяльності,
кандидат юридичних наук, професор
(*Львівський державний університет внутрішніх справ*)

ШТУЧНИЙ ІНТЕЛЕКТ І СИСТЕМА ШТУЧНОГО ІНТЕЛЕКТУ У КОНТЕКСТІ ІНФОРМАЦІЙНОГО ПРАВА

Нині немає єдиного розуміння термінів «штучний інтелект» і «система штучного інтелекту». Це з різними чинниками, зокрема з різними підходами до застосування правил логіки та юридичної техніки. Під «інтелектуальною системою», слід розуміти сукупність даних та інших відомостей, інформаційних технологій та технічних засобів, що включають апаратно-технічний комплекс, що забезпечують проведення за участю людини обробки та аналізу інформації та прийняття рішень на основі отриманих висновків з використанням, у тому числі, методів машинного навчання та спрямованих на виконання цілей функціонування.

Зазначена категорія включає автономні технічні засоби, комплекс системи розпізнавання осіб, радників та інші системи, включаючи систему штучного інтелекту. Остання буде інтелектуальною системою найвищого рівня як найбільш самостійна.

Під системою штучного інтелекту доцільно розуміти автономну, засновану на методах машинного навчання, технологічну систему, створювану для функціонування однієї або декількох інтелектуальних систем, доступ до якої здійснюється з використанням засобів обчислювальної техніки. Дані у системі штучного інтелекту поділяються на вхідні та вихідні. На основі вхідних даних програмне забезпечення, що входить до системи, навчається; їх воно використовує для подальшого аналізу.

Вихідні дані – результат інтелектуальної діяльності системи, ухвалене нею рішення. Інтелектуальні системи є різновидом інформаційних систем, щодо яких можна виділити суттєві ознаки:

автоматизоване ухвалення рішень на основі інформаційних систем технологій; обов'язкова участь людини при проведенні обробки s аналізу інформації; використання спеціального апаратно-технічного комплексу, який би аналіз інформації з урахуванням методів машинного навчання; сукупність ризиків і загроз, які мають бути враховані розробниками, операторами, користувачами і іншими суб'єктами інтелектуальних систем.

Унікальність правового режиму інтелектуальних систем як різновиду інформаційних систем обумовлена наявністю сукупності унікальних суб'єктивних прав і обов'язків суб'єктів інтелектуальних систем, спеціальних технічних і програмно-апаратних засобів, обумовлених функціональним призначенням системи, системи ризиків і загроз, які повинні встановлюватися законодавчо та враховуватися суб'єктами.

Оскільки система штучного інтелекту здатна отримувати, обробляти і аналізувати інформацію різних типів і видів і приймати самостійні рішення на основі попереднього досвіду або аналізу даних з будь-якого питання і в будь-якій галузі діяльності, на підставі прийому юридичної фікції, систему штучного інтелекту можна розглядати у визначених законом цілях як електронну особу, що має правосуб'єктність, за умови, що йдеться про визнаний правом суб'єкт, який не має природної реальності, спеціально створеної юридичної конструкції, що дозволяє визнати юридично значущий характер дій, що здійснюються такою системою, і нести за них юридичну відповідальність без вини.

Електронну особу в цьому випадку можна розглядати як новий вид суб'єкта інформаційного права, відмінний від фізичних і юридичних осіб. Категорія відповідальності до електронних осіб застосовна лише обмежено – як об'єктивна відповідальність, оскільки система штучного інтелекту може бути «винна» у сучасному значенні терміна, тому до неї застосовні лише форми відповідальності без вини.

За підсумками аналізу складових елементів правосуб'єктності сформульовані її особливості нового виду суб'єкта права – система штучного інтелекту. Правоздатність системи штучного інтелекту може виникати з моменту проходження повноцінного терміну повністю скомпільованою

програмою в оцінці результатів її здібностей до аналізу даних і побудови висновків на їх основі.

Дієздатність системи штучного інтелекту має бути безпосередньо пов'язана з теорією прийняття рішень, адже тільки так можна оцінити рівень її доцільності. Що стосується деліктоздатності, якщо застосовувати до системи штучного інтелекту поняття «відповідальності», то від класичного розуміння, розглянувши можливість використання термінів або «позитивної відповідальності», або «об'єктивної відповідальності», або інших нових підходів до даної правової категорії.

.В окремих міжнародних організаціях і країнах Європейського Союзу приймаються рамкові, декларативні та стратегічні документи, що позначають загальні підходи та цілі, але які в більшості випадків не містять конкретних механізмів правового регулювання.

Наприклад, Artificial Intelligence Act у зазначеному документі окремо виділяється обов'язок країн-членів Європейського Союзу визначити профільні органи влади, відповідальні за розвиток та застосування ШІ, вибудовувати механізми підзвітності дій штучного інтелекту (ШІ), формувати ризик-орієнтований підхід до зазначеної технології (особливо відзначається високо ризиковий характер технології при її застосуванні у сфері публічного управління) [1].

Можна виділити кілька основних підходів до регулювання питань, пов'язаних із системами штучного інтелекту:

- концептуальний (міжнародні організації та держави приймається документ (Концепцію розвитку штучного інтелекту в Україні [2]), що не містить правових норм у чистому вигляді, декларує напрями розвитку, закладає фінансове забезпечення проектів зі створення та впровадження технологій штучного інтелекту);

- етичний (міжнародна організація чи держава приймають документи, що містять етичні принципи створення, розвитку та впровадження систем штучного інтелекту у життя суспільства);

- умовно регулюючий (регулювання щодо окремих технологій чи сфер їх застосування) зараз розвивається лише технічне регулювання.

Нині принципи правового регулювання технологій штучного інтелекту розрізнені, є швидше етичними, ніж повноцінно правовими і є повною мірою обґрунтованими і достатніми.

Список використаних джерел:

1. The EU Artificial Intelligence Act. Up-to-date developments and analyses of the EU AI Act. URL. https://artificialintelligenceact.eu/

2. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України від 02.12.2020 р. № 1556-р. URL. https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text

Жук С.М.
доцент кафедри загальновійськових дисциплін,
кандидат військових наук
(Національна академія Державної прикордонної служби України імені Богдана Хмельницького)
Білявець Ю.С.
командир відділення навчальної групи
(Національна академія Державної прикордонної служби України імені Богдана Хмельницького)

МОЖЛИВОСТІ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ЗАБЕЗПЕЧЕННІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ОБОРОНИ

У сучасних умовах забезпечення національної безпеки та оборони держави дедалі більше пов'язується з використанням новітніх інформаційних технологій. Одним із найбільш перспективних напрямів їх розвитку є застосування систем штучного інтелекту. Зростання обсягів інформації, ускладнення безпекового середовища та висока динаміка сучасних загроз зумовлюють необхідність використання інструментів, здатних швидко аналізувати великі масиви даних і підтримувати процес прийняття управлінських рішень.

Однією з ключових сфер використання штучного інтелекту є обробка та аналіз інформації. У процесі забезпечення національної безпеки різні органи державної влади отримують значну кількість даних із різноманітних джерел: технічних засобів спостереження, розвідувальних систем, інформаційно-комунікаційних мереж, відкритих джерел інформації.

Окрему роль штучний інтелект відіграє у сфері розвідки та спостереження. Сучасні технічні засоби забезпечують отримання великого обсягу даних, зокрема відео та фотоматеріалів, радіолокаційної інформації та інших видів розвідувальних відомостей. Використання алгоритмів автоматичного аналізу зображень дає змогу швидше виявляти об'єкти, визначати їх характеристики та оцінювати зміни обстановки. Це сприяє більш

оперативному отриманню розвідувальної інформації та підвищує ефективність використання наявних технічних засобів.

Не менш важливим є застосування штучного інтелекту у сфері кібербезпеки. Сучасні інформаційні системи постійно зазнають впливу різноманітних кіберзагроз, що можуть бути спрямовані на порушення роботи державних органів, об'єктів критичної інфраструктури та систем управління. Алгоритми аналізу поведінки мережевого трафіку дозволяють виявляти підозрілі дії користувачів або програмного забезпечення, своєчасно реагувати на спроби несанкціонованого доступу та запобігати поширенню шкідливого програмного забезпечення. Таким чином, використання технологій штучного інтелекту сприяє підвищенню рівня захисту інформаційних ресурсів держави.

Перспективним напрямом також є використання автономних та напівавтономних технічних систем. До них належать безпілотні літальні апарати, роботизовані комплекси та інші технічні засоби, здатні виконувати певні завдання без безпосередньої участі людини. Застосування таких систем дозволяє зменшити ризики для особового складу під час виконання небезпечних завдань, а також підвищити ефективність розвідувальних і спостережних заходів.

Разом із тим широке впровадження технологій штучного інтелекту потребує врахування низки організаційних та технічних аспектів. Передусім це стосується забезпечення надійності програмних алгоритмів, захисту інформації та створення відповідної нормативної бази для використання таких технологій. Важливим чинником є також підготовка фахівців, які мають володіти необхідними знаннями у сфері інформаційних технологій та вміти ефективно застосовувати сучасні цифрові інструменти у практичній діяльності.

Отже, використання технологій штучного інтелекту відкриває нові можливості для підвищення ефективності системи національної безпеки та оборони. У перспективі подальший розвиток і впровадження таких технологій може стати одним із важливих чинників зміцнення обороноздатності держави та підвищення її здатності протидіяти сучасним викликам і загрозам.

Жук С.М.
доцент кафедри загальновійськових дисциплін,
кандидат військових наук
(Національна академія Державної прикордонної служби України імені Богдана Хмельницького)
Павлось К.В.
командир навчальної групи
(Національна академія Державної прикордонної служби України імені Богдана Хмельницького)

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В СУЧАСНИХ ВОЄННИХ КОНФЛІКТАХ: ПЕРСПЕКТИВИ ТА ВИКЛИКИ

Під час сучасних бойових дій командири та органи військового управління отримують дані з різноманітних джерел – розвідувальних засобів, безпілотних літальних апаратів, супутникових систем спостереження, засобів радіоелектронної розвідки та інших інформаційних ресурсів. У результаті формується великий масив інформації, який потребує швидкого опрацювання та оцінювання. Застосування сучасних програмно-аналітичних систем дозволяє значною мірою прискорити цей процес і підвищити якість прийнятих управлінських рішень. Традиційні методи аналізу інформації часто не дозволяють оперативно опрацьовувати такі обсяги даних. Використання інтелектуальних алгоритмів дає змогу автоматизувати значну частину аналітичної роботи, швидше виявляти закономірності у зміні обстановки та формувати обґрунтовані варіанти рішень.

Важливою сферою застосування штучного інтелекту є розвиток безпілотних і роботизованих систем. Безпілотні літальні апарати, наземні роботизовані комплекси та морські безекіпажні платформи дедалі частіше використовуються для виконання розвідувальних, спостережних та ударних завдань. Їх використання дозволяє зменшити ризики для особового складу та підвищити точність ураження цілей. Крім того, сучасні алгоритми машинного навчання сприяють підвищенню рівня автономності

таких систем, що дає можливість ефективніше застосовувати їх у складних умовах бойової обстановки.

Складні інформаційні системи можуть бути об'єктом кібератак, спрямованих на порушення їх функціонування або отримання доступу до конфіденційної інформації. У разі успішного втручання противник може отримати суттєві переваги на полі бою, що підвищує значення кіберзахисту військових інформаційних систем.

Іншим важливим викликом є етичні та правові аспекти використання автономних бойових систем. Питання відповідальності за застосування таких технологій, контроль за прийняттям рішень щодо ураження цілей та дотримання норм міжнародного гуманітарного права залишаються предметом активних дискусій у науковому та політичному середовищі. У зв'язку з цим необхідним є формування чітких правил і механізмів контролю за використанням систем штучного інтелекту у військовій діяльності.

Для ефективного впровадження сучасних технологій необхідна ретельна підготовка військових фахівців. Робота з новими інформаційними системами вимагає від особового складу високого рівня технічних знань, уміння обробляти великі обсяги інформації та швидко пристосовуватися до змін у технологічному середовищі. Тому одним із пріоритетів розвитку військової освіти є підготовка спеціалістів, здатних ефективно працювати з сучасними інформаційними та аналітичними системами.

Застосування сучасних технологій поступово стає важливим фактором розвитку воєнної справи. Вони відкривають нові можливості для підвищення ефективності розвідки, удосконалення систем управління військами та розвитку роботизованих бойових засобів. Водночас їх використання пов'язане з низкою технологічних, організаційних та правових викликів, які потребують комплексного вирішення. Подальший розвиток і впровадження технологій штучного інтелекту значною мірою визначатиме характер майбутніх воєнних конфліктів та вимагатиме адаптації підходів до забезпечення національної безпеки і оборони.

Жук С.М.
доцент кафедри загальновійськових дисциплін,
кандидат військових наук
(Національна академія Державної прикордонної служби України імені Богдана Хмельницького)
Сорока М.А.
курсант
(Національна академія Державної прикордонної служби України імені Богдана Хмельницького)

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ФАКТОР ЗМІНИ ХАРАКТЕРУ СУЧАСНОЇ ВІЙНИ

Актуальність теми дослідження зумовлена стрімким розвитком інформаційних технологій та їхнім активним впровадженням у військову сферу. Сучасні воєнні конфлікти характеризуються високою технологічністю, швидкістю змін оперативної обстановки та широким використанням цифрових систем управління. У цих умовах особливого значення набувають технології штучного інтелекту, які суттєво впливають на способи ведення бойових дій, організацію управління військами та застосування сучасного озброєння. Штучний інтелект поступово стає одним із ключових факторів трансформації характеру війни, змінюючи підходи до планування, організації та ведення воєнних операцій.

Метою дослідження є аналіз ролі технологій штучного інтелекту у трансформації характеру сучасної війни, а також визначення основних напрямів їх впливу на систему військового управління, розвідку та бойове застосування сил і засобів.

Сучасна війна характеризується значною інформатизацією та використанням складних технологічних систем. Обсяг інформації, що надходить до органів військового управління, постійно зростає, що ускладнює процес її обробки та аналізу. У таких умовах застосування штучного інтелекту дозволяє значно підвищити ефективність інформаційно-аналітичної діяльності. Інтелектуальні алгоритми здатні обробляти великі масиви даних,

виявляти закономірності та формувати прогнози щодо розвитку бойової обстановки.

Одним із помітних проявів впливу штучного інтелекту на сучасну війну є активне використання безпілотних і роботизованих систем. Безпілотні літальні апарати, наземні роботизовані комплекси та морські безекіпажні платформи дедалі ширше залучаються до виконання розвідувальних завдань, ведення спостереження, коригування вогню та ураження цілей противника. Їх застосування дає змогу підвищити ефективність бойових дій і водночас зменшити ризики для особового складу.

Важливим напрямом впливу штучного інтелекту є також зміни у процесі прийняття управлінських рішень. У традиційній системі військового управління значна частина часу відводилася на збирання, оброблення та аналіз інформації. Використання сучасних інформаційно-аналітичних систем і програм підтримки прийняття рішень дозволяє значно прискорити ці процеси та оперативніше реагувати на зміну обстановки.

Таким чином, технології штучного інтелекту поступово стають важливим чинником розвитку сучасного воєнного мистецтва. Їх застосування сприяє підвищенню результативності розвідки, удосконаленню систем управління військами, розвитку автономних бойових засобів і посиленню кіберзахисту. Очікується, що подальший розвиток цих технологій істотно впливатиме на характер майбутніх воєнних конфліктів та формування нових підходів до забезпечення національної безпеки і оборони.

Захаренко-Мившук О.М.
здобувачка ступеня магістра
інституту заочного та дистанційного навчання
(Національна академія внутрішніх справ)

АЛГОРИТМІЧНІ РІШЕННЯ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ: ПРАВОВІ ОБМЕЖЕННЯ ТА ПСИХОЛОГІЧНІ РИЗИКИ

Актуальність проблеми. Цифрова трансформація правоохоронної діяльності є закономірним етапом розвитку сучасної правової системи. Використання алгоритмічних інструментів для аналізу великих масивів даних, обробки цифрових доказів, оцінки ризиків повторного правопорушення та прогнозування криміногенних тенденцій поступово інтегрується у практику кримінального провадження. Водночас впровадження таких технологій актуалізує необхідність комплексного осмислення їх правових меж і психологічних наслідків.

Особливого значення набуває питання впливу алгоритмічних рекомендацій на процес формування внутрішнього переконання суб'єкта правозастосування. Якщо раніше джерелом оцінки доказів виступали переважно матеріали справи та професійний досвід судді або слідчого, то нині до цього процесу долучається аналітична система, результати якої можуть суттєво впливати на кінцеве рішення.

Мета дослідження полягає у визначенні психологічних та правових ризиків використання алгоритмічних рішень у кримінальному провадженні та окресленні напрямів їх мінімізації.

Правовий вимір застосування алгоритмічних систем.

У кримінальному провадженні алгоритмічні інструменти можуть виконувати допоміжні функції: систематизацію доказової інформації, виявлення статистичних закономірностей, аналіз цифрових слідів, формування рекомендацій щодо оцінки ризиків. Їх використання потенційно сприяє підвищенню оперативності та точності обробки інформації.

Однак правова природа таких рішень залишається дискусійною. Алгоритм не є суб'єктом права та не може нести відповідальність за прийняте рішення. Відтак остаточне

процесуальне рішення повинно залишатися результатом свідомої діяльності людини, яка здійснює оцінку доказів відповідно до принципів кримінального провадження.

Серед ключових правових викликів можна виокремити:

– проблему прозорості алгоритмічних моделей;

– складність перевірки коректності отриманих результатів;

– ризик формалізації індивідуалізації підходу до особи;

– ускладнення процесуального оскарження алгоритмічних рекомендацій.

Таким чином, застосування штучного інтелекту потребує нормативного визначення його допоміжного статусу та гарантій людського контролю.

Психологічні ризики алгоритмізації правозастосування.

Поряд із правовими аспектами важливим є аналіз психологічних механізмів сприйняття автоматизованих рішень. Алгоритмічні системи часто позиціонуються як більш об'єктивні та неупереджені порівняно з людським судженням. Така установка може формувати у суб'єкта правозастосування зниження рівня критичності.

Одним із релевантних феноменів є **automation bias** — схильність довіряти рекомендаціям автоматизованої системи навіть у випадках, коли вони потребують додаткової перевірки. У контексті кримінального провадження це може проявлятися у некритичному сприйнятті результатів оцінки ризику або аналітичних висновків системи.

Крім того, спостерігається ефект технологічного авторитету, за якого рішення, сформоване алгоритмом, сприймається як більш точне через його «машинну» природу. Такий ефект може впливати на процес формування внутрішнього переконання судді або слідчого, змінюючи структуру когнітивної оцінки доказів.

Не менш важливою є проблема зміщення відповідальності. Психологічно суб'єкт може сприймати алгоритмічну рекомендацію як зовнішній фактор, що частково зменшує відчуття персональної відповідальності за остаточне рішення. У довгостроковій перспективі це може трансформувати професійну роль правозастосувача.

Взаємозв'язок правових і психологічних чинників.

Правові гарантії справедливого судочинства значною мірою ґрунтуються на особистій оцінці доказів, здійсненій людиною. Якщо алгоритмічна рекомендація починає відігравати визначальну роль у процесі прийняття рішення, виникає ризик зміщення балансу між технологічною ефективністю та індивідуалізованим підходом.

Водночас повна відмова від використання цифрових інструментів є недоцільною, оскільки вони здатні підвищувати якість аналітичної роботи. Отже, ключовим завданням є забезпечення їх інтеграції у кримінальне провадження як допоміжного інструменту за умови збереження автономності людського судження.

У цьому контексті особливої ваги набуває психологічна підготовка працівників правоохоронних органів до роботи з алгоритмічними системами. Формування навичок критичного мислення, усвідомлення когнітивних викривлень та збереження відповідальності за прийняте рішення є необхідною умовою безпечної цифровізації правозастосування.

Висновки

1. Алгоритмічні системи у кримінальному провадженні мають значний потенціал для оптимізації аналітичних процесів.

2. Основні ризики їх використання пов'язані не лише з технічними обмеженнями, а й з психологічними механізмами сприйняття автоматизованих рішень.

3. Забезпечення правових гарантій справедливого судочинства в умовах цифровізації потребує:
– нормативного визначення меж застосування алгоритмічних систем;
– забезпечення прозорості та можливості перевірки результатів;
– збереження обов'язкового людського контролю;
– впровадження елементів психологічної підготовки до програм професійного навчання.

Отже, ефективна інтеграція штучного інтелекту у кримінальне провадження можлива лише за умови поєднання технологічних можливостей із правовими гарантіями та психологічною усвідомленістю суб'єктів правозастосування.

Список використаних джерел:

1. Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI (зі змінами).

2. Regulation (EU) 2024/1689 (AI Act).

3. Ethics Guidelines for Trustworthy AI. European Commission, 2019.

4. Parasuraman R., Riley V. Humans and Automation: Use, Misuse, Disuse, Abuse. Human Factors. 1997.

5. Dressel J., Farid H. The accuracy, fairness, and limits of predicting recidivism. Science Advances. 2018.

6. Citron D. Technological Due Process. Washington University Law Review. 2008.

7. Коваленко Є.В. Штучний інтелект у кримінальному судочинстві. 2022.

8. Шевченко О.О. Психологічні особливості прийняття рішень у правоохоронній діяльності. Вісник НАВС. 2021.

Здреник І.В.
доцент кафедри
загальноправових дисциплін факультету № 1,
кандидат юридичних наук, доцент
(Львівський держаний університет внутрішніх справ)

ШТУЧНИЙ ІНТЕЛЕКТ ПРИ ДОКАЗУВАННІ

Штучний інтелект (далі – ШІ) доцільно розглядати як сукупність технологічних рішень, що надають комп'ютерним системам можливість імітувати інтелектуальну діяльність людини, зокрема її когнітивні процеси. ШІ виступає як міждисциплінарний напрям, який об'єднує низку окремих галузей, кожна з яких зосереджується на специфічних вимірах функціонування інтелектуальних систем. ШІ створюється таким чином, щоб забезпечити здатність системи сприймати середовище, здійснювати обробку та інтерпретацію отриманих даних, а також приймати рішення для досягнення визначених цілей. Реалізація цих функцій ґрунтується на застосуванні складних алгоритмів і статистичних моделей, що дають змогу аналізувати значні масиви структурованої й неструктурованої інформації.

Перспективи використання ШІ у сфері правосуддя пов'язані з його здатністю обробляти великі обсяги фактичних і правових даних, нормативно-правових актів та матеріалів конкретних справ. Інтеграція інструментів машинного навчання відкриває можливості не лише для швидкого опрацювання інформації, а й для забезпечення більшої послідовності та об'єктивності при оцінюванні доказів. Застосування інтелектуальних технологій у діяльності судів сприяє оптимізації управління даними, підвищенню якості аналітичної підтримки та розвитку прогнозних механізмів, за умови обов'язкового дотримання етичних стандартів, гарантій прав людини, принципів рівності, інформаційної безпеки, прозорості та належного контролю з боку користувачів [1, с. 54].

В Україні практика судового розгляду питань, пов'язаних із використанням матеріалів, сформованих за допомогою технологій штучного інтелекту, лише починає складатися. Брак спеціалізованих нормативно-правових приписів у цій сфері

ускладнює формування єдиної позиції судів щодо можливості їх застосування в межах доказового процесу.

Станом на сьогодні відомі лише поодинокі випадки включення подібних матеріалів до матеріалів справи, причому їх використання має переважно допоміжний або апробаційний характер. Здебільшого йдеться про подання учасниками процесу аналітичних довідок, підготовлених із застосуванням мовних моделей на кшталт ChatGPT. Водночас суди, як правило, не надають таким документам статусу належних доказів, посилаючись на відсутність визначеного джерела походження інформації, суб'єкта, відповідального за її достовірність, а також неможливість перевірити механізм формування відповідного змісту.

Наразі на рівні Верховного Суду відсутня чітко сформульована правова позиція щодо прийнятності матеріалів, створених із застосуванням ШІ. Водночас у низці судових актів опосередковано наголошується, що доказове значення можуть мати лише ті відомості, які характеризуються встановленим походженням, створені відповідно до законодавчих вимог і піддаються перевірці на достовірність [2, с. 461-462]. Отже, матеріали, сформовані системами, що не наділені правосуб'єктністю та не забезпечують достатнього рівня алгоритмічної прозорості, наразі не узгоджуються з базовими критеріями допустимості доказів.

Початкові орієнтири вітчизняної судової практики щодо застосування технологій ШІ пов'язані насамперед із питанням недопустимості їх використання як інструменту для перегляду чи оскарження вже ухвалених судових рішень. Зокрема, ухвалою Верховний Суд від 08.02.2024 р. у справі № 925/200/22 було кваліфіковано як зловживання процесуальними правами звернення представника позивача до відомостей, сформованих за допомогою ChatGPT, з метою тлумачення постанови суду касаційної інстанції. У зазначеному рішенні суд акцентував, що використання інструментів ШІ не може підривати обов'язковість і авторитет судових висновків. Протиставлення правової позиції суду результатам, отриманим із застосуванням технології, яка не має нормативного врегулювання та належного наукового обґрунтування, визнано неприйнятним і таким, що потенційно

здатне негативно вплинути на довіру до судової влади. Водночас в окремій думці у цій справі було висловлено альтернативний підхід: саме по собі посилання на матеріали, згенеровані за допомогою ШІ, за відсутності інших ознак недобросовісної процесуальної поведінки, не повинно автоматично розцінюватися як зловживання процесуальними правами [3].

Проблемними питаннями використання ШІ при доказуванні є насамперед складність визначення правового статусу контенту, автономно згенерованого ШІ або відредагованого людиною за допомогою інтелектуальних інструментів, що потребує чіткого розмежування між експертними аналітичними системами та генеративними моделями. Суттєвою проблемою у правовому регулюванні залишається відсутність усталеного та вичерпного визначення категорії «штучний інтелект». У 2020 р. Кабінет Міністрів України затвердив Концепцію розвитку штучного інтелекту в Україні, в якій ШІ трактується як упорядкований комплекс інформаційних технологій, що дає змогу розв'язувати складні багаторівневі завдання шляхом застосування наукових методів і алгоритмів обробки даних, отриманих або сформованих у процесі функціонування системи. У документі також наголошується на здатності таких систем формувати та використовувати власні бази знань, моделі прийняття рішень, алгоритмічні механізми роботи з інформацією та самостійно визначати шляхи досягнення поставлених цілей [4]. Водночас запропоноване нормативне формулювання не охоплює повною мірою змістовні характеристики штучного інтелекту, зокрема його адаптивність, здатність до самонавчання та потенціал автономного функціонування, що ускладнює належне розуміння його правової природи й меж застосування.

На нормативному рівні досі не окреслено роль, функціональне призначення та коло завдань штучного інтелекту, що в перспективі здатне зумовити як теоретичні суперечності, так і прикладні труднощі у правозастосовній діяльності. Додатковим стримувальним фактором виступає недостатній рівень цифрової компетентності населення, зокрема представників юридичної професії, у питаннях використання інструментів ШІ. Причинами такої ситуації можна вважати відсутність спеціалізованих освітніх програм, спрямованих на формування практичних навичок

застосування технологій штучного інтелекту в юридичній діяльності, обмежену зацікавленість державних інституцій у розвитку відповідного напряму, а також дефіцит фінансових ресурсів. Водночас існують припущення, що делегування окремих юридичних функцій інтелектуальним системам може призвести до зменшення попиту на правничі послуги та вплинути на формування їх вартості на ринку [5, с. 33].

Таким чином, впровадження штучного інтелекту в систему доказування відкриває шлях до автоматизації аналізу колосальних масивів юридичної інформації та підвищення об'єктивності судового процесу, проте на поточному етапі вітчизняна юриспруденція демонструє стриманий консерватизм. Головною перепоною є невідповідність згенерованих ШІ матеріалів класичним критеріям допустимості через відсутність правосуб'єктності алгоритмів, невизначеність джерел походження даних та неможливість верифікації внутрішньої логіки системи. Поодинокі спроби використання мовних моделей у судах наразі сприймаються як допоміжні інструменти без доказової сили, а в окремих випадках – навіть як зловживання процесуальними правами, що ставить під загрозу авторитет судових рішень. Подальша інтеграція технологій потребує не лише нормативного закріплення статусу ШІ та подолання «алгоритмічної непрозорості», а й глибокої цифрової трансформації юридичної спільноти для забезпечення балансу між інноваційною ефективністю та непорушністю прав людини.

Список використаних джерел:

1. Лотиш Т. В. Застосування штучного інтелекту при мотивуванні судових рішень у кримінальному процесі: міжнародний досвід та перспективи для України. *Journal «ScienceRise: Juridical Science»,* 2024. № 1 (27). С. 52-57.

2. Деркач В.Г., Прокопович-Ткаченко Є.Д. та Руденко Є.Г. Використання штучного інтелекту в судовому процесі України: правові, етичні та процесуальні аспекти. *Юридичний науковий електронний журнал,* 2025. № 3. С. 460-464.

3. Ухвала від 08.02.2024 № 925/200/22 Верховний Суд. Касаційний господарський суд. Електронний ресурс. URL: https://verdictum.ligazakon.net/document/116984639?utm%20_source

=jurliga.ligazakon.net&utm_medium=news&utm_content=jl01 (дата звернення: 26.02.2026)

4. Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядження КМУ від 02.12.2020 р. № 1556-р. URL: https:// zakon.rada.gov.ua/laws/show/1556-2020-р#Text (дата звернення: 26.02.2026)

5. Гришко В.І., Вознюк С.С. Проблемні аспекти впровадження штучного інтелекту у сфері юриспруденції. *Електронне наукове видання «Аналітично-порівняльне правознавство»,* 2024. № 2. С. 29-34.

Зеленська А.В.
здобувач ступеня бакалавра
(Національна академія внутрішніх справ)
Христюк О.С.
старший викладач кафедри психології
навчально-наукового інституту права та психології
(Національна академія внутрішніх справ)

ШТУЧНИЙ ІНТЕЛЕКТ В ОСВІТІ: ПСИХОЛОГІЧНІ РИЗИКИ ТА РЕСУРСИ ДЛЯ РОЗВИТКУ ОСОБИСТОСТІ

Штучний інтелект (ШІ) сьогодні є не футуристичним прогнозом, а щоденною реальністю, що трансформує всі сфери життєдіяльності, зокрема освіту. В умовах стрімкої технологізації ключовим питанням стає характер впливу ШІ на когнітивний розвиток, емоційний інтелект та самоідентифікацію особистості. Ризики зниження автономності мислення та трансформації мотивації потребують глибокого осмислення психологічного інструментарію ШІ для забезпечення ефективного й безпечного розвитку суб'єктів навчання.

Проблематика інтеграції ШІ в освітній простір перебуває у фокусі уваги багатьох сучасних дослідників. Фундаментальні аспекти цифровізації та створення інтелектуальних навчальних середовищ аналізують українські вчені В. Биков, В. Кремень, О. Спірін та Ю. Жук, тоді як питання трансформації педагогічної майстерності й готовності викладачів до роботи з алгоритмічними системами обґрунтовує Г. Скрипка [1]. Особливого значення в межах нашого дослідження набувають розвідки, присвячені психологічним детермінантам взаємодії з ШІ. Зокрема, Н. Волянюк та Д. Охріменко [2], а також В. Снісаренко [3] акцентують увагу на ризиках втрати когнітивної автономії та загрозі зниження суб'єктності через «делегування мислення» алгоритмам. Водночас М. Мельник, А. Малиношевська та К. Андросович [4], як і А. Мельник [5], аналізують трансформацію професійної відповідальності та зміни локусу контролю здобувачів освіти. О. Мисюк, С. Постова та Ю. Черняк [6] розглядають ШІ як потужний ресурс для персоналізації та побудови індивідуальних

STEM-траєкторій. Питання формування критичного мислення в еру ШІ аналізують В. Глушко, Є. Шакуров та О. Арделян [7], а загальний аналіз переваг і недоліків впровадження ШІ в ЗВО представлений у працях М. Москалюка, Н. Москалюк та А. Леня [8]. Зарубіжний науковий дискурс доповнює ці погляди концепцією «посиленого інтелекту» Розмарі Лукін, а також аналізом впливу цифрових систем на психологічне благополуччя у працях М. Селігмана та Н. Бострома [9].

Отже, аналіз сучасних досліджень демонструє, що наукові дискусії щодо інтеграції ШІ в сферу освіти зосереджені на кількох ключових психологічних напрямах:

1. Когнітивна самостійність: чи стимулює ШІ критичне мислення, чи стає «інтелектуальним протезом», що нівелює рефлексію?

2. Технологічна адикція: формування поведінкової залежності, що охоплює емоційний та мотиваційний рівні.

3. Ціннісні орієнтації: трансформація поняття авторства та академічної доброчесності.

4. Метакогнітивний розвиток: вплив алгоритмів на здатність до саморегуляції та планування власної діяльності.

Проведене нами експрес-опитування здобувачів освіти психологічного факультету 1-3 курсів та викладачів Навчально-наукового інституту права та психології, а також включене спостереження за освітнім процесом дозволили виявити суперечливі тенденції у сприйнятті ШІ суб'єктами навчання. *З боку здобувачів освіти* констатовано високий рівень інтеграції ШІ у повсякденну навчальну діяльність (понад 70% респондентів підтверджують, що використовують генеративні системи для пошуку ідей та структурування навчального матеріалу, підготовки до навчальних занять, виконання завдань і підготовки текстів тощо). Проте виявлено тривожну динаміку: значна частина студентів демонструє «звику до швидкого результату», що призводить до зниження когнітивної витривалості та небажання працювати з першоджерелами. Мотиваційна сфера зміщується в бік прагматизму – мінімізації зусиль при отриманні позитивної оцінки.

З боку викладацької спільноти спостерігається дихотомія сприйняття: від занепокоєння щодо масової втрати академічної доброчесності до обережного оптимізму щодо автоматизації рутинної перевірки знань. Більшість викладачів (близько 60%) зазначають, що ШІ радикально змінює роль викладача, перетворюючи його з ретранслятора знань на модератора та фасилітатора, який має вчити критично верифікувати інформацію, а не просто її споживати. Крім того, викладачі зазначають, що штучний інтелект слід розглядати не як заміну когнітивної активності людини, а як інструмент її розширення.

Вважаємо, що ключовим чинником мінімізації негативних наслідків є не обмеження доступу до технологій, а формування *психологічної культури їх застосування.* Освітня система має змістити фокус на розвиток метакогнітивних навичок, що дозволять здобувачам чітко усвідомлювати межі можливостей ШІ. Саме ці результати – конфлікт між прагненням студентів до швидкого результату та потребою викладачів у глибокому засвоєнні матеріалу – стають підґрунтям для наших пропозицій.

Практичні рекомендації для освітнього середовища:

1) Формування навичок цифрової гігієни та психологічної стійкості за допомогою навчання студентів розпізнавати когнітивні упередження, що виникають при роботі з ШІ, та розуміти механізми виникнення цифрової залежності.

2) Розробка чітких правил, етико-нормативних протоколів у ЗВО, що визначають межі використання ШІ (наприклад, обов'язкове маркування згенерованого контенту та опис методики роботи з ним).

3) Застосування методу рефлексивного оцінювання, що передбачає перехід від оцінювання «продукту» (реферату, курсової роботи, виконання практичних завдань) до оцінювання «процесу». Студент має захищати не лише результат, а й логіку запитів (промптів) та аргументувати, чому він прийняв або відхилив варіанти, запропоновані ШІ.

4) Запровадження психологічного моніторингу, що включає регулярне діагностування рівня автономності мислення та самооцінки студентів для виявлення ознак «когнітивної ліні» на ранніх етапах.

5) Забезпечення трансформації ролі викладача, що забезпечує стимулювання педагогів до використання ШІ як асистента для розробки складних кейс-стаді, що вимагають від студентів не пошуку відповіді, а розв'язання етичних чи професійних дилем.

Отже, використання ШІ в освіті є амбівалентним процесом, що одночасно виступає і стимулом, і викликом для всіх учасників освітнього процесу. Перспективи подальших розвідок вбачаємо в емпіричному дослідженні кореляції між інтенсивністю взаємодії з генеративним ШІ та рівнем критичного мислення, локусом контролю й академічною відповідальністю студентів у довгостроковій перспективі.

Список використаних джерел:

1. Скрипка Г. Штучний інтелект в освіті: удосконалення програм підвищення кваліфікації педагогів. *Інформаційні технології і засоби навчання*. 2024. Том 101, № 3. С. 227–238.

2. Волянюк Н. Ю., Охріменко Д. В. Штучний інтелект: можливості та ризики для розвитку критичного і самостійного мислення особистості. *Габітус*. 2025. Вип. 78, т. 1. С. 72–77.

3. Снісаренко В. Д. Психологічні особливості використання штучного інтелекту в освіті. *Наукові записки. Серія: Психологія*. 2025. Вип. 2(8). С. 139–144.

4. Мельник М., Малиношевська А., Андросович К. Генеративний штучний інтелект у психології: наслідки та рекомендації для науки і практики. *Інформаційні технології і засоби навчання*. 2024. Т. 103, № 5. С. 188–206.

5. Мельник А. В. Застосування штучного інтелекту в освітньому середовищі: потенціал та виклики. *Розвиток педагогічної майстерності майбутнього педагога в умовах освітніх трансформацій* : матеріали III Всеукр. наук.-практ. конф. 2023. С. 250–253.

6. Мисюк О. Ю., Постова С. А., Черняк Ю. Г. Персоналізація STEM-навчання за допомогою ШІ: адаптивні платформи. *Педагогічна Академія: наукові записки*. 2025. № 16. DOI: https://doi.org/10.5281/zenodo.15109471.

7. Глушко В. В., Шакуров Є. О., Арделян О. В. Педагогічна трансформація в цифрову епоху: вплив штучного інтелекту на

формування критичного мислення та зміну ролі викладача. *Академічні візії*. 2025. Вип. 43. URL: https://www.academy-vision.org/index.php/av/article/download/1886/1757/1797.

8. Москалюк М. М., Москалюк Н. В., Лень А. В. Штучний інтелект в закладах вищої освіти: переваги та недоліки. *Відкрите освітнє е-середовище сучасного університету*. 2023. № 15. С. 85-96.

9. Штучний інтелект у вищій освіті: ризики та перспективи інтеграції : матеріали Всеукр. наук.-пед. підвищення кваліфікації (1 липня – 11 серпня 2024 р.). Львів; Торунь: Liha-Pres, 2024. 328 с.

Клюєва Є.М.
завідувач кафедри
господарського та транспортного права
навчально-наукового інституту управління,
технологій та правових наук,
доктор юридичних наук, професор
(Національний транспортний університет)

ШТУЧНИЙ ІНТЕЛЕКТ У СФЕРІ АДМІНІСТРАТИВНИХ ПОСЛУГ: ПРАВОВІ ЗАСАДИ ЗАСТОСУВАННЯ

Цифрова трансформація публічного управління зумовлює активне впровадження технологій штучного інтелекту у сфері надання адміністративних послуг. Автоматизація процедур, використання алгоритмічних систем для обробки великих масивів даних, прийняття управлінських рішень та взаємодії з громадянами розглядаються як інструменти підвищення ефективності, оперативності та прозорості діяльності органів публічної влади. У цьому контексті штучний інтелект поступово стає невід'ємним елементом сучасної адміністративної практики.

Провідні вчені наголошують, що впровадження штучного інтелекту в державному секторі відкриває нові горизонти для підвищення ефективності, прозорості, підзвітності та адаптивності державного управління. Використання алгоритмів машинного навчання дозволяє оптимізувати надання адміністративних послуг, автоматизувати рутинні процедури, забезпечувати оперативну аналітику соціально-економічних процесів, а також прогнозувати кризові ситуації та реагувати на них. Штучний інтелект особливо важливий у світлі сучасних проблем, таких як глобальні пандемії, збройні конфлікти, зміна клімату, дефіцит ресурсів та соціальна нерівність [1].

Прийняття громадянами штучного інтелекту (ШІ) у наданні державних, адміністративних послуг є важливим для його законного та ефективного використання урядом. Залучення людини до систем штучного інтелекту було запропоновано як спосіб підвищити сприйняття громадянами справедливості цих систем [2].

В епоху цифровізації та стрімким розвитком штучного інтелекту при розробці алгоритмів у прийнятті рішень, все більш важливим є розробка ефективної нормативно-правової бази, яка б забезпечувала етичне, безпечне та відповідальне впровадження штучного інтелекту в різні сфери державного управління. Україна, як держава, що прагне інтегруватися до європейського правового простору, активно працює над імплементацією сучасних підходів до регулювання ШІ, орієнтуючись на найкращі міжнародні практики.

Концепція розвитку штучного інтелекту в Україні, яка була схвалена розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р, стала першим документом, яка заклала стратегічні засади формування державної політики у сфері впровадження технологій штучного інтелекту. У документі визначено ключові напрями застосування штучного інтелекту, зокрема у публічному управлінні, наданні адміністративних послуг, цифровій трансформації державних сервісів та розвитку електронного урядування. Концепція орієнтована на підвищення ефективності діяльності органів державної влади, оптимізацію управлінських процесів, автоматизацію прийняття рішень та покращення якості взаємодії держави з громадянами, що відповідає загальним тенденціям модернізації адміністративної діяльності [3].

Практична реалізація положень Концепції розвитку штучного інтелекту в Україні, схваленої розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р, простежується у поступовому впровадженні алгоритмічних і цифрових рішень у діяльність органів публічної адміністрації, насамперед через розвиток електронних адміністративних послуг, автоматизованих систем обробки звернень, функціонування державних електронних реєстрів та сервісів електронної ідентифікації. В низці наукових дослідженнях з адміністративного права зазначається, що такі інструменти сприяють оптимізації управлінських процедур і підвищенню ефективності публічного управління, водночас потребують чіткого правового регулювання та дотримання принципів законності, прозорості й підконтрольності адміністративних рішень [4].

Мусій в своїй статті слушно зауважує, що ШІ в державному управлінні є трансформаційним інструментом з потенціалом для підвищення ефективності, надання послуг та формування політики. Водночас, його впровадження вимагає ретельного врахування етичних, правових та соціальних наслідків. Глобальна тенденція вказує на поступову, але цілеспрямовану інтеграцію штучного інтелекту в державне управління, зі зростаючим акцентом на відповідальних, прозорих та орієнтованих на громадян підходах [1].

Штучний інтелект (ШІ) у контексті публічного управління розглядається як комплекс передових цифрових технологій, що здатні трансформувати основні функції держави – аналітичні, прогностичні, управлінські та виконавчі. Н.Коротченко вказує, що йдеться не лише про автоматизацію рутинних адміністративних процедур, а й про переосмислення засад прийняття рішень, формування політик і здійснення контролю за результатами їх реалізації [5].

В своїй статті Максіменцева, аналізуючи вплив ШІ на процес прийняття управлінських рішень, зробила висновок, що На практиці впровадження ШІ у публічному управлінні та адмініструванні досить обмежене, як з точки зору кількості використовуваних програм, так і з точки зору глибини їх інтеграції, Але якщо органи державної влади запровадять процес прийняття рішень за допомогою ШІ, схвалення громадськості буде важливим аспектом його успішного впровадження. Погоджуюсь з думкою, що у сфері публічного управління штучний інтелект має багато можливостей для підвищення ефективності та якості послуг, наданих громадянам [2].

Біла книга з регулювання штучного інтелекту, яку у 2023 році презентувало Міністерство цифрової трансформації України презентувало так звану Білу книгу, яка стала своєрідною дорожньою картою для розробки комплексного правового підходу. Вона містить низку рекомендацій, зокрема щодо саморегулювання, створення так званих регуляторних пісочниць, де можна випробовувати інноваційні технології без порушення чинного законодавства. Окрему увагу в документі приділено етичним питанням, а також рекомендаціям щодо впровадження пілотних проєктів [6].

Таким чином, впровадження технологій штучного інтелекту у сфері надання адміністративних послуг є важливим етапом цифрової трансформації публічного управління, що сприяє підвищенню ефективності, оперативності та якості державних сервісів. Водночас практична реалізація потенціалу штучного інтелекту в Україні потребує подальшого розвитку нормативно-правової бази та чіткого визначення механізмів його застосування в адміністративній діяльності зокрема з урахуванням міжнародного досвіду та принципів прозорості, підзвітності й ефективності державного управління.

Список використаних джерел:

1. Мусій О.І. Використання штучного інтелекту в публічному адмініструванні: виклики та перспективи. Електронне наукове видання «Аналітично-порівняльне правознавство». Випуск № 06, 2025, частина 2. DOI https://doi.org/10.24144/2788-6018.2025.06.2.64

2. Максіменцева Н. О. Виклики застосування штучного Інтелекту у сфері публічного Управління, врядування та послуг. Інвестиції: практика та досвід №4. 2024. DOI: 10.32702/23066814.2024.4.204

3. Розпорядження Кабінету Міністрів України; Концепція № 1556-р «Про схвалення Концепції розвитку штучного інтелекту в Україні» від 02.12.2020. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text

4. Соколік В. Д., Пащенко Д. В. та ін. Правове регулювання використання штучного інтелекту в публічному управлінні: виклики цифрової епохи. Науковий вісник Одеського національного економічного університету. № 4 (329). 2025. DOI: https://doi.org/10.32680/2409-9260-2025-4-329-30-36

5. Коротченко Н.О. Штучний інтелект як чинник модернізації публічного управління в умовах діджиталізації суспільних відносин. Державне будівництво. № 1 (37). 2025. DOI: https://doi.org/10.26565/1992-2337-2025-1-06

6. Біла книга з регулювання ШІ в Україні: бачення Мінцифри / уклад. Г. Румянцев. Київ : Міністерство цифрової трансформації України, 2023. 30 с. URL: https://thedigital.gov.ua/storage/uploads/files/page/community/docs/Регулювання%20ШІ.pdf (дата звернення 01.03.2026).

Кобилянський О.Л.
доцент кафедри цивільного та кримінального права
навчально-наукового інституту
управління технологій та правових наук,
кандидат юридичних наук, доцент, доктор філософії
(Національний транспортний університет)

ШІ У ПОРІВНЯЛЬНОМУ ДОСЛІДЖЕННІ ОЗНАК ПОЧЕРКУ ТА СЛІДІВ ПАЛЬЦІВ РУК: МЕТОДОЛОГІЧНІ ТА ДОКАЗОВІ АСПЕКТИ ПОРІВНЯНО З ТРАДИЦІЙНИМИ МЕТОДАМИ

Сучасний етап розвитку криміналістики та судової експертизи характеризується інтенсивною цифровізацією доказової діяльності та впровадженням алгоритмічних інструментів обробки великих масивів даних. Особливого значення це набуває у сфері ідентифікаційних досліджень, зокрема у почеркознавчій та дактилоскопічній експертизах, де традиційно домінує експертно-інтерпретаційна модель встановлення тотожності об’єктів. Застосування систем штучного інтелекту (далі – ШІ) актуалізує необхідність переосмислення методологічних засад порівняльного дослідження ознак та визначення доказового статусу алгоритмічних результатів.

У класичній криміналістичній теорії ідентифікація ґрунтується на виявленні, фіксації та порівнянні сукупності індивідуальних ознак об’єкта. У почеркознавстві такими є загальні та окремі графічні ознаки письма; у дактилоскопії – морфологічні характеристики папілярного узору, насамперед окремі ознаки та їх просторове взаємне розташування.

Методологічно порівняльне дослідження включає:

– аналіз об’єктів;

– синтез встановлених ознак;

– їх зіставлення;

– оцінку сукупності;

– формування висновку.

Використання ШІ трансформує насамперед перші два етапи – аналіз та виділення ознак. Алгоритми машинного та глибинного

навчання здатні автоматично виявляти ознаки у зображеннях рукописних текстів і слідів пальців рук, формуючи цифрові моделі ознак без безпосереднього втручання людини. Проте постає питання: чи змінює це саму природу ідентифікації, чи лише її інструментальну складову?

У сфері дослідження ознак почерку алгоритми ШІ застосовуються для:

– автоматизованого виділення структурних елементів письма;

– дослідження просторово-графічних характеристик письма;

– класифікації графічних ознак на основі нейронних мереж;

– виявлення статистично значущих збігів між досліджуваними зразками.

Перевагою таких систем є здатність обробляти значні масиви графічних даних та мінімізувати вплив суб'єктивних когнітивних чинників. Водночас існують суттєві ризики, зокрема залежність результату від навчальної вибірки, алгоритмічне упередження та обмежена можливість обґрунтованого та процесуально допустимого висновку.

Традиційна почеркознавча експертиза передбачає аргументоване обґрунтування кожної встановленої ознаки. Натомість у випадку застосування складних нейронних мереж процес формування висновку може мати характер «чорної скриньки», що ускладнює процесуальну перевірку його достовірності.

У дактилоскопії алгоритмічні системи вже тривалий час використовуються у межах автоматизованих дактилоскопічних інформаційних систем. Сучасні моделі глибинного навчання дозволяють:

– автоматично виділяти окремі ознаки;

– оцінювати якість сліду;

– формувати цифрові шаблони папілярних узорів;

– здійснювати швидкий пошук збігів у великих базах даних.

На відміну від почеркознавства, де суб'єктивний фактор відіграє значну роль, у дактилоскопії алгоритмізація більш органічно інтегрується у методику дослідження. Проте і тут залишається принципове питання меж автоматизації: чи може

остаточний ідентифікаційний висновок формуватися без експертної оцінки?

Традиційна модель характеризується високим рівнем обґрунтованості та процесуальної зрозумілості, проте залежить від професійного досвіду експерта. Алгоритмічна модель забезпечує відтворюваність та масштабованість результатів, але може бути недостатньо прозорою.

Ключові відмінності полягають у:

– характері джерела помилки (когнітивна помилка експерта проти алгоритмічної помилки моделі);

– рівні стандартизації процедури;

– можливості статистичної верифікації результату;

– ступені пояснюваності отриманого висновку.

Оптимальною видається гібридна модель, у межах якої ШІ використовується як інструмент попереднього аналізу та статистичної підтримки, тоді як остаточна оцінка сукупності ознак і формулювання висновку залишаються за експертом.

З позиції кримінального процесу ключовими є питання допустимості та належності доказу. Для використання результатів, отриманих із застосуванням ШІ, необхідно:

– нормативне врегулювання статусу алгоритмічних інструментів;

– сертифікація програмного забезпечення;

– документування процедури обробки даних;

– забезпечення можливості перевірки та повторного тестування результату.

Доказова цінність алгоритмічного висновку безпосередньо залежить від його верифікованості та пояснюваності. Відсутність прозорості алгоритму може поставити під сумнів обґрунтованість висновку у суді.

Висновки.

Штучний інтелект трансформує інструментальну складову порівняльного дослідження, але не змінює його ідентифікаційної природи.

У почеркознавчій експертизі застосування ШІ потребує особливої уваги до можливості експертної інтерпретації отриманих результатів та підтвердження їх достовірності.

У дактилоскопії алгоритмічні системи можуть ефективно інтегруватися у методику дослідження за умови збереження експертного контролю.

Процесуальна допустимість результатів ШІ обумовлена наявністю стандартів верифікації, сертифікації та документування.

Перспективним напрямом є формування гібридної моделі «експерт-алгоритм», що поєднує статистичну точність ШІ з професійною відповідальністю експерта.

Таким чином, впровадження штучного інтелекту у порівняльне дослідження ознак почерку та слідів пальців рук має розглядатися не як заміна експерта, а як еволюція методології криміналістичної ідентифікації, що потребує комплексного теоретичного та нормативного осмислення.

Козакевич О.М.
доцент кафедри правових та інформаційних технологій,
докторка філософії
*(Хмельницький інститут соціальних технологій
Відкритого міжнародного університету
розвитку людини «Україна»)*

ШТУЧНИЙ ІНТЕЛЕКТ ЯК НОВІТНІЙ ВИМІР ЗАБЕЗПЕЧЕННЯ ДОСТУПУ ДО ПРАВОСУДДЯ

Сучасний етап розвитку правосуддя характеризується активним пошуком інструментів, здатних одночасно посилити інституційну незалежність суду та розширити фактичний доступ особи до правосуддя. Зі стрімким розвитком інформаційного суспільства та сучасних інформаційно-комунікаційних технологій, поняття «доступ до правосуддя» розглядається не тільки як можливість присутності в судовому засіданні, а крізь призму сукупності технологій, дій і процедур допоміжного характеру, що забезпечують та полегшують шляхи доступу до правосуддя. У цьому контексті, цифрові інструменти нового покоління перестають бути суто технічним феноменом і набувають ознак процесуального інструментарію [1, с.207-208]. Показовим є досвід Республіки Колумбія, де у лютому 2023 року було здійснено розгляд справи у форматі метавсесвіту — із використанням віртуально змодельованої зали судових засідань та аватарів як цифрових репрезентацій учасників процесу. Засідання транслювалося у відкритому доступі та відбулося без технічних перешкод, що засвідчило операційну придатність такого формату[2].

Зазначений крок розглядається не лише як технологічний експеримент, а як спроба відповісти на проблему перевантаженості судової системи та забезпечити ширший доступ до судового розгляду. Паралельно у різних юрисдикціях усталюється практика дистанційного судочинства з використанням платформ синхронної відеокомунікації (зокрема Zoom, Google Meet тощо), що трансформує традиційне розуміння процесуальної

присутності сторін. Технологічні рішення, які розробляються такими корпораціями, як Microsoft і Meta, відкривають перспективу подальшої інтеграції віртуальних просторів у сферу здійснення правосуддя.

Окремим виміром цифровізації є впровадження інструментів штучного інтелекту у діяльність судових органів. Нормативним орієнтиром у цій сфері стала Європейська етична хартія щодо використання штучного інтелекту в судових системах, ухвалена у 2018 році Європейською комісією з ефективності правосуддя (CEPEJ)[3]. Документ закріплює фундаментальні принципи застосування алгоритмічних технологій, спрямовані на забезпечення поваги до прав людини, недискримінаційності, прозорості, безпеки даних та обов'язкового людського контролю. У глосарії Хартії штучний інтелект визначається як сукупність наукових методів і технічних рішень, орієнтованих на моделювання когнітивних функцій людини засобами машинної обробки інформації.

Практика застосування ШІ вже виходить за межі теоретичних моделей. У тій самій Колумбії суддя під час підготовки судового рішення звернувся до системи ChatGPT як до допоміжного аналітичного інструменту, зазначивши у мотивувальній частині отримані алгоритмічні відповіді. Такий підхід актуалізував дискусію щодо меж допустимого використання штучного інтелекту та співвідношення технологічної підтримки з виключною компетенцією судді щодо оцінки доказів і формування правової позиції[2].

Для України застосування штучного інтелекту стало актуальним в середині 2022 року, із застосуванням нового чат-боту ChatGPT, компанії OpenAI. Сервіси та інструменти цього чат-боту дають можливість користувачам отримати відповідь на будь-яке поставлене питання. З огляду на План Відновлення України, а саме Національну Програму: штучний інтелект при наданні публічних послуг, інструменти ChatGPT, можуть бути корисні в правосудді, використовуючи весь його функціонал. Так, сервіси цього штучного інтелекту можна було б застосувати до підбірки нормативно-правової бази для конкретного спору чи для підготовки певних процесуальних документів. Це прискорить розгляд справ, та вплине на чинники (бар'єри) в умовах

транзитивності, що перешкоджають реалізації та захисту права на доступ до правосуддя такі як: велика кількість судових справ на кожного суддю; процесуальні перешкоди у доступі до правосуддя, та в наслідку, можливо, буде механізмом подолання цих бар'єрів.

В Україні процес застосування ШІ також набуває нормативного оформлення. Нова редакція Кодексу суддівської етики, затверджена у листопаді 2024 року, передбачає можливість використання суддями технологій штучного інтелекту за умови збереження їхньої незалежності, безсторонності та автономності у прийнятті рішень. Водночас ключовим положенням є закріплення персональної відповідальності судді за результати процесуальної діяльності незалежно від застосування алгоритмічних інструментів[4].

Подальший розвиток цієї тенденції пов’язується з ініціативами Міністерства цифрової трансформації України щодо створення цифрового суду для розгляду адміністративних справ із використанням технологій ШІ. Передбачається істотна автоматизація процедур, що має скоротити часові витрати та спростити комунікацію учасників із судовою системою[5]. Водночас практика вже демонструє ризики непрозорого використання ШІ. На початку грудня 2025 року Новозаводський райсуд Чернігова використав штучний інтелект для редагування тексту ухвали, випадково залишивши у документі фразу ШІ-асистента. Хоча формально судді не порушили законодавства, цей випадок загострює питання готовності судової системи до застосування алгоритмічних технологій[6]. Проте, впровадження ШІ в систему правосуддя потребує вирішення технічних проблем та вдосконалення алгоритмів задля неупередженого судового розгляду. Залучення штучного інтелекту в правосуддя, безумовно, має безліч переваг і спрямоване на розвантаження роботи судів, разом з тим, виникає безліч спірних питань. Зокрема, так як штучний інтелект це технології, можливий технічний збій або відсутність необхідного контролю з боку людей, що може призвести до негативних наслідків. В країнах, які використовують штучний інтелект вже виникали спірні питання по забезпеченню права на конфіденційність. Крім того, в юридичній науці виникає питання про правосуб'єктність штучного інтелекту, об’єктів

створеного штучним інтелектом та юридичної відповідальності за вчинену ним помилку.

Практика засвідчує наявність ризиків непродуманого або непрозорого використання алгоритмічних рішень. Поодинокі випадки технічного втручання ШІ у підготовку процесуальних документів без належного редагування з боку судді порушують питання професійної обачності та інституційної готовності судової системи до повномасштабної алгоритмізації. У ширшому теоретико-правовому вимірі впровадження штучного інтелекту в механізм здійснення правосуддя породжує низку складних проблем: забезпечення конфіденційності даних, недопущення алгоритмічної упередженості, визначення правового статусу результатів, створених ШІ, а також окреслення меж юридичної відповідальності у разі помилки. Переважаючою у доктрині залишається позиція, відповідно до якої штучний інтелект не є самостійним суб'єктом права, а розглядається як інструмент, відповідальність за застосування якого покладається на людину — носія владних повноважень.

Таким чином, штучний інтелект формує новий вимір механізму забезпечення доступу до правосуддя, поєднуючи потенціал підвищення ефективності з необхідністю суворого дотримання принципів незалежності суду, процесуальної справедливості та верховенства права.

Список використаних джерел:

1. Козакевич О.М. Доступність правосуддя у транзитивному суспільстві: сучасний вимір: монографія. Одеса: Видавництво «Юридика» 2023. 246 с.

2. Суд провів перше засідання у метавсесвіті, використовуючи інструменти віртуальної реальності. URL: https://sud.ua/uk/news/publication/263423-sud-provel-pervoe-zasedanie-v-metavselennoy-ispolzuya-instrumenty-virtualnoy-realnosti-video?fbclid=IwAR3zuFIPPZjuaOiTzV21CnemRs_k4SPurI57SG4BLVx-WX7QH7yUOK-aeQI

3. European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment. URL:

https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c

4. Кодекс суддівської етики : затв. рішенням З'їзду суддів України від 22 листопада 2024 р. URL: https://court.gov.ua

5. Мінцифри у 2026 році планує запустити е-суд із ШІ для адміністративного судочинства. URL: https://sud.ua/uk/news/ukraine/349754-mintsifry-v-2026-godu-planiruet-zapustit-e-sud-s-ii-dlya-administrativnogo-sudoproizvodstva#google_vignette

6. Постанова Новозаводського районного суду міста Чернігова від 17 жовтня 2025 р., судова справа № . 751/8289/25 Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Review/131196945

Колич О. І.
доцент кафедри теорії, історії
та конституційного права
кандидат юридичних наук, доцент
(Львівський державний університет внутрішніх справ)
Шербей Н.
студент навчально-наукового інституту
права та правоохоронної діяльності
(Львівський державний університет внутрішніх справ)

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ І ПРИВАТНІСТЬ

Актуальність дослідження зумовлена трансформаційними процесами в умовах цифровізації суспільства, що супроводжуються інтенсивним збиранням, зберіганням та обробкою персональних даних у різних сферах публічного і приватного життя. Забезпечення права на повагу до приватного і сімейного життя, гарантованого ст. 32 Конституція України [4], набуває особливого значення в контексті зростання кіберзагроз та розвитку інформаційних технологій.

Право на приватність є фундаментальним конституційним правом людини, яке забезпечує недоторканність особистого і сімейного життя, таємницю кореспонденції, особистих і сімейних таємниць, захист честі, гідності та ділової репутації. Воно охоплює можливість особи контролювати інформацію про себе та обмежувати втручання третіх осіб у власне життя. Нормативне закріплення цього права здійснено у ст. 32 Конституції України.

Право на приватність також виступає основою для захисту персональних даних та визначає межі законного втручання у сферу особистого життя. У науковому розумінні приватність є комплексним соціально-правовим феноменом, що забезпечує автономію особи у прийнятті рішень та контроль над поширення інформація про себе.

Персональні дані – це будь-яка інформація, що стосується фізичної особи, яка ідентифікована або може бути конкретно ідентифікована. До таких даних належать: прізвище, ім’я, по батькові, дата народження, місце проживання, ідентифікаційний

код, контактні дані, IP-адреси, біометричні та інші відомості, що дозволяють визначити особу.

Відповідно до Закон України «Про захист персональних даних», персональні дані є об'єктом правової охорони, і їх обробка допускається лише за наявності законних підстав [3].

Обробка персональних даних ґрунтується на системі принципів, що визначають законність, етичність та ефективність інформаційних відносин між суб'єктом та розпорядником даних, основні з яких:

- законність і добросовісність обробки – персональні дані повинні оброблятися відповідно до вимог чинного законодавства та з дотриманням прав і законних інтересів фізичної особи;
- цільове призначення – збір та обробка даних допускаються лише для чітко визначених і законних цілей;
- мінімізація обсягу даних – обробляються лише ті дані, які є необхідними для досягнення конкретної мети;
- точність і актуальність – дані повинні бути достовірними.

Суб'єкт персональних даних – це фізична особа, чиї дані обробляються. Законодавство надає їй низку ключових прав, які забезпечують контроль над інформацією про себе та захищають її приватність, зокрема такі: право на доступ до даних – суб'єкт має отримати інформацію про те, які дані збираються, з якою метою, хто їх обробляє та на яких умовах; право на уточнення та виправлення даних – особа може вимагати виправлення неточності або оновлення інформації.; право на видалення або обмеження обробки – у разі незаконної обробки або якщо дані більше не потрібні для визначеної мети, суб'єкт може вимагати їх видалення або обмеження обробки; право на судовий захист – у разі порушення законних прав суб'єкт може звернутися до суду або до контролюючого органу.

Гарантії реалізації цих прав забезпечуються законодавством, що регулює обробку персональних даних.

Контроль за додержанням законодавства у сфері захисту персональних даних в Україні здійснюється спеціалізованими державними органами, основним серед яких є Уповноважений Верховної Ради України з прав людини. Діяльність цього органу включає моніторинг і перевірку розпорядників даних, розгляд

скарг суб'єктів персональних даних, видачу рекомендацій та обов'язкових приписів.

Відповідальність за порушення законодавства про персональні дані передбачає застосування адміністративної, цивільно-правової або кримінальної відповідальності. Адміністративну відповідальність виражається у накладенні штрафів або інших санкцій за порушення правил обробки персональних даних.

Цивільно-правова відповідальність полягає у відшкодуванні матеріальної або моральної шкоди, завданої незаконною обробкою персональних даних. Кримінальну відповідальність застосовують у випадках несанкціонованого доступу, розголошення або використання персональних даних із тяжкими наслідками, відповідно до Кримінального кодексу України [1, с. 20].

Таким чином, система органів контролю та механізм юридичної відповідальності забезпечують комплексний захист персональних даних і сприяють дотриманню балансу між правами суб'єктів даних та законними інтересами держави й бізнесу.

Сфера захисту персональних даних і права на приватність в Україні стикається з низкою сучасних викликів, що зумовлені цифровізацією суспільства, активним розвитком інформаційних технологій, автоматизованих систем обробки даних та зростанням кіберзагроз.

Перспективи вдосконалення правового регулювання передбачають удосконалення механізмів контролю за обробкою персональних даних, посилення відповідальності за порушення прав суб'єктів, впровадження сучасних технологічних і правових засобів захисту інформації, а також підвищення правової обізнаності громадян щодо їхніх прав у сфері персональних даних.

Таке вдосконалення законодавства сприятиме ефективному захисту прав суб'єктів персональних даних, забезпеченню балансу між приватністю громадян та законними інтересами держави й бізнесу, а також підвищенню рівня інформаційної безпеки в країні.

Список використаних джерел:

1. Бєлова М.В., Бєлов Д.М. Виклики та загрози захисту персональних даних у роботі зі штучним інтелектом. Науковий

вісник Ужгородського національного університету. Серія: Право. Випуск 79: Частина 2. 2023. С. 17-22.

2. Кодекс України про адміністративні правопорушення. Закон України від 07.12.1984 №8073-X. URL: https://zakon.rada.gov.ua/laws/show/8073-10#Text

3. Кримінальний кодекс України. Закон України 05.04.2001 №2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14

4. Конституція України від 28.06.1996 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр

5. Про захист персональних даних. Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

Копча В.В.
професор кафедри кримінально-правової політики,
доктор юридичних наук, професор
(ДВНЗ «Ужгородський національний університет»)

КРИМІНАЛЬНО-ПРАВОВА ХАРАКТЕРИСТИКА ЩОДО РОЗСЛІДУВАННЯ КРАДІЖОК: ТЕОРІЯ І ПРАКТИКА

Основними елементами кримінально-правових та криміналістичних характеристик крадіжок (ст. 185 КК України) є: спосіб учинення крадіжок; предмет злочинного посягання; типова слідова картина; особа злочинця; особа потерпілого.

Однак можна зазначити, що способи учинення крадіжок, як правило можна впровадити, що поняттям «крадіжка» охоплюється значне коло злочинів, що відрізняються один від одного предметом злочинного посягання, способом учинення і приховування, місцем реалізації злочинного задуму тощо. До числа типових дій злочинців з підготовки до вчинення крадіжки слід віднести: вибір об'єкта крадіжки, у тому числі і майбутнього потерпілого; вивчення об'єкта крадіжки й обстановки, в якій злочинцю доведеться діяти; вибір найбільш ефективного способу безпосереднього заволодіння майном, а також підготовка необхідних технічних засобів, що полегшують здійснення злочинного наміру; вибір способу приховання слідів крадіжки, в тому числі приховання чи збут викрадених речей; попередню змову між співучасниками крадіжки, розподіл ролей і визначення ролі кожного у майбутньому злочині, а також при необхідності забезпечення «алібі».

Виявлено, що в практичній роботі найбільш поширеними є крадіжки з приміщень. Вони мають багато спільного: схожий характер слідів і знарядь злому, схожість обставин учинення та інше, що дозволяє згрупувати способи безпосереднього проникнення до приміщення: першу групу способів учинення крадіжок з приміщень складають дії, вчинені із застосуванням технічних засобів, що полегшують реалізацію злочинного наміру: другу групу складають способи вчинення крадіжок майна, матеріальних цінностей з приміщень, доступ до яких є відносно вільним.

Доведено напрямки виконання процесуальних дій з метою приховування крадіжок злочинцями вживаються заходи для маскування, знищення і фальсифікації слідів на місці злочину.

На сьогоднішній день дослідження фактів, щодо приховування злочинів, а саме крадіжок так як правопорушниками вживаються різні заходи, щодо приховування або знищення та фальсифікації слідів на місці злочину, де застосовуються рукавички, покриття долонь рук лаком або знежирюючим розчином, взуття більшого розміру або жіноче, зміна зовнішнього вигляду або призначення предмета крадіжки. Окрім цього, предмет крадіжки, знищення маркувальних і номерних знаків, обмова співучасників, створення фальшивих алібі тощо); швидкий збут викраденого або його приховання на певний час; викидання викраденого майна у випадку виникненні небезпеки викриття; за дачу неправдивих показань, відмова від дачі показань; вплив на очевидців, свідків, потерпілих з метою дачі ними неправдивих показань або відмови від дачі показань тощо.

В правовій науці деякі напрями, що стосуються предмету злочинного посягання, під час квартирних крадіжок, як правило, викрадаються: гроші, цінні папери, вироби з коштовних металів та каменю, антикваріат, сучасні технічні пристрої, одяг, взуття та інші предмети господарсько-побутового призначення. Також предметом кишенькових крадіжок є гроші, коштовності та невеликі технічні пристрої, які викрадають з кишень, сумок, портфелів тощо. Сферою комунального господарства предметами крадіжок є каналізаційні люки, будинкові лічильники, агрегати ліфтів, металеві елементи споруд, обладнання в трансформаторних підстанціях тощо.

Визначення предмета крадіжки під час розслідування конкретного злочину під час воєнного стану, сприяє встановленню інших його елементів, зокрема окремих характеристик особи злочинця, обстановки вчинення тощо. Типовою та слідовою картиною, можна вважати механізм утворення слідів під час учинення крадіжок обумовлюється характером взаємодії злочинця з оточуючою матеріальною обстановкою.

Щодо вчинення крадіжки, як правило, залишаються сліди: злочинця (сліди рук, ніг, зубів, губ, крові, слини, інших виділень, мікрочастинок одягу і взуття, запахові сліди тощо); знарядь

злочину (сліди «віджиму» дверей, примусового відкриття запірних пристроїв, сліди дії агресивної рідини тощо).

Загалом за достатню поширеність правопорушники (злочинці), які як правило вчиняють крадіжки, умовно поділяють на дві групи: професійні крадії, для яких крадіжки є основним джерелом існування. Як правило, такі особи раніше судимі за аналогічні злочини. Ці особи мають певну спеціалізацію; особи, які вчинили крадіжку вперше, або вчиняють їх нерегулярно внаслідок конкретних обставин: по-перше, сприятливих умов для вчинення крадіжки; по-друге, дані особи допускають можливість вчинення інших аморальних вчинків. Ці особи, як правило, діють спонтанно, не професійно, викрадають предмети, що перебувають без нагляду. [1, с. 118 с.].

За даними криміналістичної характеристики крадіжок свідчать про якісні зміни злочинного середовища. Також спостерігається значне омолодження квартирних злодіїв, середній вік яких складає 24 роки лиши п'ятий з числа засуджених за крадіжки був старше 28 років. У той же час серед засуджених за крадіжки державного і колективного майна вдвічі більше питома вага осіб середнього віку (32–47 років). Майже половина крадіжок учиняється злочинними групами з розподілом ролей між їх членами і відповідною «технологією» підготовки, вчинення і приховання даних злочинів (наводка, збирання інформації, відпрацювання плану, розподіл функцій виконання, збут краденого тощо). Особа потерпілого. Взаємозв'язок «злочинець або потерпілий» часто посідає ключове місце у виявленні різноманітних обставин. [3, 397 с.].

Вивченням щодо криміналістичної характеристики крадіжок головним чином акумулюється інформація про потерпілого та його поведінку, що дозволяє отримати уявлення про специфіку його взаємовідносин зі злочинцем, спосіб виникнення цього зв'язку. Даним напрямком можна визначити, щодо, важливого значення набувають відомості про потерпілого, якими міг скористатися злочинець під час підготовки і вчинення крадіжки. Слідчий поліції проводить початковий етап розслідування крадіжок, і під час розслідування крадіжок необхідно встановити такі основні обставини: факт таємного викрадення майна; місце, час та умови вчинення крадіжки; предмет крадіжки, його вартість,

особливі ознаки; спосіб учинення крадіжки, технічні засоби, які були застосовані для таємного викрадення і приховання; тривалість перебування і конкретні дії злочинця на місці крадіжки; особа, яка вчинила крадіжку, мотиви її поведінки; наявність злочинної групи та роль кожного з її членів; спосіб, час і місце збуту вкраденого; обставини, що сприяли вчиненню крадіжки; обставини, що впливають на ступінь і характер вини особи.

Щодо початкового етапу розслідування крадіжок найбільш типовим є такі слідчі ситуації: факт крадіжки встановлено і підозрюваного затримано з речовими доказами або за «гарячими слідами». Основне тактичне завдання в даній ситуації зафіксувати сліди злочину. Типові загальні версії у вказаній ситуації: а) злочин вчинила затримана особа; б) злочину не було повідомлення помилкове або неправдиве (затриманий придбав майно та володіє правами на нього тощо). Крім того, висуваються та перевіряються окремі версії про обставини розслідуваної події (наявність співучасників, щодо ролі кожного із них, тощо).

Метою перевірки цих версій проводяться такі слідчі (розшукові) дії: особистий обшук; огляд одягу, речей, вилучених у затриманого, а також його допит. Далі слід допитати свідків, потерпілого, посадових або матеріально відповідальних осіб, що дозволить отримати важливу доказову інформацію про обставини крадіжки, та її виявлення, учасників та обставини затримання підозрюваного, коло осіб, поінформованих про розслідувану подію, опис викраденого майна. Після виконання вказаних слідчих (розшукових) дій слідчий проводить огляд місця події (завчасно забезпечивши його охорону), в тому числі й місця затримання підозрюваного з метою виявлення, фіксації, вилучення інших речових доказів, що підтверджують причетність затриманого до розслідуваної крадіжки. [6, 474 с.].

Початковий етап розслідування в даній ситуації закінчується проведенням обшуку за місцем проживання затриманого; пред'явленням для впізнання потерпілому або матеріально відповідальній особі майна (матеріальних цінностей), вилучених у підозрюваного; призначенням криміналістичних експертиз. а. Факт крадіжки встановлено, є відомості про особу злочинця (або групу злочинців), проте ніхто не затриманий.

Висновки. В ході здійсненого аналізу, щодо призначення і проведення експертиз, під час розслідування крадіжок, експертизи що призначаються, можуть бути поділені на дві групи: а) ті, що призначаються для ідентифікації злочинця, знарядь злочину, взуття, транспортних засобів (або їх частин), дослідження способу подолання перешкод, укриття сховищ; б) ті, що призначаються для дослідження викраденого майна. До першої групи належать, наприклад, дактилоскопічна експертиза, судово-медична, трасологічна (в тому числі встановлення цілого за частинами), експертиза слідів нашарування тощо. До другої групи належать товарознавча, хімічна і біологічна експертизи.

Список використаних джерел:

1. Іщенко А.В., Пясковський В.В., Самодін А.В. та ін. Криміналістика у питаннях і відповідях : навч. посіб. К.: ТОВ «Видавництво «Центр учбової літератури», 2016. 118 с.
2. Кобилянський О.Л., Кофанов А.В. Криміналістика : конспект лекцій. К.: Держ. ун-т інфраструктури та технологій, Укр. ДГРІ, 2019. 380 с.
3. Криміналістика (курс лекцій): навч. посібн. М.Ю. Будзієвський, О.В. Лускатов, І.В. Пиріг та ін. Дніпропетровськ : Дніпроп. держ. ун-т внутр. справ, 2013. 397 с.
4. Криміналістика у питаннях та відповідях : навч. посіб. А.В. Іщенко, В.В. Пясковський, А.В. Самодін, Ю.М. Чорноус та ін. Київ: Центр учбової літератури, 2016. 118 с.
5. Криміналістика. Академічний курс: підручник Т.В. Варфоломеєва, В.Г. Гончаренко, В.І. Бояров та ін. Київ: Юрінком Інтер, 2011. 504 с.
6. Криміналістика: навчальний посіб. для студ. юрид. спец. вищ. навч. закл. в двох частинах. Частина ІІ: Криміналістична тактика. Методика розслідування Б.Є. Лук'янчиков, Є.Д. Лук'янчиков, С.Ю. Петряєв. К.: Нац. тех. ун-т України «Київський політехнічний інститут ім. Ігоря Сікорського». 2017. 474 с.
7. Криміналістика: підруч. для студ. вищ. навч. закл. К.О. Чаплинський, О.В. Лускатов, І.В. Пиріг та ін. 2-е вид, перероб. і доп. Дніпро: Дніпроп. держ. ун-т внутр. справ; Ліра ЛТД, 2017. 480 с.
8. В.В. Копча, Н.В. Копча: Криміналістична техніка, тактика і методика: Навчальний посібник. м. Одеса: Видавничий дім «Гельветика», 2022. 284 с.

Краснобриж Б.О.
курсант
(Харківський національний університет внутрішніх справ)
Сліпченко С.П.
курсант
(Харківський національний університет внутрішніх справ)
Горбунова К.В.
доцент кафедри кримінального процесу
та організації досудового слідства ННІ № 1,
доктор філософії
(Харківський національний університет внутрішніх справ)

ПРОЦЕСУАЛЬНІ АСПЕКТИ ТА ДОКАЗОВЕ ЗНАЧЕННЯ РЕЗУЛЬТАТІВ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Стрімкий ріст використання технологій сучасною злочинністю зумовлює нагальну потребу в імплементації дієвих та ефективних заходів протидії з боку правоохоронних органів. У цьому контексті системи штучного інтелекту (далі ШІ) трансформуються з теоретичних концепцій у практичні інструменти досудового розслідування, зокрема в аспектах інтелектуального аналізу великих масивів даних (Big Data), автоматизованої ідентифікації суб'єктів за біометричними параметрами та аналітики кримінальних правопорушень.

Водночас, інтеграція алгоритмічних рішень у кримінальне провадження являє складну правову дилему. Вона полягає у необхідності дотримання балансу між процесуальною ефективністю та забезпеченням фундаментальних засад, закріплених у КПК України та Конвенції про захист прав людини і основоположних свобод, а саме: законності (ст. 9 КПК) у питаннях допустимості доказів, отриманих ШІ; принципу верховенства права (ст. 8 КПК) та права на справедливий судовий розгляд.

На даний час, правоохоронні органи використовують штучний інтелект у декількох ключових сферах:

1. Для аналізу часу, місця та характеру попередніх правопорушень, використовують великі дані (Big Data), що

дозволяють у просторово-часовому кластері прогнозувати кримінальну активність.

2. Сучасні системи розпізнавання облич, інтегровані в міські мережі відеоспостереження, дозволяють ефективно ідентифікувати підозрюваних у реальному часі.

3. ШІ здатний обробляти терабайти інформації з вилучених гаджетів за лічені хвилини, знаходячи приховані зв'язки між фігурантами, які людина-слідчий могла б пропустити [1, с. 112].

Результати, отримані за допомогою штучного інтелекту (наприклад, звіт про ймовірність рецидиву або протокол розпізнавання обличчя), за своєю природою є цифровими доказами. Проте, для надання їм юридичної сили, вони мають бути легалізовані через існуючі процесуальні форми: висновок експерта або додаток до протоколу слідчої дії [2, с. 47].

Критичним детермінантом процесуальних ризиків при імплементації систем штучного інтелекту, є непрозорість архітектури алгоритмів глибокого навчання, що в теорії права класифікується як проблема відсутності інтерпретованості результатів. У ситуації, коли сторона обвинувачення залучає висновки, генеровані ШІ, як підґрунтя для формування доказової бази, виникає системна загроза порушення фундаментальних засад кримінального провадження [3, с. 42].

На наше переконання, сучасна правозастосовна практика із використанням штучного інтелекту, може опинитись у безвихідному стані. Будова кримінального процесу заснована на безпосередньому дослідженні доказів, де свідок підлягає допиту, а експерт – надає роз'яснення щодо застосованої методики дослідження та отриманих результатів у своєму висновку. Проте, використання у кримінальному процесі нейромереж, де відбувається машинне обчислення мільярдів параметрів без експліцитного логічного ланцюжка, унеможливлює проведення аналогічних процесуальних дій. Водночас, для того, щоб в Україні використовувати штучний інтелект як допустимий доказ у кримінальному провадженні, треба адаптувати Кримінальний процесуальний кодекс до нових викликів цифровізації, а саме: 1) введення поняття «цифровий доказ, отриманий за допомогою автоматизованих систем»; 2) розробка методики судової експертизи алгоритмів ШІ; 3) встановлення обов'язкового

людського контролю – жодне процесуальне рішення не може ґрунтуватися виключно на висновку ШІ.

Імплементація застосування штучного інтелекту у кримінальне провадження має відбуватись не шляхом заміни людського правосуддя певними алгоритмами, а через створення жорсткої правової рамки, яка б виключала ризики цифрової упередженості отриманих даних. Враховуючи той факт, що нейромережа не є учасником кримінального провадження і не може нести кримінальну відповідальність за завідомо неправдиві показання, її висновки мають сприйматися судом виключно як складна технічна документація, що потребує обов'язкового роз'яснення експерта відповідної галузі знань. Тільки через висновок експерта (ст. 101 КПК) можна інтерпретувати дані, отримані штучним інтелектом. Експерт, використовуючи спеціальні знання, проводить дослідження результатів, переводячи їх із категорії технічної інформації в категорію процесуальних доказів. При цьому, експерт бере на себе юридичну відповідальність за достовірність висновків, передбачену ст. 384 КК України, що забезпечує дотримання принципу законності.

Адаптація КПК України через введення поняття автоматизованих доказів та методик їхньої перевірки — це єдиний шлях вивести використання ШІ на рівень змагальності у кримінальному провадженні та використовувати його як один із процесуальних інструментів. Використання систем штучного інтелекту має підлягати суворому судовому та процесуальному контролю. Технічні звіти ШІ повинні проходити обов'язкову перевірку експертами, а правоохоронним органам варто використовувати алгоритми виключно для попереднього аналізу даних, уникаючи їх застосування як самостійного доказу винуватості.

Підбиваючи підсумок, варто наголосити, що технічний засіб не може замінити суддю. Штучний інтелект у кримінальному провадженні – це сучасний та потужний інструмент аналітики, що значно підвищує ефективність досудового розслідування проте, він не володіє процесуальною правосуб'єктністю і не може замінити слідчого чи суддю з моральною відповідальністю людини.

Список використаних джерел:

1. Григоренко В. М. Штучний інтелект у криміналістиці: нові горизонти. Юридичний часопис. 2023. Т. 12. С. 110-115.

2. Михайленко В. В. Цифрові докази в кримінальному процесі: теорія та практика застосування. Юридичний радник. 2022. № 4. С. 47.

3. Sartor G., Lagioia F. The impact of algorithms on fundamental rights and European case law. European Parliament Research Service. 2020. С. 42

Кутаєв С.В.
старший викладач кафедри інформаційних технологій
(Львівський державний університет внутрішніх справ)

КІБЕРБЕЗПЕКА ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У СИСТЕМАХ ШІ

Сучасна трансформація правової системи України неможлива без інтеграції інструментів штучного інтелекту (далі – ШІ). Проте, швидкість технологічного прогресу значно випереджає розвиток механізмів кіберзахисту. В умовах гібридної агресії та масових цифрових атак, питання захисту конфіденційної інформації стає не просто юридичним обов'язком, а складником національної безпеки. Як зазначається у «Білій книзі з питань регулювання ШІ в Україні», створення безпечного середовища для інновацій є пріоритетом держави на найближчі роки [1]. Серед основних загроз персональним даним у системах ШІ доцільно виокремити такі:

1. Технічні вразливості ШІ-систем у правовій сфері. Системи ШІ, що використовуються у LegalTech (аналіз судових рішень, підготовка позовів), є об'єктами специфічних кібератак, які відрізняються від традиційного зламу баз даних:

- Інверсія моделі та атаки на вилучення (Extraction Attacks): Дослідження показують, що зловмисники можуть «допитати» нейромережу так, щоб вона видала фрагменти персональних даних, на яких її навчали [2].

- Отруєння даних (Data Poisoning): Якщо ШІ-модель автоматично збирає дані з відкритих реєстрів, існує ризик внесення туди фальсифікованої інформації для викривлення майбутніх юридичних висновків.

- Prompt Injection (Ін'єкція запитів): Маніпуляція алгоритмом через спеціально сформовані текстові команди, що дозволяє обійти фільтри конфіденційності.

2. Масштабний витік даних та ризики агрегації через ШІ. Нещодавній інцидент, коли в мережі опинилися персональні дані понад 20 мільйонів українців [3], продемонстрував критичну вразливість державних реєстрів. Проблема посилюється з появою ШІ, оскільки:

- Алгоритми здатні проводити «дереактивізацію» анонімних даних, зіставляючи різні витоки.

- ШІ автоматизує створення фішингових повідомлень, використовуючи деталі з вкрадених баз, що робить їх практично невідрізняними від офіційних звернень суду чи держорганів. Це прямо порушує базові принципи, закладені в Законі України «Про захист персональних даних» [4].

Для мінімізації ризиків, описаних у міжнародних стандартах кібербезпеки ШІ [5], необхідно впроваджувати такі технічні підходи:

- Federated Learning (Федеративне навчання): Дані залишаються на локальних серверах юридичних фірм або судів, а центральна модель лише збирає «досвід» без копіювання самих документів.

- Диференційна приватність: Математичне зашумлення вибірки, що не дає змогу ідентифікувати конкретну особу у звіті ШІ.

- On-premise deployment: Відмова від використання публічних хмарних сервісів (як-от ChatGPT) на користь розгортання локальних моделей (Llama 3, Mistral) всередині захищеного периметра організації.

Процес гармонізації національного законодавства з правовим полем Європейського Союзу зумовлює необхідність впровадження системних стандартів регулювання новітніх технологій, зокрема у сфері правоохоронної діяльності та судочинства. Пріоритетним завданням для України в цьому контексті є адаптація європейських безпекових протоколів, що базуються на ризик-орієнтованому підході до використання інструментів штучного інтелекту. Орієнтиром для України є Регламент (ЄС) 2024/1689 (EU AI Act) [6]. Згідно з цим актом, системи ШІ, що застосовуються у правосудді, належать до категорії високого ризику. ля нівелювання зазначених ризиків та забезпечення етичного впровадження технологій штучного інтелекту в правову систему, критично важливим є формування комплексної системи запобіжників. Реалізація цього підходу передбачає дотримання низки обов’язкових вимог:

- Належне управління даними (Data Governance): забезпечення високої якості, репрезентативності та актуальності

масивів даних, що використовуються для навчання алгоритмів, з метою недопущення упередженості та дискримінації.

- Системне логування (Logging): запровадження механізмів безперервної реєстрації всіх дій та процесів системи, що є необхідною умовою для проведення подальшого аудиту та верифікації прийнятих рішень.

- Забезпечення людського нагляду (Human-oversight): обов'язкове залучення кваліфікованого фахівця до процесу контролю за роботою алгоритму, що гарантує неможливість прийняття остаточного процесуального рішення виключно автоматизованою системою без участі людини.

Захист персональних даних у системах ШІ вимагає комплексного підходу: від суворого дотримання стандартів ISO/IEC 42001:2023 [5] до імплементації норм європейського права [6, 7]. Тільки технічно захищений та етично налаштований ШІ зможе стати надійною опорою для українського правосуддя, не створюючи при цьому загрози приватності громадян.

Список використаних джерел:

1. Біла книга з питань регулювання штучного інтелекту в Україні. Міністерство цифрової трансформації України. Київ, 2024. 30 с.

2. Goodfellow I., Bengio Y., Courville A. Deep Learning. MIT Press, 2016. 800 p. (Chapter 20: Security and Privacy in AI).

3. У мережі опинилися персональні дані понад 20 мільйонів українців : веб-сайт. URL: https://suspilne.media/1120080-u-merezi-opinilisa-personalni-dani-ponad-20-miljoniv-ukrainciv-nardep/ (дата звернення: 06.03.2026).

4. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481.

5. ISO/IEC 42001:2023. Information technology – Artificial intelligence – Management system. International Organization for Standardization, 2023. 54 p.

6. Про штучний інтелект (Акт про штучний інтелект) : Регламент (ЄС) 2024/1689 Європейського Парламенту та Ради від

13 черв. 2024 р. *Official Journal of the European Union*. 2024. L series. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689 (дата звернення: 06.03.2026).

7. Штучний інтелект у правосудді: огляд міжнародного досвіду та виклики для України / Центр демократії та верховенства права (CEDEM). Київ, 2023. 42 с.

Левченко Т.І.
курсант навчально-наукового інституту
поліцейської діяльності
(Національна академія внутрішніх справ)

РОЗСЛІДУВАННЯ ЗЛОЧИНІВ ШЛЯХОМ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

У сучасних умовах стрімкого розвитку інформаційних технологій та цифровізації суспільства значно зростає роль інноваційних інструментів у сфері протидії злочинності. Одним із таких інструментів є штучний інтелект, який поступово інтегрується у діяльність правоохоронних органів різних держав. Використання штучного інтелекту під час розслідування злочинів відкриває нові можливості для аналізу великих масивів інформації, підвищення ефективності кримінального провадження та швидкого виявлення злочинців. У зв'язку з цим питання застосування штучного інтелекту в криміналістиці та правоохоронній діяльності набуває особливої актуальності.

Штучний інтелект являє собою сукупність технологій і програмних рішень, здатних імітувати інтелектуальну діяльність людини, зокрема аналіз інформації, навчання на основі даних, розпізнавання образів та прийняття рішень. У сфері кримінального правосуддя такі системи можуть використовуватися для автоматизованого аналізу доказів, обробки великих обсягів цифрової інформації, прогнозування кримінальних ризиків та ідентифікації осіб, причетних до злочинів. Застосування штучного інтелекту сприяє підвищенню ефективності розслідування, оскільки дозволяє швидше встановлювати зв'язки між фактами та подіями, що мають значення для кримінального провадження [1].

Однією з сфер використання штучного інтелекту під час розслідування злочинів є аналіз великих масивів даних. Сучасні кримінальні провадження часто пов'язані з опрацюванням значної кількості інформації: електронних листів, повідомлень у соціальних мережах, фінансових операцій, записів з камер відеоспостереження та інших цифрових джерел. Людині складно швидко та ефективно опрацювати такий обсяг інформації, тоді як алгоритми штучного інтелекту здатні аналізувати тисячі

документів і записів за короткий час, виявляючи підозрілі зв'язки або закономірності.

Важливим напрямом застосування штучного інтелекту є розпізнавання облич та інших біометричних даних. Системи автоматичного розпізнавання можуть аналізувати відеозаписи з камер спостереження, фотографії або інші цифрові зображення для встановлення особи підозрюваного. Такі технології активно використовуються правоохоронними органами багатьох країн світу та дозволяють значно пришвидшити процес ідентифікації осіб, причетних до злочинів. Разом із тим застосування подібних технологій потребує чіткого правового регулювання, оскільки існує ризик порушення права людини на приватність та захист персональних даних [2].

Ще одним перспективним напрямом використання штучного інтелекту є прогнозування злочинності. Завдяки аналізу статистичних даних, інформації про попередні правопорушення, соціально-економічних факторів та інших показників алгоритми можуть визначати території або ситуації з підвищеним ризиком вчинення злочинів. Це дає змогу правоохоронним органам ефективніше планувати свою діяльність, спрямовувати ресурси у найбільш проблемні регіони та запобігати правопорушенням ще до їх вчинення.

У криміналістиці штучний інтелект також використовується для автоматизації експертних досліджень. Наприклад, спеціальні програмні комплекси здатні аналізувати почерк, відбитки пальців, балістичні характеристики зброї або інші сліди злочину. Завдяки машинному навчанню такі системи поступово вдосконалюються та можуть забезпечувати високий рівень точності результатів. Це сприяє підвищенню об'єктивності експертних досліджень та зменшенню ймовірності помилок під час проведення криміналістичних експертиз [3].

Разом з тим використання штучного інтелекту під час розслідування злочинів має не лише переваги, але й певні ризики та проблеми. По-перше, існує небезпека технічних помилок або некоректної роботи алгоритмів, що може призвести до неправильних висновків або необґрунтованих підозр. По-друге, важливим є питання відповідальності за рішення, прийняті із застосуванням автоматизованих систем.

Для України питання використання штучного інтелекту у сфері розслідування злочинів також набуває дедалі більшої актуальності. У сучасних умовах зростає кількість кіберзлочинів, фінансових правопорушень, а також злочинів, пов'язаних із використанням інформаційних технологій. Тому впровадження сучасних аналітичних систем та алгоритмів машинного навчання може суттєво підвищити ефективність діяльності правоохоронних органів, сприяти швидкому виявленню злочинців та забезпечити належний рівень доказової бази у кримінальних провадженнях.

Отже, штучний інтелект стає інструментом у процесі розслідування злочинів та боротьби зі злочинністю загалом. Його застосування дозволяє значно підвищити ефективність аналізу інформації, автоматизувати окремі етапи кримінального провадження та сприяти швидкому встановленню обставин вчинення правопорушень. Водночас впровадження таких технологій повинно здійснюватися з урахуванням принципів законності, захисту прав людини та етичних стандартів. Лише за умови належного правового регулювання та контролю використання штучного інтелекту може стати ефективним інструментом забезпечення правопорядку та справедливості у сучасному суспільстві.

Список використаних джерел:

1. Атаманенко Ю.Ю. Інноваційні технології в діяльності поліцейських підрозділів України. URL: https://dnuvs.ukr.education/wpcontent/uploads/2023/06/zbirnyk_mnpk_bezpeka_na_dorozi_18_05_2023.pdf (дата звернення: 11.03.2026).

2. Баловсяк Н. Справжній робокоп: як використовують ШІ для розкриття злочинів. robot_dreams - онлайн-курси для фахівців у сфері big data, machine learning, data science | Робот Дрімс. URL: https://robotdreams.cc/uk/blog/362-spravzhniy-robokop-yak-vikoristovuyut-shi-dlyarozkrittya-zlochiniv (дата звернення: 11.03.2026).

3. Європарламент схвалив план регулювання штучного інтелекту. Суспільне | Новини. URL: https://suspilne.media/507905-evroparlament-shvalivplan-reguluvanna-stucnogo-intelektu/ (дата звернення: 11.03.2026).

Лепей С.
здобувач вищої освіти факультету № 1
(Львівський державний університет внутрішніх справ)
Гуцуляк Ю.В.
доцент кафедри кримінального процесу
та криміналістики факультету № 1, доктор філософії
(Львівський державний університет внутрішніх справ)

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ OSINT З КОЛАБОРАЦІЄЮ ЗІ ШІ У КРИМІНАЛЬНОМУ ПРОЦЕСІ

OSINT (Open Source Intelligence) – це новітній метод, який використовується для збору та обробки інформації у сфері оборони, безпеки та розслідування з відкритих джерел уповноваженими державними органами, і не передбачає дотримання додаткових гарантій забезпечення прав учасників правовідносин. Оскільки, це відносно новий метод як для України так і для європейських країн, тому існує потреба у його дослідженні та пошук прогалин, що існують в цій сфері з огляду на відсутність єдиного підходу до процесуального статусу інформації, отриманої з відкритих джерел [1, с. 21].

Стрімкий розвиток цифрових технологій, соціальних мереж, онлайн-платформ та супутникових сервісів суттєво розширює можливості органів досудового розслідування щодо встановлення обставин кримінального правопорушення, водночас породжуючи низку проблем, пов'язаних із допустимістю, належністю та достовірністю таких доказів у кримінальному провадженні. Найчастіше саме цей метод використовується при розслідуванні кримінальних правопорушень проти основ національної безпеки, громадського порядку та безпеки, корупційних та кібер злочинів.

В епоху цифрових технологій, коли інформація стає доступною з різних джерел, використання OSINT інструментарію набуває важливого значення при розслідуванні кримінальних правопорушень. Слід зазначити, що (OSINT) – це процес збору,аналізу і використання інформації, яка відкрито доступна. Ця інформація може бути отримана з різних джерел, таких як:

вебсайти, соціальні мережі, публічні бази даних, новинні ресурси,блоги тощо. Основна мета OSINT – зібрати релевантну інформацію для подальшого аналізу і прийняття рішень. Цей підхід застосовується в різних сферах, включаючи правоохоронну діяльність, розвідку, бізнес-аналітику, кібербезпеку та ін. В сучасних умовах, коли велика кількість інформації публікується онлайн, OSINT стає важливим інструментом для здійснення різних видів аналізу та досліджень, у тому числі і при розслідуванні кримінальних правопорушень проти власності.

Найбільш поширеними та ефективними цифровими OSINT, на наш погляд є:

- Maltego - це інструмент аналітики з відкритим вихідним кодом і графічного аналізу посилань для збору і зв'язку інформації для дослідницьких завдань;

- SpiderFoot – інструмент для професіоналів, які хочуть автоматизувати OSINT для аналізу загроз, виявлення активів, моніторингу поверхні атаки або оцінки безпеки;

- Creepy - інструмент геолокації з відкритим вихідним кодом. Він збирає інформацію про геолокації за допомогою різних платформ соціальних мереж і послуг хостингу зображень, які вже опубліковані десь ще [2].

Цей список не є вичерпним, але це найпопулярніше програмне забезпечення для збору інформації.

Пошук за фотографіями чи зображеннями, стало актуальним з появою великої кількості камер відео спостереження та таких систем як «Безпечне місто». Для того щоб дізнатися, де використовувалося зображення або де воно з'явилося вперше, використовуйте пошук по зображеннях. Він є в основних пошукових системах, таких як Google Images, Bing Images, Baidu Images. Також варто скористатися сервісом TinEye, чиї алгоритми відрізняються від Google. Пошук за зображеннях є і в соціальних мережах: Findclone і Findmevk.com. Крім цього існують спеціалізовані плагіни - RevEye для Chrome, Image Search Options для Firefox. Мобільні додатки на зразок CamFind можуть впізнати речі з реального світу. А Image Identification Project використовує для цього штучний інтелект. Якщо зображення містить EXIF-дані (інформацію про камеру, геокоординати, режиму зйомки і т.п.), то варто їх проаналізувати. Побачити (і змінити) їх можна за

допомогою будь-якого редактора зображень або невеликої програми Exiftool. Є також схожі онлайн-сервіси: exifdata.com і viewexifdata.com. Видалити EXIFдані можна за допомогою exifpurge.com або verexif.com. Інший ресурс, stolencamerafinder.com, визначає камеру за серійним номером і шукає в інтернеті, які ще фото були зроблені нею. Перевірити зображення на предмет монтажу та інші маніпуляції можна за допомогою Forensically або FotoForensics [3, с. 139].

Корисним може бути OSINT при розслідуванні корупційних правопорушень або будь-яких форм фінансового чи економічного шахрайства. У даному випадку ці категорії кримінальних правопорушень поєднуються тим, що при їхньому розслідуванні можуть застосовуватися однакові відкриті джерела, адже досить часто дані правопорушення доповнюють одне одного.

Спеціалісти Bellingcat на прикладах демонструють, яким чином можна використовувати відкриті джерела для виявлення прикладів корупції.

До таких прикладів відносяться:

– поява політиків на публіці в дороговартісних коштовностях, годинниках тощо (які легко ідентифікувати за зображенням та визначити їхню реальну вартість, в подальшому порівнявши її з деклараціями таких осіб чи іншими даними про їхні статки);

– користування соціальними мережами дітей чи інших родичів корумпованих політиків, які хваляться своїми статками, публікуючи фотографії в дорогих авто чи будинках (наявні численні приклади, коли такі особи, особливо молодшого віку, самі в коментарях на власні дописи відповідають на питання підписників щодо місця чи часу, коли було зроблено фото, чим ще більше полегшують роботу аналітиків);

– пошук за базами даних. Наприклад, на сайті https://id.occrp. можна знайти посилання на сотні онлайн ресурсів у залежності від регіону, країни або сфери, яка вас цікавить.

При розслідуванні воєнних злочинів OSINT найяскравіше проявляються саме в процесі ідентифікації та розслідування воєнних злочинів, адже значна кількість порушень МГП, які в подальшому кваліфікуються як воєнні злочини, зачіпають невизначене або дуже широке коло осіб, а їхні наслідки дуже

складно приховати. При цьому необхідно зазначити, що не існує окремих спеціальних методів розслідування з використанням відкритих джерел, які б стосувалися виключно воєнних злочинів. У процесі розслідування такого роду правопорушень будуть корисними всі раніше здобуті знання та навички, які в тій чи іншій мірі дозволяють користуватися відкритими джерелами задля, наприклад, ідентифікації місцевості чи осіб, які зображені на фото чи фігурують у відео. Власне, розрізняють пасивні та активні методи проведення розслідування воєнних злочинів з допомогою відкритих джерел.

Пасивні методи дозволяють отримувати загальну інформацію про об'єкт. Вона збирається вручну або за допомогою спеціальних сервісів та інструментів, що спрощують збір, систематизацію та аналіз даних. Наприклад, програм для парсингу сайтів. По суті, пасивною веброзвідкою можуть займатися абсолютно всі, хто має комп'ютер і доступ в інтернет, — від простого користувача до співробітника аналітичного або маркетингового відділу.

До пасивних методів можна віднести:

– збирання інформації (у тому числі за фотографіями) з відкритих пошукових систем; – аналіз активності користувача в соціальних мережах і блогах, на форумах, інших віртуальних платформах;

– пошук відкритих персональних даних користувачів у соціальних мережах, месенджерах;

– перегляд збережених копій сайтів у пошукових системах, інтернет-архіві;

– отримання геолокаційних даних за допомогою загальнодоступних ресурсів, таких як Google Maps.

Активні методи. Такі методи мають на увазі безпосередній вплив аналітика на досліджуваний об'єкт, використання спеціалізованих засобів отримання даних або здійснення дій, що вимагають певних зусиль, наприклад:

– збір даних на закритих ресурсах, доступ до яких можливий лише за передплатою;

– застосування спеціалізованих сервісів та програм, які активно впливають на досліджуваний об'єкт – наприклад, автоматично реєструються на сайті;

– використання сервісів, що сканують програми, файли чи сайти на наявність шкідливого коду;

– створення підроблених вебресурсів, каналів у месенджерах, які збирають дані користувачів, конфіденційні чи секретні відомості [4].

Отже, OSINT є важливим та перспективним інструментом у розслідуванні кримінальних правопорушень в умовах цифровізації суспільства та зростання обсягів відкритої інформації. Його застосування суттєво розширює можливості органів досудового розслідування, зокрема у справах щодо національної безпеки, корупції, кібер- та воєнних злочинів. Водночас відсутність єдиного законодавчо закріпленого підходу до процесуального статусу інформації з відкритих джерел зумовлює проблеми її допустимості та доказового значення. Це обумовлює необхідність подальших наукових досліджень і вдосконалення правового регулювання використання OSINT у кримінальному провадженні.

Список використаних джерел:

1. OSINT Open Source Intelligence. Інструменти та методи: навчальний посібник / Користін О., Демедюк С., Ісмайлов К., Ланде Д. та ін., за заг. ред. Користіна О.Є., Демедюка С.В. – Київ: 7БЦ, 2025. 460 с. URL: https://aord.com.ua/cms/uploads/OSINT_Open_Source_Intelligence_Instrumenti_ta_metodi_31913d17f8.pdf (дата звернення: 15.02.2026).

2. «Чорний» ринок даних і розвідка для чайників. URL: https://www.epravda.com.ua/columns/2020/12/30/669656/ (дата звернення: 15.02.2026).

3. Михайлов В. О. Питання використання методів OSINT у криміналістиці. DICTUM FACTUM. № 2(10), 2021. С. 139. URL: https://df.duit.in.ua/index.php/dictum/article/view/207/184 (дата звернення: 15.02.2026).

4. Торбас О.О. OSINT при розслідуванні кримінальних правопорушень : підручник / О.О. Торбас. – Одеса : Видавництво «Юридика», 2024. 180 с. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/106c5467-2afb-4055-a0fb-3a500102db9c/content

Лисюк А.М.
курсант
(Харківський національний університет внутрішніх справ)
Пчеліна О.В.
професор кафедри кримінального процесу
та організації досудового слідства,
доктор юридичних наук, професор
(Харківський національний університет внутрішніх справ)

ВИКОРИСТАННЯ ШІ ДЛЯ АНАЛІЗУ СУПУТНИКОВИХ ЗНІМКІВ ЯК ДОКАЗІВ У МІЖНАРОДНОМУ КРИМІНАЛЬНОМУ СУДІ

Застосування штучного інтелекту (далі – ШІ) для аналізу супутникових знімків у діяльності Міжнародного кримінального суду (далі – МКС) є одним із найсучасніших підходів дистанційного документування злочинів, передбачених Римським статутом. В умовах збройних конфліктів, коли фізичний доступ слідчих до місць учинення злочинів обмежений або неможливий, супутниковий моніторинг стає особливо цінним джерелом інформації. ШІ у цьому контексті виконує роль високоточного аналітика, здатного обробляти масиви геопросторових даних, які людське око не в змозі осягнути в повному обсязі. Проте статус таких даних як доказів у міжнародному кримінальному процесі вимагає неухильного дотримання стандартів автентичності та наукової обґрунтованості, що і становить основний фокус сучасних правових дискусій.

Як указує В.С. Коваленко, супутникові дані – це інформація, отримана через супутники, яка використовується для моніторингу стану Землі, її поверхні, кліматичних умов, а також для дослідження природних і антропогенних явищ [1, с. 6]. В умовах розвитку технологій особливого значення набувають способи отримання супутникових даних і методи їхнього оброблення й аналізу. Саме тут провідну роль відіграють інструменти ШІ, які забезпечують якісно новий рівень ефективності використання зазначеної інформації у кримінальних провадженнях. Зокрема, ключовим технічним методом, що застосовується ШІ, є

автоматизоване виявлення змін (Change Detection). Алгоритми глибокого навчання (Deep Learning) через аналіз великих масивів даних порівнюють архівні та актуальні знімки однієї локації, що дозволяє виявляти приховані закономірності, фіксуючи появу нових об'єктів або руйнування існуючих [2, с. 82]. Для МКС це має критичне значення при доведенні нападів на цивільну інфраструктуру. ШІ здатен автоматично розпізнавати специфічні образи воєнних злочинів. Наприклад, ШІ може розпізнавати військову техніку, фортифікаційні споруди та сліди переміщення груп осіб, що вказують на вчинення злочину, що допомагає ідентифікувати підозрюваних та зіставляти їх з наявними доказами [3, с. 128]. Використання мультиспектрального аналізу дозволяє ШІ «бачити» крізь дим або хмари, що забезпечує безперервність моніторингу зон ведення бойових дій.

Процесуальний порядок застосування супутникових даних базується на нормах статті 69 Римського статуту МКС [4], згідно з якими Суд приймає будь-які докази, що мають суттєве значення для справи. Проте ключовою проблемою є верифікація алгоритмів ШІ, оскільки захист, посилаючись на статтю 67 Римського статуту [4], може заявляти про похибки піксельного аналізу та помилкову ідентифікацію об'єктів. Для запобігання цьому застосовується стандарт «підтверджувальних доказів» (corroboration), що вимагає зіставлення результатів ШІ з перехопленнями радіомовлення, даними OSINT та показаннями свідків. Також МКС вимагає надання технічної документації про архітектуру моделі ШІ для виключення цифрових маніпуляцій (pixel-tampering) або штучного внесення об'єктів у кадр, що відповідає принципам автентичності електронних документів, передбаченим статтею 99 КПК України [5].

Особлива увага приділяється методу «цифрової тріангуляції». Це процес, за якого ШІ об'єднує супутниковий знімок із відеозаписами з мобільних телефонів, що мають GPS-мітки. Якщо супутник зафіксував проліт ракети, а ШІ синхронізував цей час із відео вибуху на землі, такий ланцюжок доказів стає майже неспростовним. МКС активно впроваджує стандарти протоколу Берклі, адже це перший набір глобальних керівних положень щодо використання цифрових даних, які є у відкритому доступі, як доказів у міжнародних розслідуваннях

щодо порушень прав людини. Цей документ містить стандарти знаходження, збирання, зберігання, перевірки та аналізу контенту із соцмереж та інших відкритих джерел [6]. Протокол Берклі вимагає збереження метаданих супутникових знімків у незмінному вигляді. ШІ також допомагає у визначенні «наміру», через аналіз динаміки руйнувань може показати, що обстріли велися цілеспрямовано по цивільних кварталах, а не були випадковими помилками під час ударів по військових цілях. Це важливий елемент для висунення обвинувачень вищому військовому керівництву держави-агресора.

Отже, ШІ у поєднанні із супутниковою розвідкою став «цифровим очевидцем», якого неможливо залякати чи підкупити. Для МКС це знаменує якісно новий рівень доказування, заснований на об'єктивних, верифікованих і науково обґрунтованих даних, що особливо важливо у контексті розслідування злочинів, передбачених Римським статутом. Водночас юридична спільнота стоїть перед необхідністю вироблення чіткого й прозорого регламенту перевірки та верифікації ШІ-моделей, які використовуються для аналізу супутникових знімків, із метою мінімізації ризиків похибок і забезпечення дотримання фундаментального права обвинуваченого на справедливий судовий розгляд. Особливого значення набуває впровадження стандарту «підтверджувальних доказів» (corroboration), що передбачає обов'язкове зіставлення результатів ШІ з іншими джерелами інформації, такими як дані OSINT, перехоплення радіопереговорів, показання свідків, а також збереження метаданих супутникових знімків у незмінному вигляді.

Подальший розвиток міжнародного кримінального правосуддя безпосередньо залежить від здатності гармонізувати стрімкий технологічний прогрес із незмінними засадами верховенства права, а також принципами автентичності, наукової обґрунтованості та презумпції невинуватості. У цьому контексті ШІ має розглядатися винятково як інструмент для встановлення обставин, що підлягають доказуванню та мають значення для кримінального провадження, а не як самостійний чи автоматичний суб'єкт ухвалення рішень. Використання Україною можливостей ШІ для збору й аналізу супутникових доказів у справах проти рф у

МКС є стратегічно важливим кроком, що дозволяє фіксувати кожен випадок агресії з максимальною точністю.

Список використаних джерел:

1. Коваленко В.С. Розробка прикладного програмного інтерфейса (API) для систематизації супутникових даних = Development of an application program interface (API) for systematization of satellite data: кваліфікаційна робота магістра. Одеса, 2024. 55 с. URL: https://dspace.onu.edu.ua/server/api/core/bitstreams/a9651c3e-bb79-45e0-b869-23de9e6356d2/content .

2. Удовенко Ж.В., Галаган В.І., Шкелебей В.А. Використання штучного інтелекту у кримінальному провадженні під час дії воєнного стану. *Право і безпека*. 2025. № 3 (98). С. 78–90. URL: https://pb.univd.edu.ua/index.php/PB/article/view/883/721.

3. Орлов В. Застосування штучного інтелекту у розслідуванні воєнних злочинів. *Протидія кримінальним правопорушенням на деокупованих територіях*: збірник матеріалів Всеукраїнської науково-практичної конференції (в авторській редакції), (м. Кропивницький, 27 жовтня 2023 року). Кропивницький, 2023. С. 127-129. URL: https://www.researchgate.net/publication/377263353_Zastosuvanna_stucnogo_intelektu_u_rozsliduvanni_voennih_zlociniv.

4. Римський Статут Міжнародного Кримінального Суду: Статут Міжнародного суду від 17.07.1998 № 995_588. URL: https://zakon.rada.gov.ua/laws/card/995_588.

5. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/card/4651-17.

6. Протокол Берклі щодо розслідування із використанням відкритих цифрових даних. Юрфем. URL: https://surl.li/akzjrt.

Лісніченко Д.В.
доцент кафедри кримінального
процесу та криміналістики,
кандидат юридичних наук, доцент
(Одеський державний університет внутрішніх справ)

ЦИФРОВІ ДОКАЗИ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ: ПРОЦЕСУАЛЬНІ АСПЕКТИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ЇХ АНАЛІЗУ

Стрімка цифровізація суспільних відносин зумовила якісну зміну доказової бази у кримінальному провадженні. Значний масив відомостей, що мають значення для встановлення обставин кримінального правопорушення, нині існує в електронній формі: у вигляді електронних документів, листування в месенджерах, фото- і відеофайлів, метаданих, відомостей із соціальних мереж, навігаційних систем, мобільних пристроїв та інших цифрових джерел. Це актуалізує питання не лише технічного вилучення й збереження таких відомостей, а й їх належної процесуальної інтерпретації та оцінки.

В сучасній доктрині цифрові докази розглядаються як специфічний різновид інформації, зафіксованої в електронному середовищі та здатної підтверджувати або спростовувати обставини, що входять до предмета доказування [1; 2]. Їх особливість полягає у високій динамічності, здатності до швидкого копіювання, модифікації, видалення або маскування. Саме тому ключового значення набувають питання автентичності, цілісності, простежуваності походження та дотримання процедури отримання таких даних.

Нормативне підґрунтя використання цифрових доказів у кримінальному провадженні України формується насамперед положеннями ст. 84, 99, 100 КПК України, які дають змогу розглядати електронні носії та електронні документи як джерела доказової інформації [3]. Водночас чинне кримінальне процесуальне законодавство не містить розгорнутого визначення цифрових доказів і не встановлює вичерпного алгоритму їх фіксації, перевірки та оцінки. Така нормативна неповнота

ускладнює уніфіковане правозастосування та зумовлює потребу у виробленні належних методичних стандартів.

У цьому контексті штучний інтелект поступово перетворюється на важливий допоміжний інструмент аналізу цифрових даних. Алгоритми машинного навчання здатні обробляти великі масиви різнорідної інформації, автоматично класифікувати файли, виявляти зв'язки між окремими цифровими об'єктами, встановлювати повторювані патерни поведінки, а також ідентифікувати потенційно релевантні дані для потреб досудового розслідування і судового розгляду [4; 5]. Особливого значення це набуває в умовах документування воєнних злочинів, коли значна частина доказової інформації походить із відкритих джерел, мобільних пристроїв, камер спостереження, супутникових знімків і цифрових платформ.

Практична цінність таких технологій виявляється у декількох напрямах. По-перше, системи комп'ютерного зору можуть застосовуватися для аналізу зображень і відеозаписів, розпізнавання об'єктів, локалізації місця події та виявлення ознак монтажу. По-друге, інструменти аналітики метаданих дають змогу відтворювати хронологію подій, перевіряти час і місце створення файлів, зіставляти джерела походження інформації. По-третє, інтелектуальні пошукові модулі дозволяють швидше відбирати релевантні матеріали з великих масивів даних, що істотно підвищує ефективність кримінального аналізу [2; 6].

Разом із тим використання штучного інтелекту у сфері доказування не може розглядатися як самодостатня гарантія достовірності результату. Автоматизований аналіз пов'язаний із ризиками похибок алгоритму, недостатньої прозорості його роботи, упередженості навчальних вибірок, а також складності перевірки відтворюваності отриманих висновків. З огляду на це результати, сформовані за допомогою систем штучного інтелекту, мають оцінюватися не ізольовано, а в сукупності з іншими доказами та з урахуванням джерела походження даних, способу їх отримання і процесуальної форми фіксації.

Принципово важливо, щоб застосування технологій штучного інтелекту не підміняло внутрішнє переконання слідчого, прокурора чи суду. Такі системи повинні виконувати допоміжну, а не вирішальну функцію. Остаточне рішення щодо належності, допустимості, достовірності та достатності доказів має залишатися

за уповноваженим суб'єктом кримінального провадження. Відтак одним із перспективних напрямів розвитку кримінального процесу є нормативне врегулювання критеріїв використання інструментів штучного інтелекту під час роботи з цифровими доказами, а також підготовка фахівців, здатних одночасно оцінювати як технічні, так і процесуально-правові аспекти цифрової інформації.

Отже, цифрові докази дедалі виразніше формують нову конфігурацію доказування у кримінальному провадженні, а штучний інтелект створює додаткові можливості для їх систематизації, перевірки та аналітичного опрацювання. Проте ефективність такого підходу безпосередньо залежить від поєднання технологічних рішень із процесуальними гарантіями, вимогами допустимості доказів і принципом судового контролю за результатами їх використання.

Список використаних джерел:

1. Casey E. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. 4th ed. London : Academic Press, 2020. 864 p. URL: https://rishikeshpansare.wordpress.com/wp-content/uploads/2016/02/digital-evidence-and-computer-crime-third-edition.pdf

2. Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence (CETS No. 224) (2022) URL: https://www.coe.int/en/web/cybercrime/second-additional-protocol

3. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI. URL: http://zakon4.rada.gov.ua/lams/show/4651-17

4. Eurojust. *SIRIUS EU Electronic Evidence Situation Report 2023 5th Annual Report*. URL: https://www.eurojust.europa.eu/publication/sirius-eu-electronic-evidence-situation-report-2023

5. Kermode L., Freyberg J., Akturk A. et al. *Objects of Violence: Synthetic Data for Practical Machine Learning in Human Rights Investigations*. arXiv. 2020. URL: https://arxiv.org/pdf/2004.01030

6. Khan S., Furuly J., Vold H., Tahseen R., Dang-Nguyen D. *Online Multimedia Verification with Computational Tools and OSINT*. arXiv. 2023. URL: https://arxiv.org/pdf/2310.01978

Лісник Р.І.
курсант факультету № 1
(Львівський державний університет внутрішніх справ)
Гуцуляк Ю.В.
доцент кафедри кримінального процесу
та криміналістики факультету № 1
доктор філософії права
(Львівський державний університет внутрішніх справ)

ВПРОВАДЖЕННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ НА ОСНОВІ ШТУЧНОГО ІНТЕЛЕКТУ ЗАДЛЯ ЗАПОБІГАННЯ ЗЛОВЖИВАНЬ ПРОЦЕСУАЛЬНИМИ ПРАВАМИ У ВИГЛЯДІ ПОДАННЯ ОДИНАКОВИХ ЗА ЗМІСТОМ КЛОПОТАНЬ З МЕТОЮ ЗАТЯГУВАННЯ СУДОВОГО РОЗГЛЯДУ

Штучний інтелект, машинне та глибоке навчання в останні роки набули значної популярності, що зумовлено розвитком обчислювальних потужностей і стрімким приростом хмарних технологій, які відкрили можливість створення ШІ, здатного виконувати вражаючі завдання - від написання статей до перемог у художніх конкурсах. Такий розвиток спонукає суспільство замислюватися над реальними можливостями новітніх технологій і шляхами їх практичного використання.

У контексті діджиталізації державного апарату судова гілка влади також не стане винятком, адже впровадження автоматизованих програм у систему правосуддя може суттєво розвантажити рутинну роботу з процесуальними документами та делегувати окремі повноваження програмному забезпеченню.

Безпосередня роль запропонованого інноваційного рішення полягає у превентивному та організаційному забезпеченні належного перебігу судового розгляду шляхом своєчасного виявлення однакових або змістовно тотожних клопотань і заяв, подання яких може бути спрямоване не на реалізацію права на захист, а на безпідставне ускладнення та затягування провадження. У такому аспекті її призначення зводиться не лише до полегшення роботи суду з великим обсягом процесуальної

документації, а й до підтримання оперативності розгляду справ, дотримання розумних строків та зміцнення процесуальної дисципліни учасників провадження. Відтак практична цінність такої системи вбачається у тому, що вона виступає допоміжним інструментом для своєчасного реагування на можливі прояви зловживання процесуальними правами, сприяє більш впорядкованому здійсненню судового контролю та створює умови для підвищення загальної ефективності судочинства.

Основним питанням розробки стоїть не лише коректний вибір мови програмування та архітектури моделі, а й належним налаштуванням її параметрів, оскільки саме від цього залежить точність розпізнавання змістовно тотожних документів, стійкість роботи системи та практична придатність отриманих результатів для потреб судового провадження. Найважливішим елементом у рамках встановлення меж діяльності програми, її задач та загалом способу встановлення цих рамок є мова програмування, вибір якої у даному випадку є цілком обґрунтованим. Застосування мови програмування Python є ефективним саме тому, що дана мова вважається однією з найбільш пристосованих для розробки рішень на основі штучного інтелекту завдяки простоті синтаксису, легкій для перегляду структурі та величезному переліку екосистем бібліотек, що дозволяє швидко писати, тестувати й удосконалювати код, не витрачаючи зайвий час на складнощі, пов’язані із самою мовою. У межах запропонованої ідеї це має особливе значення, оскільки основний акцент переноситься не на технічні труднощі програмування, а на логіку моделі, обробку текстів клопотань, очищення даних, токенізацію, побудову ембеддингів та подальше порівняння змісту документів. Додатково ефективність такого вибору посилюється використанням PyTorch, динамічної обчислювальної графи та нейронної мережі «Siamese Network», яка дає змогу створити гнучку, легко налагоджувану та адаптивну модель, що є надзвичайно важливим для завдань NLP, де в процесі розробки може виникати потреба змінювати структуру мережі, параметри навчання та окремі функціональні модулі без втрати загальної цілісності системи.

Ефективність запропонованої моделі підтверджується результатами дослідження Н. Раймерса та І. Гуревич, у якому

доведено, що сіамська архітектура є придатною для завдань семантичного зіставлення текстів і суттєво знижує обчислювальні витрати при пошуку змістовно подібних висловлювань. Зокрема представлена ними мовна модель «SBERT», на відміну від попередньої («BERT»), дозволяє не лише істотно підвищити якість семантичного зіставлення текстів, а й радикально скоротити час пошуку подібних документів: зокрема, для масиву з 10 000 речень час пошуку найбільш схожої пари було зменшено приблизно з 65 годин до 5 секунд, що прямо свідчить про її практичну придатність для задач виявлення змістовно подібних текстів [1].

Якщо у наведеному прикладі йдеться про загальне порівняння речень у широкому текстовому масиві, то в межах запропонованої нами моделі об'єкт аналізу є значно вужчим і більш формалізованим, оскільки стосується процесуальних документів зі спільною структурою, типовою лексикою та єдиним контекстом судового провадження. Саме тому використання такого підходу для виявлення однакових або близьких за змістом клопотань є не лише теоретично виправданим, а й практично більш передбачуваним за результатом, оскільки модель застосовується в межах предметно однорідного середовища, де змістова подібність піддається точнішому виявленню.

Також, такого роду розробка обґрунтована не лише з позиції технічної доцільності, а й з огляду на сучасні підходи до підвищення ефективності правосуддя, відображені у Рамковій основі Організації економічного співробітництва та розвитку (далі – ОЕСР) щодо онлайн-врегулювання спорів. Наголошено, що цифрові рішення у сфері правосуддя здатні підвищувати доступність і своєчасність вирішення правових питань, покращувати якість судових послуг, а також зменшувати загальне навантаження на судову систему та тиск на її ресурси. Окремо підкреслено, що механізми діагностики й процесуального спрямування матеріалів сприяють більш ефективному, результативному та своєчасному управлінню розглядом справ, оскільки дозволяють ідентифікувати їх характер, співвіднести із належною процедурою та уникати зайвого втручання суду там, де це можливо. У цьому контексті система виявлення ідентичних або змістовно близьких клопотань відповідає загальній логіці таких реформ, адже орієнтована на впорядкування роботи з

повторюваними процесуальними документами, своєчасне виявлення потенційно зловживальних практик та зосередження людського ресурсу суду на тих питаннях, які справді потребують повноцінної правової оцінки.

Не менш важливо, що ОЕСР прямо вказує на особливу корисність автоматизації для тих стадій провадження, де значну частину навантаження становлять повторювані дії, які не потребують складного аналітичного осмислення, а також для належного перерозподілу обмежених ресурсів системи правосуддя на більш складні завдання. Документ також підкреслює значення безперервного руху інформації та матеріалів між різними етапами й механізмами розгляду, оскільки саме така узгодженість сприяє економії часу, уникненню дублювання дій та підвищенню загальної ефективності судочинства. З огляду на це, запропонована розробка може розглядатися як інструмент раннього виявлення однотипних процесуальних звернень, який не підміняє судове вирішення питання по суті, але створює передумови для більш впорядкованого руху документів, оперативнішого реагування на спроби затягування розгляду та загального посилення процесуальної економії. Саме в такому аспекті її необхідність узгоджується з перспективами, окресленими ОЕСР: цифрові інструменти мають не просто супроводжувати правосуддя, а забезпечувати його більшу ефективність, узгодженість і раціональне використання ресурсів [2, с. 31-37].

Загалом, слід зазначити, що перспективи подальших наукових розвідок у цьому напрямі вбачаються у поглибленому дослідженні критеріїв змістовної подібності процесуальних документів, визначенні оптимальних параметрів функціонування такої системи, оцінці точності її роботи на реальному масиві судових матеріалів, а також у з'ясуванні меж її допустимого використання в контексті гарантій справедливого судового розгляду та недопущення обмеження процесуальних прав учасників провадження.

Список використаних джерел:

1. Reimers N., Gurevych I. Sentence-BERT: Sentence Embeddings using Siamese BERT-Networks [Електронний ресурс] //

Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing (EMNLP-IJCNLP). Hong Kong, China, 2019. P. 3982–3992. URL: https://arxiv.org/abs/1908.10084 (дата звернення: 05.03.2026).

2. OECD Online Dispute Resolution Framework [Electronic resource]. Paris : OECD Publishing, 2024. 65 с. URL: https://read.oecd-ilibrary.org/content/dam/oecd/en/publications/reports/2024/10/oecd-online-dispute-resolution-framework_e88b6c6a/325e6edc-en.pdf (дата звернення: 05.03.2026).

Лукащук Ю.А.
асистент кафедри
автоматизованих систем управління,
доктор філософії
(Національний університет «Львівська політехніка»)

КІБЕРБЕЗПЕКА СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ: ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У КОНТЕКСТІ ВИМОГ ЗАГАЛЬНОГО РЕГЛАМЕНТУ ПРО ЗАХИСТ ДАНИХ

Цифрова трансформація державного управління, економіки та суспільних відносин супроводжується стрімким розвитком систем штучного інтелекту (ШІ), які дедалі частіше використовуються для автоматизованого прийняття рішень, прогнозування поведінки, профілювання та аналізу великих масивів інформації. Основним ресурсом функціонування таких систем є дані, зокрема персональні. Водночас розширення сфер застосування алгоритмічних технологій зумовлює зростання ризиків порушення права на приватність, незаконної обробки інформації та несанкціонованого доступу до неї.

У праві Європейського Союзу фундаментальним актом, що визначає стандарти захисту персональних даних, є Загальний регламент про захист даних (GDPR) [1]. Його положення мають екстериторіальний характер та застосовуються до будь-яких суб'єктів, які обробляють дані громадян ЄС. З огляду на євроінтеграційний курс України, імплементація принципів GDPR у сфері використання ШІ є не лише правовим обов'язком, а й стратегічною умовою розвитку цифрової економіки.

На відміну від традиційних інформаційних систем ШІ не лише зберігає або передає інформацію, а й формує статистичні моделі на основі аналізу великих обсягів даних. Машинне навчання передбачає накопичення тренувальних вибірок, їх попередню обробку, оптимізацію параметрів та подальше використання моделі для прогнозування або класифікації.

Особливу складність становить те, що персональні дані можуть бути «вбудовані» у параметри моделі. Дослідження

доводять, що зловмисник здатен визначити, чи входили дані конкретної особи до навчальної вибірки [3], або частково відновити конфіденційну інформацію через аналіз відповідей моделі [4]. Таким чином, навіть формально знеособлені дані можуть створювати ризики повторної ідентифікації.

Крім того, алгоритмічні системи часто здійснюють профілювання суб'єктів даних, що може впливати на забезпечення та реалізацію їхніх прав та свобод. Автоматизовані рішення у сфері кредитування, працевлаштування чи правоохоронної діяльності здатні мати значні правові наслідки для особи. Це актуалізує необхідність чіткого нормативного регулювання та впровадження ефективних механізмів кіберзахисту.

GDPR закріплює базові принципи обробки персональних даних, серед яких законність, добросовісність, прозорість, мінімізація даних та обмеження мети обробки [1]. Для систем ШІ ці принципи означають необхідність чіткого визначення цілей використання даних ще до початку розробки алгоритму.

Принцип «конфіденційність за замовчуванням» передбачає інтеграцію механізмів захисту даних у технічну архітектуру системи. Це включає належне налаштування параметрів конфіденційності, обмеження доступу до даних, журналювання операцій та впровадження процедур оцінки ризиків. Важливим інструментом є проведення оцінки впливу на захист даних у випадку високо ризикованої обробки даних.

Окремої уваги заслуговує стаття 22 GDPR, яка гарантує право особи не підлягати рішенню, заснованому виключно на автоматизованій обробці, якщо таке рішення має юридичні наслідки. У контексті ШІ це означає необхідність забезпечення людського контролю та можливості оскарження результатів алгоритмічної обробки. Практичні аспекти застосування цих норм деталізуються у рекомендаціях Європейської ради з захисту даних [2].

Кібербезпека ШІ має комплексний характер, оскільки загрози можуть виникати на різних етапах життєвого циклу системи. На етапі збору та підготовки даних існує ризик їх компрометації або навмисного спотворення. Під час експлуатації моделі можливі адверсарійні-атаки, коли спеціально сформовані вхідні дані призводять до некоректних результатів.

Крім того, значну небезпеку становить несанкціонований доступ до інфраструктури зберігання або обробки даних, особливо у хмарних середовищах. Витік параметрів моделі може створити передумови для реконструкції навчальних даних. У випадку порушення безпеки персональних даних контролер зобов'язаний повідомити наглядовий орган протягом 72 годин [1], що підкреслює важливість своєчасного виявлення інцидентів.

Для мінімізації ризиків доцільно застосовувати комплекс технічних заходів. Анонімізація та псевдонімізація знижують ймовірність ідентифікації особи, однак потребують ретельної оцінки ефективності [5]. Перспективним напрямом є використання диференційної приватності, яка забезпечує математично обґрунтовані гарантії конфіденційності.

Моделі можна навчати без збору всіх даних у одному місці, що знижує ризик компрометації інформації. Криптографічні методи, зокрема гомоморфне шифрування, забезпечують можливість обробки даних у зашифрованому вигляді. Базові принципи побудови безпечних моделей машинного навчання викладені у фундаментальних працях з глибинного навчання [6].

Водночас технічні рішення мають поєднуватися з організаційними заходами, такими як аудит безпеки, контроль доступу, навчання персоналу та впровадження політик реагування на інциденти.

В українській правовій доктрині активно обговорюються проблеми правового забезпечення розвитку ШІ та необхідність гармонізації законодавства із європейськими стандартами [7]. Науковці наголошують на важливості захисту прав людини в умовах цифровізації та впровадження ризик-орієнтованої моделі регулювання [8].

В умовах воєнного стану та зростання кіберзагроз питання захисту персональних даних набуває додаткового значення. Забезпечення кіберстійкості ШІ-систем є елементом національної безпеки та довіри до цифрових сервісів держави.

Гармонізація національного законодавства із вимогами GDPR передбачає не лише його формальне оновлення, а й формування культури захисту даних, підготовку фахівців та розвиток міждисциплінарної співпраці між ІТ-експертами та юристами.

Отже, кібербезпека систем штучного інтелекту є ключовою умовою забезпечення ефективного та правомірного використання цифрових технологій. Вимоги GDPR формують комплексну нормативну рамку, що зобов'язує інтегрувати принципи захисту персональних даних у саму архітектуру ШІ.

Поєднання технічних інновацій, правового регулювання та етичних стандартів дозволяє забезпечити баланс між розвитком технологій і гарантуванням фундаментальних прав людини. Для України імплементація європейських стандартів у сфері кібербезпеки ШІ є стратегічним напрямом цифрової трансформації та інтеграції до правового простору ЄС.

Список використаних джерел

1. General Data Protection Regulation (EU) 2016/679. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj

2. European Data Protection Board. Guidelines on Automated decision-making and profiling for the purposes of Regulation 2016/679. URL: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/automated-decision-making-and-profiling_en.

3. Shokri R. et al. Membership inference attacks against machine learning models, 2017 IEEE Symposium on Security and Privacy. 2017.

4. Fredrikson M. et al. Model inversion attacks that exploit confidence information. ACM CCS '15. 2015.

5. Voigt P., von dem Bussche A. The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer, 2017.

6. Abadi M., Chu A., Goodfellow I., McMahan H. B., Mironov I., Talwar K., Zhang L. *Deep Learning with Differential Privacy*: Proceedings of the 2016 ACM Conference on Computer and Communications Security (CCS) / M. Abadi, A. Chu, I. Goodfellow, H.B. McMahan, I. Mironov, K. Talwar, L. Zhang. Vienna, Austria, 2016. Pp. 308-318. DOI: 10.1145/2976749.2978318.

7. Баранов О. А. Правове забезпечення розвитку штучного інтелекту в Україні. *Інформація і право*. 2020. № 3.

8. Петришин О. В., Барабаш Ю. Г. Права людини в цифрову епоху: виклики та перспективи правового регулювання. *Право України*. 2021. № 7.

Ляшенко О. С.
декан факультету комп'ютерної інженерії
та інформаційних технологій,
кандидат технічних наук, доцент
(Харківський національний університет радіоелектроніки)
Велікан О. В.
аспірант кафедри ЕОМ
(Харківський національний університет радіоелектроніки)

ФЕДЕРАТИВНЕ МАШИННЕ НАВЧАННЯ ЯК ТЕХНОЛОГІЯ ОБРОБКИ МЕДИЧНИХ ДАНИХ З ДОТРИМАННЯМ ПРИНЦИПІВ ЗАХИСТУ ПЕРСОНАЛЬНОЇ ІНФОРМАЦІЇ ПАЦІЄНТІВ

Сучасна медицина генерує колосальні обсяги даних: електронні медичні картки, результати візуалізаційних досліджень (КТ, МРТ), геномні послідовності, дані носимих пристроїв. Централізоване зберігання та обробка цих даних вступає в конфлікт із принципами захисту персональної інформації, оскільки дані про здоров'я належать до особливої категорії чутливих даних [1].

Основна проблема – протиріччя між потребою в спільному навчанні високоточних моделей ШІ для покращення діагностики, прогнозування захворювань і персоналізованої медицини та жорсткими правовими обмеженнями на передачу сирих медичних даних. Традиційні централізовані підходи порушують принципи мінімалізації даних і збільшують ризики витоків [2].

Федеративне машинне навчання (ФН), запропоноване у 2016–2017 рр., дозволяє навчати моделі локально на даних кожної установи, передаючи на сервер лише оновлення параметрів. Це дає змогу отримувати глобально узагальнену модель без розкриття сирих даних пацієнтів [3, 4].

Метою роботи є аналіз можливостей ФН для обробки медичних даних з забезпеченням правового захисту персональної інформації, оцінка відповідності чинному законодавству України та міжнародним стандартам, а також визначення перспектив впровадження.

Федеративне навчання реалізується як ітеративний процес, у якому K клієнтів (лікарень, лабораторій) мають локальні датасети D_k. Глобальна модель оновлюється за допомогою алгоритму FedAvg [3]:

$$w^{t+1} = \sum_{k=1}^{K} \frac{n_k}{n} w_k^{t+1},$$

де w_k^{t+1} – модель, навчена на k-му клієнті, $n = \sum n_k$.

Розрізняють горизонтальне ФН – однакова структура ознак, різні зразки, вертикальне ФН та федеративне навчання з підкріпленням [2, 5]. Перевагами ФН є збереження суверенітету даних, зниження комунікаційних витрат і підвищення узагальненості моделі завдяки гетерогенним даним з різних установ.

ФН ефективно застосовується для діагностики медичних зображень, прогнозування захворювань на основі електронних карток, епідеміологічного моделювання та генерації синтетичних даних [2, 6]. Точність моделей часто досягає 95–98 % і є порівнянною з централізованими підходами. Реальні проєкти включають федеративне навчання для QSAR-моделей у відкритті ліків без розкриття даних [7], а також ініціативи з інтеграції ФН у європейський простір даних про здоров'я. В Україні технологія актуальна для Електронної системи охорони здоров'я (ЕСОЗ), де сирі дані залишаються в локальних системах, а агрегуються лише модельні оновлення [1, 8].

Базовий ФН вразливий до атак на градієнти. Тому застосовуються додаткові технології [2, 9]:

- диференціальна приватність (ДП) – додавання контрольованого шуму до градієнтів. Параметр ε контролює рівень приватності; втрата точності зазвичай становить 2–5 % при правильному налаштуванні [9, 10];
- безпечне агрегування – криптографічні протоколи, за яких сервер бачить лише суму оновлень;
- гомоморфне шифрування та безпечне мультистороннє обчислення.

Комбінація ФН + ДП + PET забезпечує математичні гарантії приватності та відповідає принципам privacy-by-design [2, 11].

Згідно із Законом України «Про захист персональних даних» № 2297-VI, дані про здоров'я є особливою категорією. Їх обробка можлива за спеціальними підставами (медична допомога, наукові дослідження). Оскільки при ФН сирі дані не покидають локальних систем, не відбувається передачі третім особам у розумінні закону. Для наукових цілей достатньо знеособлення, ДП та угод про спільну обробку [12]. У контексті євроінтеграції ФН стає інструментом гармонізації з GDPR.

Перспективи для України, це створення національного ФН-хабу на базі ЕСОЗ, участь у програмах EU4Health та Horizon Europe, пілотні проєкти в онкології та радіології 2026–2028 рр., інтеграція фреймворків Flower або TensorFlow Federated з урахуванням національних вимог безпеки [8].

Федеративне машинне навчання радикально вирішує конфлікт між потребою у великих даних для ШІ в медицині та вимогами захисту персональної інформації. Комбінація ФН з ДП та іншими PET забезпечує високий рівень конфіденційності при збереженні корисності моделей. Технологія відповідає міжнародним (GDPR, HIPAA) та національним нормам, що робить її юридично безпечною для впровадження в Україні.

Подальші дослідження повинні фокусуватися на стандартизації, масштабуванні пілотів, боротьбі з non-IID даними та гібридних архітектурах з генеративним ШІ. Впровадження ФН сприятиме підвищенню якості медичної допомоги та зміцненню довіри пацієнтів.

Список використаних джерел:

1. Brauneck A. et al. Federated Machine Learning, Privacy-Enhancing Technologies, and Data Protection Laws in Medical Research: Scoping Review. J Med Internet Res. 2023;25:e41588. doi:10.2196/41588.

2. Pati S. et al. Privacy preservation for federated learning in health care. Patterns. 2024. doi:10.1016/j.patter.2024.100982 (або повний: https://www.sciencedirect.com/science/article/pii/S2666389924000825).

3. McMahan H.B. et al. Communication-Efficient Learning of Deep Networks from Decentralized Data. arXiv:1602.05629, 2016 (опубліковано в AISTATS 2017). https://arxiv.org/abs/1602.05629.

4. Abbas S.R. Federated Learning in Smart Healthcare: A Comprehensive Review on Privacy, Security, and Predictive Analytics with IoT Integration. Healthcare. 2024;12(24):2587. doi:10.3390/healthcare12242587.

5. Haripriya R. et al. Privacy-preserving federated learning for collaborative medical data mining in multi-institutional settings. Scientific Reports. 2025;15:12482. doi:10.1038/s41598-025-97565-4.

6. Horst A. et al. Federated learning: a privacy-preserving approach to data collaboration in regulatory sciences. Front Drug Saf Regul. 2025. doi:10.3389/fdsfr.2025.1579922.

7 Heyndrickx W. et al. MELLODDY: Cross-pharma Federated Learning at Unprecedented Scale Unlocks Benefits in QSAR without Compromising Proprietary Information. J Chem Inf Model. 2023. doi:10.1021/acs.jcim.3c00799.

8. Li M. et al. Implementing federated learning in healthcare. Medical Image Analysis. 2025 (огляд до травня 2024). https://www.sciencedirect.com/science/article/pii/S1361841525000453.

9. Wassan S. et al. Federated learning and differential privacy: Machine learning and deep learning for biomedical image data classification. 2025 (PMC).

10. Onireti M.Y. et al. Splitting smarter: Differential privacy for secure healthcare federated learning. Scientific Reports. 2025. doi:10.1038/s41598-025-27472-1.

11. Eden R. et al. A scoping review of the governance of federated learning in healthcare. npj Digital Medicine. 2025;8:427. doi:10.1038/s41746-025-01836-3.

12. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI (зі змінами). https://zakon.rada.gov.ua/laws/show/2297-17.

Майданюк В.А.
професор кафедри артилерії,
доктор філософії
(Національна академія сухопутних військ
імені Петра Сагайдачного)
Гончаров В.В.
старший викладач кафедри наземної артилерії
(Національна академія сухопутних військ
імені Петра Сагайдачного)
Горобець В.В.
старший викладач кафедри наземної артилерії
(Національна академія сухопутних військ
імені Петра Сагайдачного)

МЕТОДОЛОГІЧНІ ТА ТЕХНОЛОГІЧНІ АСПЕКТИ ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМАХ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ

Сьогодні штучний інтелект (ШІ) все активніше проникає у військову сферу. Його застосування може суттєво вплинути на способи ведення війни – від автоматизації рутинних процесів до покращення точності прийняття рішень. Але впровадження таких технологій – це не просто «вставити програму в танк». Потрібно враховувати багато нюансів: і технічних, і методологічних, і навіть етичних. У цьому матеріалі йдеться про ключові моменти, які варто враховувати під час розробки та інтеграції ШІ у військові системи.

Перш за все, потрібно чітко зрозуміти, для яких саме задач буде використовуватись ШІ. Чи це автоматичне керування вогнем? А може, аналіз супутникових знімків або підтримка під час планування операцій? Важливо також визначити, наскільки автономною має бути система: повна автоматизація чи постійний контроль з боку людини?

Без добрих алгоритмів – нікуди. Сучасні військові системи з ШІ спираються на машинне та глибинне навчання. Зокрема, використовуються нейронні мережі, які можуть розпізнавати

об'єкти на фото і відео, оцінювати ситуацію та навіть приймати рішення на ходу.

ШІ сам по собі нічого не робить – його треба підключити до іншої техніки. Наприклад, до радарів, безпілотників або систем управління вогнем. Тільки тоді вийде створити справді ефективну бойову машину, яка зможе швидко реагувати на зміну ситуації.

Жодна система ШІ не може бути впроваджена "наосліп". Її потрібно постійно тестувати, перевіряти, як вона поводиться в різних умовах, і бути готовим до того, що можуть виникнути помилки. Тому треба мати плани дій, якщо щось піде не так.

Щоб штучний інтелект працював швидко й точно, йому потрібні серйозні «залізяки». Потужні процесори, спеціалізовані чіпи та сервери – усе це забезпечує обробку великих обсягів даних у реальному часі. І, що важливо, ця техніка має бути не тільки в командному центрі, а й на мобільних платформах – наприклад, у дронах чи бойових роботах.

Одне з головних завдань – навчити машину розпізнавати об’єкти. Камери, сенсори, супутникові знімки – все це "очі" для ШІ. Система має не просто бачити, а й розуміти, що перед нею: друг, ворог, загроза чи щось нейтральне. Усе це допомагає краще орієнтуватися на полі бою.

Завдяки ШІ можна створювати техніку, яка діє самостійно. Наприклад, дрони, які самі обирають маршрут і ціль, або роботи, що виконують завдання без постійного нагляду. Але автономність – це не лише зручність, а й відповідальність: машина повинна вміти приймати рішення швидко та в правильному напрямку, навіть у складних умовах.

Чим розумніша система – тим більше охочих її зламати. Тому кіберзахист – це must have. Потрібно надійно захищати дані, з якими працює ШІ, від хакерських атак, фальсифікацій або втручання ззовні. Інакше замість переваги на полі бою можна отримати великий ризик.

Один з найважчих моментів – це вирішити, наскільки автономною має бути бойова система. Чи має машина право приймати рішення про знищення цілі без участі людини? Тут важливо провести чітку межу: де закінчується автоматизація і починається етика. Ніхто не хоче, щоб роботи самі вирішували, хто має жити, а хто ні.

Щоб уникнути хаосу, потрібні міжнародні домовленості. Без загальних стандартів може початися гонка озброєнь, де кожен сам за себе. Правила мають чітко регламентувати, як і де можна використовувати ШІ у військовій сфері, щоб не вийшло так, що технологія стане неконтрольованою загрозою.

Підсумовуючи вище зазначене, можемо зазначити, що штучний інтелект у військовій сфері – це не просто про нові "розумні" машини. Це про зміну підходів до ведення війни, підвищення ефективності та швидкості дій, але також і про нові ризики. Щоб ШІ справді працював на користь, потрібно добре продумати, як його створювати, як впроваджувати і як контролювати. Надійні алгоритми, міцна кібербезпека та чіткі міжнародні правила — ось три кити, на яких має триматися ця технологічна революція.

Список використаних джерел:

1. Russell S., Norvig P. Artificial intelligence: a modern approach. 4th ed. Hoboken : Pearson, 2021. 1136 p.

2. Goodfellow I., Bengio Y., Courville A. Deep learning. Cambridge : MIT Press, 2016. 775 p.

3. Scharre P. Army of none: Autonomous weapons and the future of war. New York : W. W. Norton & Company, 2018. 448 p.

4. United Nations. Report of the Secretary-General on lethal autonomous weapons systems. New York : United Nations, 2021. URL: https://undocs.org (date of access: 24.02.2026).

5. NATO. NATO’s approach to artificial intelligence. Brussels : NATO, 2021. URL: https://www.nato.int (date of access: 24.02.2026).

6. Department of Defense. Summary of the 2018 Department of Defense Artificial Intelligence Strategy. Washington : U.S. Department of Defense, 2018. URL: https://media.defense.gov (date of access: 24.02.2026).

7. Brundage M. et al. The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. Oxford : University of Oxford, 2018. 101 p.

8. European Commission. Artificial intelligence act: Proposal for a regulation laying down harmonised rules on artificial intelligence. Brussels : European Commission, 2021. URL: https://eur-lex.europa.eu (date of access: 24.02.2026).

Манжай О.В.
завідувач кафедри протидії кіберзлочинності
навчально-наукового інституту № 4,
кандидат юридичних наук, професор
(Харківський національний університет внутрішніх справ)

ОДИН МЕТОД ОРГАНІЗАЦІЇ МОНІТОРИНГУ ПОДІЙ, ЯКІ СТАНОВЛЯТЬ ІНТЕРЕС ДЛЯ ПРАВООХОРОННИХ ОРГАНІВ

У діяльності правоохоронних органів нерідко постає завдання відслідковування певних подій для своєчасного реагування на них. Постійний великий потік інформації зумовлює необхідність автоматизації його моніторингу для своєчасного прийняття рішень. У даному випадку на допомогу може прийти математичний апарат та штучний інтелект, але проблема в тому, що в поліції досить часто існує брак спеціалістів з глибокими знаннями у сфері математики та штучного інтелекту.

Враховуючи викладене, для проведення відповідного аналізу на місцях може бути застосоване рішення, яке не потребує глибоких технічних знань та водночас може стати достатньо ефективним способом організації моніторингу подій, які становлять інтерес. Суть даного рішення полягає у перетворенні інформаційного потоку в RSS та використання інструментів прогнозування належності подій з RSS-стрічок до того або іншого кластеру, сформованого аналітиком.

Наведений метод можна представити у вигляді послідовності таких кроків:

1. Підготувати перелік інформаційних ресурсів (сайтів, Telegram-каналів) для моніторингу.

2. Організувати RSS-попередження щодо появи контенту, який становить інтерес. Це можна зробити, наприклад, за допомогою Google дорків та інструменту Google Alerts (google.com/alerts), Talkwalker Alerts (talkwalker.com/alerts).

3. З використанням ресурсу RSSHub (rsshub.app) здійснити перетворення у RSS-стрічку даних з каналів Telegram (https://rsshub.app/telegram/channel/**НАЗВА_КАНАЛУ**).

4. Об'єднати отримані RSS-стрічки у єдиному вебдокументі, який можна переглядати, автоматично перекладати, аналізувати тощо. Для вирішення завдання такого об'єднання можна скористатися сервісом FEED.INFORMER (feed.informer.com). Одержаний RSS-потік даних буде подаватися на вхід системи для аналізу.

5. Сформувати досьє на подію, місце, групу або особу, які становлять інтерес (перекладаємо досьє різними мовами). На базі досьє формується набір даних для порівняння. Для цього для тексту кожного досьє здійснюється нормалізація (приведення слів до єдиного формату, вилучення прийменників, займенників, прикметників тощо) та токенізація (розбиття тексту на слова). На основі вхідних наборів слів створюється терм-документна матриця, що відображатиме частоту появи певних слів у досьє. Терм-документна матриця для кожного досьє буде визначати кластер для подальшого порівняння.

6. Після того, як сформовано кластери, слід реалізувати схему прогнозування належності подій з RSS-стрічок до того або іншого кластеру. Для цього в схему слід додати модуль логістичної регресії (Random Forest або SVM), який буде виводити ймовірності належності до кластеру. Кожне повідомлення з RSS-стрічок та прогноз ймовірності належності об'єкта до певного класу з Logisitc Regression далі слід передавати на модуль прогнозування, який має вивести передбачені значення цільової змінної на основі моделі, яку навчили у Logistic Regression.

7. У випадку високої ймовірності належності повідомлення до певного кластеру слід вилучити його зі стрічки, завантажити в систему та надіслати на перевірку оператору.

Для відпрацювання даної методики було проведено моделювання з використанням рішення Orange Data Mining (orangedatamining.com), яке за допомогою візуального програмування дозволяє комплексно вивчати дані, у тому числі проводити їх класифікацію, кластеризацію, готувати прогнози тощо.

За допомогою засобів штучного інтелекту та інформаційних джерел сформовано декілька зведень про вчинення вбивств

відомими маніяками та знеособлено їх. Ці дані можуть бути неточними, але для вирішення завдань моделювання є придатними.

Після імпорту даних до Orange було проведено їх попередню обробку за допомогою віджета Preprocess Text. У налаштуваннях віджету було обрано параметри нормалізації (приведення слів до єдиного формату) та токенізації (розбиття тексту на частини, речення, слова тощо). Для числового представлення завантаженого тексту використано віджет Bag of Words, який створює терм-документну матрицю, що відображатиме частоту появи певних термінів (слів) у документах (повідомленнях).

Підготовлена матриця подається а вхід віджета Distances, за допомогою якого обчислюється міра схожості або відмінності між об'єктами (рядками даних). У налаштуваннях цього віджету було обрано метрику «Косинусна схожість» (Cosine), за допомогою якої вимірюється кут між векторами частот слів, що часто використовується саме для текстових даних. Таким чином, на виході отримаємо матрицю відстаней між векторами, якими представлені об'єкти тексту. Ця матриця відстаней надалі подається на вхід віджету Hierarchical Clustering, що використовується для групування об'єктів за схожістю та побудови ієрархії кластерів у вигляді дендрограми (дерева).

На рис. 1 наведена підсумкова схема поєднання віджетів для реалізації описаного завдання.

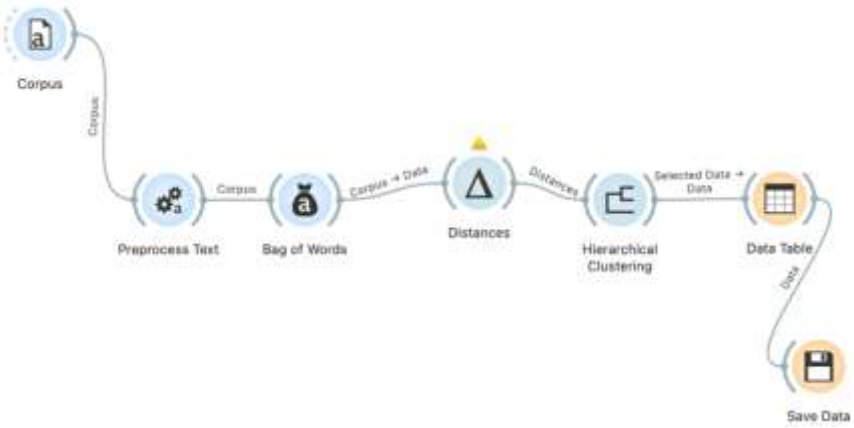

Рис. 1. Схема для виявлення кластерів

На початковому етапі було вірно визначено два кластери, інші визначені частково. Для того, щоб підвищити точність групування було подано на вхід створеної схеми більш повні дані зі зведень, а також прибрано зайві слова типу прийменників, займенників, часток за допомогою поля Stopwords у віджеті Preprocess Text.

У результаті було отримано дерево кластерів як на рис. 2.

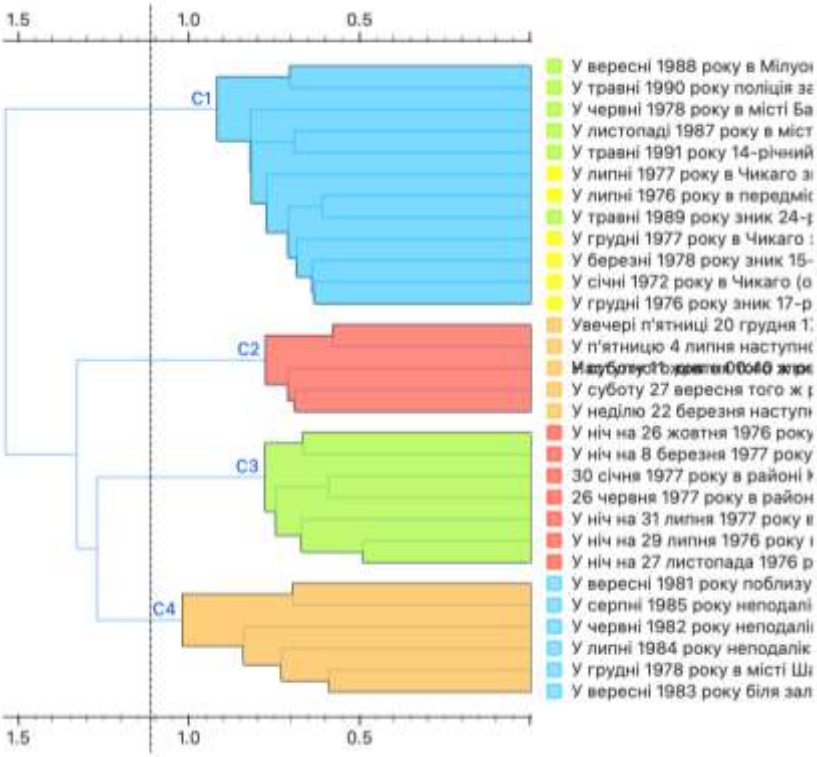

Рис. 2. Визначені кластери для розширених зведень

Чим більше фактичних відомостей буде подано на вхід схеми з кластеризації та чим краще будуть оброблені вхідні відомості, тим точніше буде здійснено групування.

Після того, як сформовано кластери для серій злочинів, було реалізовано схему прогнозування належності інших подій до того або іншого кластеру. Для цього в схему додається віджет Select

Columns, у якому слід обрати для подальшого аналізу сформовані кластери як Target та відповідні зведення як Meta. Одержані дані надалі можна передати у віджет Logisitc Regression, який буде виводити ймовірності належності до кластеру.

Описане моделювання засвідчило теоретичну придатність даної методики для моніторингу появи контенту, який становить інтерес для правоохоронних органів.

Марченко К.О.
курсант
навчально-наукового інституту
поліцейської діяльності
(*Національна академія внутрішніх справ*)

ЗНАЧЕННЯ ТА ПЕРСПЕКТИВИ ШТУЧНОГО ІНТЕЛЕКТУ В ФУНКЦІОНУВАННІ ІНСТИТУТУ АДВОКАТУРИ УКРАЇНИ

Сучасний етап розвитку суспільства характеризується активною цифровізацією різних сфер діяльності людини. Одним із найважливіших напрямів технологічного поступу є розвиток штучного інтелекту, який поступово інтегрується у правову систему та юридичну практику. Використання інтелектуальних технологій стає важливим інструментом підвищення ефективності правничої діяльності, зокрема й у межах функціонування інституту адвокатури. У сучасних умовах розвитку інформаційного суспільства штучний інтелект відкриває нові можливості для вдосконалення діяльності адвокатів, забезпечення доступу до правничої допомоги та підвищення якості юридичних послуг.

Інститут адвокатури є важливою складовою правової системи України, оскільки забезпечує реалізацію конституційного права кожної особи на правничу допомогу. Адвокатура виступає незалежним професійним інститутом, діяльність якого спрямована на захист прав, свобод і законних інтересів людини та громадянина. В умовах постійного розвитку законодавства та збільшення обсягу правової інформації адвокати змушені працювати з великими масивами нормативно-правових актів, судової практики та наукових джерел. Саме тому використання сучасних технологій, зокрема штучного інтелекту, стає важливим інструментом оптимізації їх професійної діяльності [1, с. 42].

Штучний інтелект у правничій сфері передусім використовується для аналізу значних обсягів правової інформації. Сучасні алгоритми дозволяють швидко опрацьовувати судову практику, нормативно-правові акти, юридичну літературу та інші

правові матеріали. Завдяки цьому адвокати можуть значно швидше знаходити потрібну інформацію для підготовки правової позиції у справі. Крім того, спеціалізовані правові системи можуть аналізувати тенденції судової практики та допомагати прогнозувати можливі результати судового розгляду. Такий підхід сприяє підвищенню якості юридичної допомоги та ефективності захисту прав клієнтів.

Окрім цього, штучний інтелект може сприяти підвищенню доступності правничої допомоги для громадян. У сучасних умовах активно розвиваються онлайн-платформи та електронні сервіси, які дозволяють отримувати правову інформацію дистанційно. Наприклад, правові чат-боти можуть надавати первинні консультації, пояснювати порядок звернення до суду або інших державних органів, а також допомагати громадянам підготувати стандартні документи. Завдяки таким технологіям правнича допомога стає більш доступною для населення, особливо для осіб, які проживають у віддалених регіонах або не мають можливості швидко звернутися до адвоката [2, с. 58].

Водночас використання штучного інтелекту у діяльності адвокатури пов’язане з певними викликами та ризиками. Однією з головних проблем є забезпечення конфіденційності інформації, яка становить адвокатську таємницю. Адвокатська діяльність передбачає роботу з великою кількістю персональних даних та іншої чутливої інформації, тому використання цифрових технологій повинно супроводжуватися надійним захистом даних. Порушення конфіденційності може призвести до негативних правових наслідків і втрати довіри клієнтів до адвоката. Також важливим аспектом є етичні питання використання штучного інтелекту у правничій діяльності. Незважаючи на значні можливості сучасних технологій, вони не можуть повністю замінити професійну діяльність адвоката. Юридична діяльність передбачає не лише впровадження правових норм, а й оцінку певних життєвих обставин, моральних аспектів та індивідуальних рис кожної ситуації. Саме тому функція правника залишається центральною у процесі надання правової підтримки, а штучний інтелект виступає лише додатковим засобом.

Можливості застосування штучного інтелекту у функціонуванні інституту адвокатури України є досить великими.

У найближчому майбутньому очікується подальша розбудова інформаційних правових систем, які комбінуватимуть бази законодавства, судових рішень та аналітичні інструменти. Це дозволить адвокатам оперативно одержувати потрібну правову інформацію та якісно готуватися до розгляду справ. Вагомим напрямком прогресу є також злиття штучного інтелекту із системами електронного правосуддя. Впровадження цифрових методів сприятиме зростанню ефективності судових процесів, зменшенню термінів розгляду справ та підвищенню відкритості діяльності судових установ. У таких умовах правники зможуть більш продуктивно взаємодіяти із судами, подавати документи у цифровій формі та контролювати хід розгляду справи у режимі реального часу.

Окрім того, значну роль у розвитку застосування штучного інтелекту в адвокатурі відіграє система правової освіти. Майбутні правники мусять володіти не лише традиційними юридичними знаннями, але й уміннями роботи із сучасними інформаційними засобами. Розуміння принципів роботи штучного інтелекту дасть змогу адвокатам ефективно користуватися подібними системами у своїй практиці та зважено оцінювати результати їхньої роботи [3, с. 91].

Отже, штучний інтелект поступово стає суттєвим складником розвитку сучасної правової системи. Його використання у діяльності адвокатури сприяє посиленню ефективності роботи правників, оптимізації аналізу правової інформації та розширенню доступу громадян до правової допомоги. Водночас запровадження таких технологій вимагає належного правового регламентування, дотримання етичних норм та забезпечення охорони конфіденційної інформації. Подальший розвиток штучного інтелекту може докорінно змінити юридичну професію, однак роль адвоката як носія правничих знань, фахового досвіду та етичної відповідальності залишиться головною у гарантуванні справедливості та захисту прав особи

Список використаних джерел:

1. Святоцький О. Д. Адвокатура України: сучасний стан та перспективи розвитку. Київ: Юрінком Інтер, 2021. 256 с. URL: https://unba.org.ua/assets/uploads/publications/%D0%90%D0%B4%D

0%B2%D0%BE%D0%BA%D0%B0%D1%82%D1%83%D1%80%D0%B0%20%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8%20%D1%81%D1%83%D1%87%D0%B0%D1%81%D0%BD%D0%B8%D0%B9%20%D1%81%D1%82%D0%B0%D0%BD%20%D1%82%D0%B0%20%D0%BF%D0%B5%D1%80%D1%81%D0%BF%D0%B5%D0%BA%D1%82%D0%B8%D0%B2%D0%B8%20%D1%80%D0%BE%D0%B7%D0%B2%D0%B8%D1%82%D0%BA%D1%83.pdf (дата звернення 11.03.2026)

2. Коваленко Т. О. Використання штучного інтелекту у правничій діяльності. Право України. 2022. № 5. С. 54–60. URL: https://lib.iitta.gov.ua/id/eprint/734475/1/2023-381-marienkokovalenko.pdf (дата звернення 11.03.2026)

3. Харитонов Є. О., Харитонова О. І. Цифровізація правової системи та перспективи застосування штучного інтелекту. Одеса: Фенікс, 2020. URL: https://dspace.onua.edu.ua (дата звернення 11.03.2026)

Матвійчук А.І.
курсант
навчально-наукового інституту
поліцейської діяльності
(Національна академія внутрішніх справ)

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПОКРАЩЕННЯ ТА ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РОБОТИ ПОЛІЦІЇ

Останніми десятиліттями штучний інтелект (ШІ) став звичною річчю в багатьох сферах нашого життя, і правоохоронна діяльність тут не виняток. Якщо використовувати його з розумом, він може серйозно допомогти поліції працювати ефективніше. Але, звісно, є й інша сторона медалі – одразу виникають питання щодо приватності, безпеки даних та моральних аспектів.

Для початку варто зрозуміти, які саме завдання правоохоронців можна вирішувати за допомогою ШІ. Їх можна розділити на дві великі групи: аналітичні завдання та робота з інформацією, а також завдання, пов'язані з моніторингом і запобіганням загрозам.

Що стосується аналітики – це коли треба обробляти величезні обсяги даних, щоб знаходити якісь закономірності, тенденції чи зв'язки. Наприклад, ШІ можна використовувати для виявлення підозрілої активності або розкриття злочинів, що, власне, є звичайною роботою поліцейського. Сюди ж належить обробка та інтерпретація інформації для прийняття рішень. Скажімо, штучний інтелект цілком може автоматично аналізувати докази в кримінальних справах або допомагати ухвалювати рішення в питаннях безпеки. Щодо моніторингу та запобігання загрозам – тут ШІ використовують для того, щоб вчасно помічати небезпеку або підозрілі дії та вживати заходів. Найпростіший приклад – камери відеоспостереження зі штучним інтелектом, які самі розпізнають небезпечні ситуації й одразу повідомляють відповідні служби.

Хочеться окремо зупинитися на тому, як ШІ працює разом із безпілотниками (БПЛА). Це дуже вдале поєднання. Дрони можуть

швидко облітати великі території й збирати корисну інформацію, тому їх активно використовують для стеження за транспортом, фіксації аварій, отримання оперативних даних про ситуацію на місцях. Вони допомагають поліції краще захищати людей і швидше реагувати на правопорушення, виявляти незаконні дії (як-от контрабанда чи торгівля наркотиками), а також контролювати натовп під час масових заходів [1]. Тому безпілотники разом зі штучним інтелектом можуть стати справді потужним інструментом для виконання завдань, які стоять перед Національною поліцією України.

Ось декілька прикладів, де ШІ може бути корисним працівникам поліції:

Найвідоміший приклад – це системи оптичного розпізнавання символів (OCR). Вони вже давно чудово справляються з тим, щоб розпізнавати текст на зображеннях (іноді навіть рукописний) і перетворювати його на звичайний документ [2].

Жодна людина, навіть цілий відділок поліції, не зможе переглянути й проаналізувати величезну кількість фото або відео, порівняти їх з наявними зразками й зробити правильні висновки. А от системи розпізнавання роблять це з дуже високою точністю — аж до 99,7%. Наприклад, Facebook DeepFace визначає, чи одна людина на двох фотографіях, з точністю 97% [2].

Системи розпізнавання облич, щоправда, можуть помилятися, якщо знімок нечіткий, але більшість із них усе одно досить точно "впізнають" людей на фото чи відео. Гарний приклад ефективного інструменту, яким уже користуються поліцейські в різних країнах, – це програма від компанії Clear View AI [2].

У всього цього величезний потенціал для того, щоб зробити роботу поліції ефективнішою та безпечнішою. Але при цьому не можна забувати про питання приватності, безпеки та етики — їх доведеться дуже уважно вирішувати.

Час серйозно зайнятися законодавчим регулюванням використання штучного інтелекту. Наразі у світі практично немає чітких законів, які б визначали, як саме можна використовувати ШІ. Щоправда, Європейський Союз уже взявся до цього і розглядає проєкт Регламенту та Закону про штучний інтелект [3].

Ми переконані, що й науковці, й практики мають зосередити свої зусилля саме на цьому напрямку – він зараз дуже важливий.

Отже, штучний інтелект дійсно може стати дуже потужним помічником у забезпеченні безпеки й правопорядку. Але дуже важливо не забувати про етичні й правові моменти, щоб використання таких технологій не порушувало права та свободи людей. Якщо розробити чіткі правила й норми для використання ШІ в поліції, тоді можна буде знайти баланс між ефективністю роботи й захистом прав громадян.

Список використаних джерел:

1. Атаманенко Ю.Ю. Інноваційні технології в діяльності поліцейських підрозділів України. URL: https://dnuvs.ukr.education/wp-content/uploads/2023/06/zbirnyk_mnpk_bezpeka_na_dorozi_18_05_2023.pdf дата звернення: (11.03.2026).

2. Баловсяк Н. Справжній робокоп: як використовують ШІ розкриття злочинів. robot_dreams - онлайн-курси для фахівців у сфері big data, machine learning, data science Робот Дрімс. URL: https://robotdreams.cc/uk/blog/362-spravzhniy-robokop-yak-vikoristovuyut-shi-dlya-rozkrittya-zlochiniv (дата звернення: (11.03.2026).

3. Європарламент схвалив план регулювання штучного інтелекту. Суспільне | Новини. URL: https://suspilne.media/507905-evroparlament-shvaliv-plan-reguluvanna-stucnogo-intelektu/дата звернення: (11.03.2026).

Меликов Р.
науковий співробітник науково-дослідної лабораторії
з актуальних питань кримінального аналізу,
доктор філософії
(Одеський державний університет внутрішніх справ)

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В УМОВАХ ВІЙНИ: МОЖЛИВОСТІ ДЛЯ КРИМІНАЛЬНОГО АНАЛІЗУ, OSINT ТА ДОКУМЕНТУВАННЯ ВОЄННИХ ЗЛОЧИНІВ

Повномасштабна збройна агресія проти України супроводжується значною кількістю воєнних злочинів та інших порушень норм міжнародного гуманітарного права, що потребують належної фіксації, документування та подальшого розслідування. Масштабність таких правопорушень зумовлює необхідність використання сучасних цифрових інструментів, здатних забезпечити швидку обробку значних обсягів інформації. Значна частина відомостей про події війни поширюється у відкритому інформаційному просторі - у соціальних мережах, медіа, супутникових знімках, фото- та відеоматеріалах очевидців. У зв'язку з цим особливого значення набуває застосування технологій штучного інтелекту та методів OSINT (Open Source Intelligence), які дозволяють автоматизувати аналіз інформації, виявляти цифрові докази та підвищувати ефективність кримінального аналізу під час розслідування воєнних злочинів.

Сучасні збройні конфлікти характеризуються інтенсивним використанням цифрових технологій, серед яких важливу роль відіграє штучний інтелект. Його застосування відкриває нові можливості для підвищення ефективності кримінального аналізу, обробки великих масивів даних із відкритих джерел, а також документування воєнних злочинів. В умовах війни такі технології стають важливим інструментом для правоохоронних органів, аналітичних підрозділів та міжнародних інституцій, які займаються фіксацією та розслідуванням злочинів, пов'язаних із порушенням норм міжнародного гуманітарного права.

Однією з ключових переваг використання штучного інтелекту є здатність швидко аналізувати значні обсяги інформації з різних джерел: супутникових знімків, відеоматеріалів із безпілотних літальних апаратів, контенту соціальних мереж, новинних повідомлень та інших відкритих ресурсів. Алгоритми машинного навчання дозволяють автоматично ідентифікувати об'єкти на зображеннях і відео, визначати геолокацію подій, встановлювати часові параметри та виявляти закономірності, що мають значення для кримінального аналізу.

У сфері OSINT технології штучного інтелекту значно розширюють можливості пошуку та систематизації інформації. Зокрема, вони можуть застосовуватися для автоматичного моніторингу соціальних мереж, виявлення фото- та відеоматеріалів, що можуть містити ознаки воєнних злочинів, а також для аналізу метаданих та встановлення автентичності цифрових доказів. Використання таких інструментів дозволяє значно скоротити час обробки інформації та підвищити точність аналітичних висновків під час проведення кримінального аналізу.

Важливим напрямом застосування штучного інтелекту у сфері документування воєнних злочинів є його інтеграція з безпілотними літальними апаратами (БПЛА). У сучасних умовах війни безпілотники активно використовуються для аерофіксації наслідків бойових дій, зокрема руйнувань цивільної інфраструктури, місць обстрілів, позицій військової техніки та інших об'єктів, що можуть мати доказове значення у кримінальних провадженнях. Отримані за допомогою БПЛА фото- та відеоматеріали можуть містити значні обсяги інформації, аналіз яких у ручному режимі потребує значного часу та ресурсів.

Використання алгоритмів штучного інтелекту дозволяє автоматизувати обробку таких даних. Зокрема, технології комп'ютерного зору здатні здійснювати автоматичне розпізнавання об'єктів на зображеннях, виявляти пошкоджені будівлі, сліди вибухів, вирви від боєприпасів, військову техніку або інші елементи, що можуть свідчити про характер та обставини вчинення воєнного злочину. Поєднання даних аерозйомки з геоінформаційними системами та інструментами кримінального аналізу дозволяє створювати аналітичні карти подій, встановлювати просторові зв'язки між окремими епізодами та

реконструювати хронологію подій, що має важливе значення для формування доказової бази.

Водночас використання штучного інтелекту у сфері кримінального аналізу та OSINT в умовах війни пов'язане з низкою ризиків. Серед них – можливість поширення дезінформації, використання технологій deepfake, помилки алгоритмів під час автоматичного аналізу даних, а також проблеми забезпечення достовірності та процесуальної допустимості цифрових доказів. Крім того, існує ризик навмисного створення фальсифікованих цифрових матеріалів, які можуть ускладнювати процес розслідування.

Таким чином, застосування штучного інтелекту значно розширює можливості кримінального аналізу, використання OSINT та документування воєнних злочинів у сучасних умовах війни. Ефективність використання таких технологій залежить від розроблення чітких методологічних підходів до їх застосування, належного правового регулювання, а також підготовки фахівців, здатних поєднувати аналітичні методи кримінального аналізу з сучасними цифровими технологіями. Це створює підґрунтя для підвищення ефективності розслідування воєнних злочинів та забезпечення невідворотності відповідальності за їх вчинення.

Список використаних джерел:

1. Khan S., Furuly J., Vold H., Tahseen R., Dang-Nguyen D. Online Multimedia Verification with Computational Tools and OSINT: Russia-Ukraine Conflict Case Studies. 2023. https://arxiv.org/abs/2310.01978

2. Abedin A., Bais A., Buntain C. та ін. A Call to Arms: AI Should be Critical for Social Media Analysis of Conflict Zones. 2023.https://arxiv.org/abs/2311.00810

3. Kermode L., Freyberg J., Akturk A. та ін. Objects of Violence: Synthetic Data for Practical Machine Learning in Human Rights Investigations. 2020. https://arxiv.org/abs/2004.01030

4. Artificial Intelligence and War Crimes Investigations. Institute for War and Peace Reporting. https://iwpr.net/global-voices/artificial-intelligence-and-war-crimes-investigations

5. OSINT as Evidence in War Crimes Investigations. Верховний Суд України. https://court.gov.ua/eng/supreme/pres-centr/news/1883443/

6. Use of OSINT for the Collection of Electronic Evidence in War Crimes. Council of Europe CyberUA Project. https://www.coe.int/en/web/kyiv/-/cyberua-use-of-osint-for-the-collection-of-electronic-evidence-in-war-crimes-for-journalists-media-and-civil-society

7. Mudra I. Documentation of War Crimes in Projects of Ukrainian Online Media. Lviv Polytechnic National University. https://science.lpnu.ua/sjs/all-volumes-and-issues/number-1-11-2026/documentation-war-crimes-projects-ukrainian-online-media

8. Puzzling Pieces: OSINT and War Crime Accountability in Ukraine. Royal United Services Institute (RUSI).https://www.rusi.org/explore-our-research/publications/commentary/puzzling-pieces-osint-and-war-crime-accountability-ukraine

9. Ukraine's Prosecutors Launch OSINT War Crime Unit. Ukrinform. https://menafn.com/1109605661/Ukraines-Prosecutors-Launch-OSINT-War-Crime-UnitOSINT for Ukraine – Analytical Platform for War Crime Investigations. https://osintforukraine.com

Михаліцька Н.Я.
доцент кафедри менеджменту та економічної безпеки
кандидат наук з державного управління, доцент,
(Львівський державний університет внутрішніх справ)
Яцик М.Р.
доцент кафедри менеджменту та економічної безпеки
кандидат педагогічних наук, доцент,
(Львівський державний університет внутрішніх справ)

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ ТРАНСФОРМАЦІЇ СТРАТЕГІЧНОГО УПРАВЛІННЯ ПЕРСОНАЛОМ В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ

Цифрові технології суттєво змінюють сучасну економіку та трансформують підходи до управління організаціями і їх людськими ресурсами. У таких умовах саме люди, їх знання, навички та здатність швидко адаптуватися до змін стають одним із головних чинників конкурентоспроможності підприємств. Відповідно змінюється і роль HR-менеджменту: від виконання переважно адміністративних функцій він поступово переходить до формування стратегічних рішень, пов'язаних із розвитком людського капіталу.

Одним із технологічних драйверів цих змін стає штучний інтелект. Його можливості обробляти великі масиви даних, виявляти закономірності та моделювати потенційні сценарії розвитку кадрових процесів відкривають нові можливості для управління персоналом. Використання інтелектуальних алгоритмів дозволяє організаціям не лише автоматизувати окремі HR-процеси, а й глибше розуміти динаміку кадрового потенціалу, прогнозувати потреби у компетентностях і формувати більш обґрунтовані управлінські рішення [1].

Питання використання штучного інтелекту у сфері управління персоналом активно досліджується в сучасній науковій літературі. Зокрема, І. Дашко розглядає принципи впровадження інтелектуальних технологій у HR-процеси підприємств та їх вплив на ефективність управління людськими ресурсами [1]. О. Кравчук та І. Варіс досліджують трансформацію HR-менеджменту під

впливом цифрових технологій, зокрема аналізують управлінські та етичні аспекти використання штучного інтелекту, а також практичні питання застосування інтелектуальних технологій у рекрутингу та цифровізації кадрових процесів [2, 3]. Н. Черненко та З. Кобеля підкреслюють важливість використання HR-аналітики для оцінювання кадрового потенціалу та підтримки управлінських рішень у сфері управління персоналом [4, 5]. У працях [7, 8] акцентується увага на стратегічних і антикризових аспектах управління організаціями, що підсилює значення використання сучасних цифрових інструментів у системі менеджменту.

Практика управління персоналом у сучасних організаціях змінюється під впливом розвитку аналітичних цифрових інструментів. Одним із ключових серед них є штучний інтелект, який дозволяє працювати з великими масивами кадрових даних та отримувати нову інформацію про стан і динаміку людського капіталу підприємства.

У сфері HR це відкриває можливості для більш глибокого аналізу кадрових процесів. Алгоритми машинного навчання дозволяють аналізувати дані про продуктивність працівників, визначати фактори їх мотивації та прогнозувати ризики плинності персоналу. Завдяки цьому управлінські рішення дедалі частіше базуються на результатах аналітики даних, а не лише на управлінському досвіді або інтуїції менеджерів [4].

Одним із найбільш поширених напрямів використання штучного інтелекту є рекрутинг. Інтелектуальні системи здатні аналізувати резюме кандидатів, оцінювати їх відповідність вимогам вакансій та здійснювати попередній відбір претендентів. Це дозволяє суттєво скоротити час підбору персоналу та підвищити ефективність процесу найму [3].

Ще одним важливим напрямом є використання HR-аналітики. Інтелектуальні алгоритми машинного навчання дають змогу аналізувати дані про продуктивність працівників, визначати фактори їх мотивації та прогнозувати ризики плинності персоналу. У результаті керівники отримують інструменти для глибшого розуміння кадрових процесів і більш обґрунтованого планування розвитку людських ресурсів.

Крім того, штучний інтелект відкриває нові можливості у сфері навчання і розвитку персоналу. Сучасні цифрові платформи

дозволяють аналізувати рівень компетентностей працівників та формувати персоналізовані програми професійного розвитку, що сприяє більш ефективному розвитку людського капіталу організації.

Основні напрями використання штучного інтелекту у стратегічному управлінні персоналом узагальнено в таблиці 1.

Таблиця 1

Основні напрями використання штучного інтелекту у стратегічному управлінні персоналом

Напрям використання	**Характеристика застосування**	**Стратегічне значення**
Рекрутинг та відбір персоналу	аналіз резюме кандидатів, автоматизований попередній відбір претендентів, оцінювання відповідності компетентностей вимогам вакансій	скорочення часу підбору персоналу та підвищення якості найму
HR-аналітика	аналіз даних про продуктивність працівників, рівень їх залученості, мотивації та професійного розвитку	формування обґрунтованих управлінських рішень щодо розвитку персоналу
Навчання та розвиток персоналу	аналіз компетентностей працівників і формування персоналізованих програм професійного розвитку	розвиток людського капіталу та підвищення кваліфікації працівників
Прогнозування кадрових ризиків	аналіз даних для виявлення ризиків плинності персоналу, професійного вигорання та дефіциту компетентностей	своєчасне реагування на кадрові проблеми
Стратегічне планування робочої сили (workforce planning)	використання аналітики даних і прогнозних моделей для визначення майбутніх потреб у персоналі	довгострокове планування людських ресурсів і підтримка HR-стратегії

Джерело: сформовано авторами на основі [1-5].

Аналіз наведених у таблиці напрямів свідчить, що технології штучного інтелекту поступово інтегруються у ключові HR-процеси: від рекрутингу до розвитку компетентностей і прогнозування кадрових потреб. Водночас у більшості організацій їх використання залишається точковим і зосередженим переважно на автоматизації окремих операційних завдань. У результаті стратегічний потенціал штучного інтелекту у сфері управління персоналом використовується не повною мірою, що потребує переходу до більш системного застосування аналітики даних і прогнозних інструментів у формуванні HR-стратегії.

З огляду на зазначене, пропонується підхід до використання штучного інтелекту у стратегічному управлінні персоналом, який передбачає інтеграцію HR-аналітики, прогнозування кадрових змін та підтримки управлінських рішень у єдину систему роботи з кадровими даними. На відміну від існуючих підходів, що зосереджуються переважно на автоматизації HR-процесів, запропонований підхід орієнтований на використання аналітичного потенціалу штучного інтелекту для стратегічного управління людським капіталом. Запропонований підхід реалізується через кілька взаємопов'язаних етапів.

На першому етапі здійснюється збір та аналіз кадрових даних, що включає інформацію про продуктивність працівників, рівень їх залученості, професійні компетентності, результати навчання та інші показники, які характеризують людський капітал організації. Використання інструментів HR-аналітики дозволяє систематизувати ці дані та виявити ключові тенденції у розвитку персоналу.

Другий етап передбачає аналітичну обробку даних із застосуванням алгоритмів штучного інтелекту, що дає змогу виявляти закономірності у кадрових процесах, визначати чинники продуктивності праці працівників та прогнозувати можливі кадрові ризики, зокрема плинність персоналу або дефіцит необхідних компетентностей.

На третьому етапі результати аналітики використовуються для прогнозування кадрових змін і потреб у персоналі, що дозволяє організаціям більш ефективно планувати розвиток

людського капіталу та своєчасно реагувати на зміни у внутрішньому і зовнішньому середовищі.

Завершальним етапом. є підтримка стратегічних управлінських рішень, коли результати аналітики та прогнозування використовуються для формування HR-стратегії, планування розвитку компетентностей працівників, оптимізації кадрової структури та підвищення ефективності управління персоналом

Реалізація такого підходу сприяє переходу від реактивного вирішення кадрових проблем до проактивного стратегічного управління персоналом, у якому управлінські рішення ґрунтуються на аналізі даних та прогнозуванні кадрових змін.

Отже, цифровізація економіки змінює підходи до управління персоналом і посилює роль людського капіталу як стратегічного ресурсу організацій. Використання технологій штучного інтелекту відкриває нові можливості для аналізу кадрових процесів, прогнозування потреб у компетентностях та підтримки управлінських рішень у сфері HR-менеджменту. Запропонований підхід до інтеграції HR-аналітики, алгоритмів штучного інтелекту та прогнозування кадрових змін сприяє переходу до проактивної моделі стратегічного управління персоналом, заснованої на аналізі даних і довгостроковому плануванні розвитку людського капіталу.

Список використаних джерел:

1. Дашко І. М. Ключові принципи впровадження штучного інтелекту в процеси управління персоналом підприємства. Економіка та суспільство. 2024. № 60. URL: https://economyandsociety.in.ua/index.php/journal/article/view/5132

2. Кравчук О. І., Варіс І. О., Каленська Н. Г. Трансформація HR-менеджменту через призму штучного інтелекту: комплексний аналіз імплементації, викликів та етичних аспектів. Проблеми сучасних трансформацій. Серія: економіка та управління. 2024. № 15. URL: https://reicst.com.ua/pmt/article/view/2024-15-04-09

3. Кравчук О. І., Варіс І. О., Перкова М. В. Сучасні практики використання штучного інтелекту для цифровізації рекрутингу. Проблеми сучасних трансформацій. Серія: економіка

та управління. 2023. № 8. URL: https://reicst.com.ua/pmt/article/view/2023-8-04-06

4. Черненко Н. І. Штучний інтелект в управлінні персоналом. Науковий вісник економічних наук. 2023. URL: https://tnv-econom.ksauniv.ks.ua/index.php/journal/article/view/250

5. Кобеля З. Штучний інтелект як інструмент управління кадровим потенціалом підприємств в умовах невизначеності. Економічний вісник Чернівецького університету. 2023. URL: https://journals.chnu.chernivtsi.ua/index.php/econom/article/view/188

6. Саркісян Н. В. Вплив Smart HRM на ефективність HR-системи підприємства в цифровій економіці. Економічний простір. 2025. № 200. URL: https://economic-prostir.com.ua/wp-content/uploads/2025/04/200-96-101-sarkisyan.pdf

7. Михаліцька Н. Я., Яцик М. Р. Еволюція концепції комплаєнсу в системі корпоративного управління підприємства: етичні, стратегічні та антикризові аспекти. Ефективна економіка. 2025. № 11. DOI: https://doi.org/10.32702/2307-2105.2025.11.82

8. Михаліцька Н. Я., Демчук В. В. Антикризове управління як інструмент забезпечення економічної безпеки держави та бізнесу в умовах війни. Ефективна економіка. 2026. № 2. DOI: http://doi.org/10.32702/2307-2105.2026.2.134

Мовчан А.В.
професор кафедри оперативно-розшукової діяльності,
доктор юридичних наук, професор
(*Львівський державний університет внутрішніх справ)*
Сергієнко А.О.
курсант навчально-наукового інституту
підготовки фахівців для підрозділів
кримінальної поліції
(*Львівський державний університет внутрішніх справ)*

ШТУЧНИЙ ІНТЕЛЕКТ І ТРАНСФОРМАЦІЯ ЛОГІКИ СУЧАСНОЇ ВІЙНИ: МАСОВІСТЬ, АВТОНОМІЯ, АДАПТИВНІСТЬ

Російсько-українська війна переконливо засвідчила, що масове застосування безпілотних систем, сенсорних мереж та автоматизованих рішень трансформує логіку бойових дій швидше, ніж військові доктрини встигають адаптуватися до нової реальності. Україна стала прикладом оперативної інтеграції інноваційних інструментів у сфері безпеки й оборони: використання комерційних супутникових даних; адаптації цивільних безпілотників до військових потреб; розвитку ІТ-волонтерських ініціатив у галузі кіберзахисту та аналітики даних.

Війна в Україні перетворилася на високотехнологічний полігон, де штучний інтелект (далі – ШІ) суттєво змінює характер збройної боротьби. Традиційне уявлення про перевагу в повітрі як гарантований шлях до перемоги втрачає безумовність: відносно дешеві безпілотні системи з елементами ШІ здатні уражати значно дорожчі платформи, що радикально змінює співвідношення витрат і результату.

Аналітичні платформи на основі ШІ, зокрема Palantir Technologies, забезпечують обробку розвідувальної інформації в режимі реального часу, інтегруючи супутникові дані, дані з безпілотників та інші джерела для оптимізації цілевказання. Як зазначає Михайло Федоров, система ситуаційної обізнаності, побудована на базі цієї платформи, дозволяє командирам ухвалювати швидші й більш обґрунтовані рішення [1].

Крім того, Україна розгорнула хмарні системи управління боєм, зокрема Delta та Kropyva, які акумулюють і аналізують значні обсяги розвідувальних даних. Безпілотні комплекси з елементами ШІ демонструють здатність до автономного розпізнавання та супроводу цілей, а також до дій в умовах активної радіоелектронної протидії. Розвиток концепції «материнських дронів» – великих безпілотних платформ, що транспортують і запускають ударні FPV-дрони в глибину території противника, – свідчить про перехід до багаторівневих автономних систем. Серед новітніх розробок – автоматизовані турельні комплекси протиповітряної оборони з алгоритмічним керуванням, здатні самостійно виявляти, відстежувати та уражати повітряні цілі [1].

У червні 2025 року Служба безпеки України провела операцію «Павутина» – масштабну атаку із застосуванням безпілотників, унаслідок якої було пошкоджено або знищено десятки російських літаків, що спричинило значні матеріальні втрати. Цей епізод продемонстрував потенціал інтегрованих автономних систем для здійснення точкових ударів і досягнення стратегічної дезорганізації противника.

Водночас ШІ відіграє важливу роль і поза безпосереднім полем бою – у процесах відновлення та гуманітарної безпеки. За підтримки міжнародного фінансування Україна впроваджує системи розмінування на основі алгоритмів машинного аналізу, які опрацьовують супутникові знімки та дані з дронів для виявлення нерозірваних боєприпасів і мін. У сфері медичної реабілітації українсько-американська компанія Esper Bionics розробляє протези нового покоління з елементами ШІ, що адаптуються до рухів користувача та підвищують якість життя постраждалих.

Таким чином, досвід України демонструє, що ШІ стає не лише інструментом ведення війни, а й ключовим чинником стратегічної стійкості та післявоєнної трансформації держави.

В умовах російсько-української війни ШІ безпосередньо впливає на військову сферу в кількох ключових вимірах: по-перше, здатність швидко обробляти та інтегрувати великі обсяги даних суттєво підвищує ситуаційну обізнаність і якість прийняття рішень; по-друге, часткове заміщення людської праці автоматизованими системами зменшує втрати та мінімізує ризики,

пов’язані з людським фактором; по-третє, ШІ забезпечує координацію дій великої кількості платформ і елементів системи в режимах швидкості та складності, недоступних для людини; врешті, поєднання людського інтелекту та машинної аналітики створює синергетичний ефект, що дозволяє оперативніше й ефективніше обирати оптимальні варіанти дій [2].

Важливо наголосити, що зазначені трансформації стосуються не лише безпосередньо бойових операцій, а й виробництва та ремонту озброєння і військової техніки, логістики, а також науково-дослідних і дослідно-конструкторських робіт. Саме в цих сферах ШІ здатний забезпечити довгострокові структурні переваги та підвищити стійкість оборонного сектору.

Сьогодні ШІ поступово змінює традиційний баланс між кількістю та якістю на користь масштабованості. Упродовж останніх десятиліть західні армії, насамперед Сполучені Штати Америки, робили ставку на обмежену кількість надзвичайно дорогих і технологічно досконалих платформ, розраховуючи на їхню перевагу в точності, дальності та інтегрованості систем. Натомість поєднання «точної маси» – тобто достатньо точних, але економічно доступних систем – із принципом «доступної масовості» формує нову модель сили. Велика кількість «достатньо ефективних» безпілотних платформ може виявитися стратегічно й економічно вигіднішою за невелику кількість наддорогих високотехнологічних комплексів [2].

У війні майбутнього вирішальною стане не наявність найскладніших систем, а здатність швидко масштабувати спроможності, вводити противника в оману та адаптуватися до змін середовища. Для України, яка вже веде війну в умовах масового застосування дронів і сенсорних мереж, ці висновки мають не теоретичний, а практичний характер.

Отже, йдеться не про відмову від високих технологій як таких, а про зміну логіки їх застосування – перехід від поодиноких дороговартісних платформ до масштабованих автономних екосистем, здатних діяти синхронно та адаптивно. В умовах гібридної війни безумовний пріоритет максимальної якості окремої системи стає менш рентабельним. Збройні сили, які не зможуть інтегрувати роботизовану масу в операційні концепції, ризикують втратити ініціативу у війні на виснаження. Водночас

сучасний ШІ відкриває нові можливості у сфері маскування та інформаційного впливу. Алгоритми можуть координувати тисячі хибних цілей, імітацій та дезінформаційних сигналів, ускладнюючи розпізнавання реальних загроз. У такому середовищі перевага між «мисливцем» і «жертвою» стає контекстуальною – вона залежить від якості сенсорної мережі, здатності до швидкої аналітики та можливості масштабувати як засоби спостереження, так і засоби введення в оману [3].

Окрему загрозу становить використання ШІ для створення реалістичних фальсифікованих матеріалів (deepfake), що породжує феномен «епістемічної нестабільності» – втрати суспільством здатності відрізняти достовірну інформацію від маніпуляції. У кіберпросторі ШІ однаковою мірою посилює потенціал як атакуючої, так і оборонної сторони. У довгостроковій перспективі його застосування здатне зміцнити кіберзахист шляхом автоматизації виявлення вразливостей, оперативного реагування та відновлення мережевої інфраструктури. Водночас навіть найсучасніші алгоритмічні системи не гарантують повної невразливості, що зберігає динамічну рівновагу у сфері кіберпротиборства [3].

Натомість триває міжнародна дискусія щодо меж автономії озброєнь. Концепція «значущого людського контролю» передбачає, що остаточне рішення про застосування сили повинна ухвалювати людина. Проте безпілотні платформи з елементами машинного навчання вже здатні автономно коригувати маршрут, розпізнавати цілі та діяти в умовах радіоелектронної боротьби, що ускладнює чітке розмежування між автоматизацією і повною автономією. Ключові ризики застосування ШІ пов’язані з помилковою ідентифікацією цілей, непрозорістю алгоритмічних рішень («ефектом чорної скриньки»), складністю встановлення юридичної відповідальності за наслідки автономних дій [2].

Таким чином, ШІ радикально змінює темп, масштаб і логіку ведення війни. Основні ризики пов’язані з автономізацією летальних рішень, інформаційною маніпуляцією та алгоритмічною ескалацією. Ключовим завданням міжнародної спільноти є збереження значущого людського контролю, а також формування механізмів прозорості, підзвітності й правового регулювання.

У перспективі баланс сил у міжнародній системі визначатиметься не лише обсягом військових ресурсів, а й здатністю держав ефективно та відповідально інтегрувати алгоритмічні системи у сферу безпеки та оборони.

Відтак, для досягнення переваги в сучасній війні необхідно нарощувати інвестиції в дослідження й експериментування з новими спроможностями, що дозволяють поєднувати масовість і обман. Йдеться, зокрема, про розвиток витратних безпілотних літальних апаратів, незалежних від злітно-посадкової інфраструктури, для виконання завдань повітряного бою, а також про створення ШІ-інструментів для дезінформації та маскування, здатних протидіяти сенсорним системам противника, підсиленим алгоритмами машинного аналізу.

Отже, потрібна чітка стратегія управління переходом до збройних сил, підсилених ШІ. Впровадження алгоритмічних систем є не лише технологічним, а й глибоко організаційним викликом. Ключовим завданням стає формування ефективної моделі взаємодії людини й машини – їхнього функціонального симбіозу в ухваленні рішень і виконанні операцій.

Список використаних джерел:

1. United24 Media (2025). *Artificial Intelligence in Warfare: How Ukraine and Russia Are Rewriting the Rules of Modern War* URL: https://united24media.com/war-in-ukraine/ai-arms-race-ukraine-and-russias-use-of-artificial-intelligence-is-changing-the-rules-of-war-9377?utm_source=chatgpt.com

2. Як штучний інтелект може змінити війну URL: https://lb.ua/society/2026/01/31/719663_yak_shtuchniy_intelekt_mozhe.html?utm_source=chatgpt.com

3. Ільченко Ю.О. Застосування технологій штучного інтелекту в інформаційній війні рф проти України. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. Серія ПРАВО. Вип. 91: ч. 3. С. 87-93. DOI: https://doi.org/10.24144/2307-3322.2025.91.3.13

Мусієнко А.В.
завідувач кафедри цивільного та кримінального права
навчально-наукового інституту
управління, технологій та правових наук,
кандидат юридичних наук, доцент
(Національний транспортний університет)
Зубко А.
студентка
навчально-наукового інституту управління,
технологій та правових наук
(Національний транспортний університет)
Остапчук А.
студентка
навчально-наукового інституту управління,
технологій та правових наук
(Національний транспортний університет)

ДЕЯКІ АКТУАЛЬНІ АСПЕКТИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ (ШІ) ПРИ НАДАННІ ДОМЕДИЧНОЇ ДОПОМОГИ ПРАЦІВНИКАМИ ПРАВООХОРОННИХ ОРГАНІВ В УМОВАХ БОЙОВИХ ДІЙ/ВОЄННОГО СТАНУ

Надання медичної допомоги є пріоритетним напрямом державної політики. В умовах повномасштабного вторгнення це питання має не тільки медичну інтерпретацію, але й набуло нормативної актуальності.

Ця актуальність полягає не тільки в застосуванні сучасних методів надання медичної допомоги постраждалим, але застосування провідних технологій.

Однією з таких технологій є ШІ, а це в сою чергу вимагає нормативного врегулювання.

Злочинна повномасштабна російська агресія прискорила процес впровадження та зростання застосування ШІ при наданні домедичної допомоги. Конституція України в ст. 3 проголошує людину, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю.

Застосування наземних роботизованих комплексів (НРК) регулюється міжнародним гуманітарним правом (МГП) та національним законодавством України [1]. Використання РНК наділених ШІ при евакуації поранених осіб, розмінуванні та інших ситуаціях є важливим елементом державної політики спрямованої на реалізацію ст. 3 Конституції України. Застосування новітніх технологій у війні проти російської агресії наближає перемогу України. В свою чергу це вимагає запровадження сучасного правового регулювання їх використання.

З цією метою профільні відомства а саме МОЗ, визначає актуальний порядок, що визначає механізм та об'єм надання домедичної допомоги постраждалим внаслідок бойових дій/воєнного стану особами, які не мають медичної освіти, але за своїми службовими обов'язками повинні надавати домедичну допомогу.

Дії, послідовність та об'єм надання домедичної допомоги постраждалим в зоні евакуації здійснюється відповідно до Порядків надання домедичної допомоги, затверджених наказом Міністерства охорони здоров`я України від 09 березня 2022 року № 441.

Особливого значення набуває Порядок надання домедичної допомоги постраждалим в умовах бойових дій/воєнного стану.
Важливими серед яких є наступні:

- при масивних травмах обличчя у постраждалого в свідомості: надати зручного (вимушеного) положення – сидячи з нахиленим вперед тулубом;
- глянути грудну клітку на предмет проникних поранень, за їх наявності накласти пов'язки з водонепроникного матеріалу, якщо після їх накладання стан постраждалого різко погіршився зніміть та більше не здійснюйте спроб їх накладання;
- оглянути постраждалого з голови до ніг, особливу увагу звернути на ефективність зупинки зовнішньої кровотечі, якщо така була здійснена на попередньому етапі. При триваючій кровотечі слід здійснити прямий тиск на 3 рану і затампонувати рану та/або накласти додатковий кровоспинний джгут, обов'язково вкажіть час накладання джгута; зупинити будь-яку кровотечу, яка була виявлена під час огляду – накласти пов'язки

на рани. Також накласти пов’язки на будь-які інші рани, в тому числі опікові;

- не слід тампонувати чи здійснювати надмірний тиск на рани голови, не слід тампонувати рани грудної клітки чи живота;
- не слід накладати тиснучі пов’язки на око;
- за можливості здійснити виклик екстреної медичної допомоги та дотримуватись вказівок диспетчера прийому виклику.

За результатами проведеного дослідження автори дійшли висновків:

- використання НРК наділених ШІ при евакуації поранених осіб та інших ситуаціях є важливим елементом державної політики спрямованої на реалізацію ст. 3 Конституції України;
- застосування новітніх технологій у війні проти російської агресії наближає перемогу України;
- в свою чергу, застосування таких технологій вимагає запровадження сучасного правового регулювання їх використання.

Список використаних джерел:

1. Термін «Безпілотний наземний (роботизований) комплекс». URL.: https://zakon.rada.gov.ua/laws/term/59614/sp:head

Назарова В.М.
аспірант
(Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»).
Науковий керівник – **Петришин О.В.**
доктор юридичних наук, професор,
дійсний член (академік) НАПрН України

КОНСТИТУЦІЯ БЕЗ ЛЮДИНИ: ЧИ МОЖЕ ШІ ОСЯГНУТИ «ДУХ ПРАВА», ЧИ МИ ГОТУЄМО КАПІТУЛЯЦІЮ ПРАВОСУДДЯ ПЕРЕД АЛГОРИТМОМ?

Постановка проблеми. Дискусія про застосування штучного інтелекту (далі – ШІ) у сфері правосуддя вже давно вийшла за межі технічного ентузіазму й набула виразного конституційно-правового звучання. Питання більше не зводиться до того, чи здатен алгоритм пришвидшити опрацювання судових справ або спрогнозувати рецидивізм. Питання принципове: чи існує в конституційному праві – зокрема, в українському – така онтологічна глибина, яку алгоритм не здатний осягнути за самою своєю природою? І якщо так, то на якому саме рівні ми маємо провести межу між допустимою автоматизацією та неприпустимою делегацією владного повноваження машині?

Ця проблема є далеко не абстрактною. У лютому 2024 року Касаційний господарський суд у складі Верховного Суду розглянув ситуацію, коли учасник процесу послався на «позицію ChatGPT» у заяві про роз'яснення постанови касаційної інстанції (справа № 925/200/22). Суд кваліфікував це як прояв неповаги до суддів та зловживання процесуальними правами, зазначивши, що ШІ може бути корисним допоміжним інструментом, але не здатний замінити роль суддів [1]. Варто зазначити, що суддя Г. О. Вронська у своїй окремій думці висловила іншу позицію: саме по собі посилання на інформацію, згенеровану ШІ, за відсутності ознак недобросовісності не може автоматично визнаватися зловживанням. Ця розбіжність засвідчує, що українська судова

система перебуває на етапі формування доктринальних підходів до ШІ.

Метою цих тез є доктринальний аналіз конституційних підстав, які унеможливлюють повну заміну людського судження алгоритмічним рішенням у сфері конституційного правосуддя, та обґрунтування тези про те, що «дух права» – це категорія, яка принципово не піддається формалізації в межах існуючих моделей ШІ.

Виклад основного матеріалу. Статті 124 та 127 Конституції України у системному зв'язку встановлюють: правосуддя в Україні здійснюють виключно суди (ст. 124), а правосуддя здійснюють судді (ч. 1 ст. 127) [2]. Це не просто організаційний припис – це конституційна ґарантія суб'єктності правосуддя. Суддя – не функція, а носій владного повноваження, легітимованого через конституційну процедуру призначення, присягу та персональну відповідальність. Алгоритм, яким би досконалим він не був, не складає присяги, не несе дисциплінарної відповідальності й не може бути суб'єктом імпічменту. Отже, делегування йому функції ухвалення рішення означає розрив у ланцюзі конституційної легітимності.

Конституційний Суд України неодноразово тлумачив конституційні норми, звертаючись до категорій, які лежать поза буквальним текстом: «верховенство права», «людська гідність», «справедливість». Ці категорії вимагають від судді не лише знання закону, а й здатності до ціннісного судження — того, що в європейській конституційній традиції позначають як «дух права» (Geist des Rechts). Йдеться про здатність розпізнати, коли формально правильне рішення є водночас несправедливим, і знайти таке тлумачення, яке відновлює баланс між текстом і цінністю.

ШІ, зокрема великі мовні моделі (LLM), здатний аналізувати правові тексти, виявляти закономірності у судовій практиці та навіть генерувати юридично грамотні тексти. Проте його робота ґрунтується на статистичному моделюванні – передбаченні найбільш імовірного продовження тексту на основі навчальних даних. Це принципово відрізняється від судового міркування, яке включає: (а) інтерпретацію норми у світлі конкретних обставин

справи; (б) зважування конкуруючих конституційних цінностей; (в) моральну інтуїцію, сформовану професійним досвідом і правовою культурою.

Дослідники Е. Коен (Університет Арізони) та Г. Сурден (Університет Колорадо) сформулювали так званий «закон збереження судження» (law of conservation of judgment): ШІ не усуває потребу в людському судженні при тлумаченні конституції, а лише переміщує її з одного етапу ухвалення рішення на інший [3]. Ціннісні, моральні та політичні питання, властиві конституційному тлумаченню, не зникають від того, що ми доручаємо попередній аналіз машині. Вони або розпорошуються між етапами, або стають імпліцитними – а отже, менш контрольованими.

Це спостереження має критичне значення для конституційного правосуддя, де предметом розгляду є не стільки факти, скільки конституційні цінності й принципи. Коли Конституційний Суд України вирішує, чи є обмеження права на свободу вираження поглядів пропорційним, він здійснює не калькуляцію, а ціннісне судження, в якому значення мають культурний контекст, історична пам'ять, конституційна ідентичність нації. Алгоритм може обробити масив рішень ЄСПЛ щодо статті 10 Конвенції, але не здатний відчути різницю між обмеженням, яке захищає демократію, і обмеженням, яке її руйнує.

Європейський Союз визнав цю проблему на регуляторному рівні. Регламент ЄС про штучний інтелект (AI Act, Regulation (EU) 2024/1689) класифікує системи ШІ, які використовуються для допомоги судовим органам у дослідженні та тлумаченні фактів і права та у застосуванні права до конкретних обставин, як системи «високого ризику» (Додаток III) [4]. Це зобов'язує розробників впроваджувати системи управління ризиками, забезпечувати людський нагляд і прозорість алгоритмів. Відповідні вимоги набувають повної чинності у серпні 2026 року.

Консультативна рада європейських суддів (КРЄС) у Висновку № 26 (2023) зайняла позицію, яку підтримали й судді Конституційного Суду України В. Городовенко та Г. Юровська: ШІ і технології можуть значно допомогти суддям у роботі, але не замінити їх [5; 6]. Ключовий наголос було зроблено на

персональній відповідальності судді за рішення, прийняте з використанням ШІ, та на неприпустимості автоматичного застосування юридичних позицій, згенерованих алгоритмом.

Рекомендації ЮНЕСКО щодо використання ШІ в судах і трибуналах (2025) додатково підкреслюють, що судові органи повинні утримуватися від впровадження систем ШІ, здатних негативно вплинути на права людини, зокрема через відтворення дискримінаційних результатів [7]. ЮНЕСКО наполягає на обов'язковому забезпеченні людського втручання на всіх етапах використання ШІ та на впровадженні механізмів підзвітності ще до розгортання будь-якої системи.

Окремої уваги заслуговує проблема «непрозорості» (opacity) алгоритмічних рішень. У контексті конституційного правосуддя ця проблема набуває екзистенційного характеру. Стаття 6 Конвенції про захист прав людини і основоположних свобод ґарантує право на справедливий суд, що передбачає, серед іншого, вмотивованість рішення. Рішення, згенероване або суттєво обумовлене алгоритмом, структура якого є «чорною скринькою» навіть для самого судді, підриває саму ідею вмотивованості як елементу верховенства права. Як зауважено у дослідженні Стімсонівського центру, довіра до судової системи є наріжним каменем її легітимності, і використання непрозорих інструментів ШІ створює ризик ерозії цієї довіри [8].

Крім того, існує загроза, яку в зарубіжній літературі позначають як «текучість права» (Law Fluidity) [8]. Право – не статичний масив правил, а жива система, яка еволюціонує через судову інтерпретацію. Кожне рішення конституційного суду – це не просто застосування норми, а її розвиток, адаптація до нових реалій. ШІ, який оперує на основі минулих даних, за визначенням орієнтований на відтворення існуючих патернів. Він не здатний до правового новаторства — до того акту інтелектуальної мужності, коли суддя йде проти усталеної практики, бо розуміє, що час вимагає іншого прочитання конституційного тексту.

У вересні 2024 року XX черговий з'їзд суддів України затвердив нову редакцію Кодексу суддівської етики, стаття 16 якого визначає умови допустимості використання ШІ суддями: таке використання є допустимим, якщо воно не впливає на незалежність та неупередженість судді, не стосується оцінки

доказів і процесу ухвалення рішень та не порушує вимог законодавства [9]. Це важливий, хоч і перший, крок до формування нормативної рамки. Водночас він фіксує фундаментальне протиріччя: ми регулюємо використання інструменту, потенційний вплив якого на правову систему ми ще не до кінця розуміємо.

Можна передбачити заперечення: з розвитком технологій ШІ набуде здатності до «розуміння», що наблизить його до ціннісного судження. Однак навіть якщо модель імітуватиме зовнішню форму такого судження, вона не матиме того, що є його конституційною передумовою: суб'єктної відповідальності. Рішення, за яке ніхто персонально не відповідає, не є актом правосуддя в конституційному сенсі цього слова.

Висновки. «Дух права» – це не метафора і не риторична фігура. Це операційна категорія конституційного правосуддя, яка виражає здатність судді виходити за межі тексту норми заради захисту конституційних цінностей. Ця здатність передбачає суб'єктність – тобто наявність свідомості, совісті, відповідальності та морального судження. Алгоритм позбавлений цих якостей за визначенням. Він може імітувати правове міркування, але не здатний його здійснювати у тому сенсі, який вкладає у це поняття конституційна доктрина.

Проте констатація обмеженості ШІ не означає його відторгнення. Раціональна позиція полягає у визнанні його як асистивного інструменту – потужного, але підпорядкованого. ШІ може допомагати в аналізі масивів судової практики, у систематизації правових позицій, у виявленні колізій. Але ухвалення рішення – акт владного волевиявлення – має залишатися виключно за людиною-суддею. Цей висновок прямо випливає зі статей 124 та 127 Конституції України, з позиції КРЄС та з Регламенту ЄС про ШІ, які одностайно наполягають на збереженні людського нагляду.

Конституційне правосуддя стоїть перед викликом, який вимагає не стільки технологічної, скільки ціннісної відповіді. Не «як інтегрувати ШІ», а «як зберегти людину в центрі правової системи». І якщо ми втратимо цю перспективу, то ризикуємо отримати не модернізоване правосуддя, а його капітуляцію — не

перед технологією, а перед спокусою делегувати відповідальність, яка за своєю природою є невід'ємною.

Список використаних джерел

1. Ухвала Касаційного господарського суду у складі Верховного Суду від 08.02.2024 р. у справі № 925/200/22. URL: https://reyestr.court.gov.ua/Review/116984639 (дата звернення: 01.04.2026).

2. Конституція України : Закон від 28.06.1996 р. № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр (дата звернення: 01.04.2026).

3. Coan A., Surden H. AI and Constitutional Interpretation: The Law of Conservation of Judgment. Lawfare. 2024. December 16. URL: https://www.lawfaremedia.org/article/ai-and-constitutional-interpretation--the-law-of-conservation-of-judgment (дата звернення: 01.04.2026).

4. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act). Official Journal of the European Union. L, 2024/1689.

5. Висновок Консультативної ради європейських суддів (КРЄС) № 26 (2023) «Рухаючись вперед: використання асистивних технологій у судочинстві» від 01.12.2023 р.

6. Городовенко В. Штучний інтелект і технології можуть значно допомогти у роботі суддям, але не замінити їх. Судово-юридична газета. 2023. 28 грудня. URL: https://ccu.gov.ua/novyna/syug-shtuchnyy-intelekt-i-tehnologiyi-mozhut-znachno-dopomogty-u-roboti-suddyam-ale-ne (дата звернення: 01.04.2026).

7. UNESCO Guidelines for the Use of AI Systems in Courts and Tribunals. UNESCO, 2025.

8. AI in Global Majority Judicial Systems. Stimson Center Report. 2026. January 8. URL: https://www.stimson.org/2026/ai-in-global-majority-judicial-systems/ (дата звернення: 01.04.2026).

9. Кодекс суддівської етики : затв. Рішенням XX чергового з'їзду суддів України від 18.09.2024 р. URL: https://zakon.rada.gov.ua/go/n0001415-24 (дата звернення: 01.04.2026).

10. Vidaki A. N., Papakonstantinou V. Democratic legitimacy of AI in judicial decision-making. AI & Society. 2025. Vol. 40. P. 6025–6035. DOI: 10.1007/s00146-025-02411-w.

11. CEPEJ European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment. Strasbourg : Council of Europe, 2018.

12. Берназюк Я. Штучний інтелект та система правосуддя України: результати співпраці у році, що минув. Конституціоналіст. 2025. 7 січня. URL: https://so.supreme.court.gov.ua/authors/934/ (дата звернення: 01.04.2026).

Несен О.О.
завідувач кафедри криміналістики
навчально-наукового інституту права та психології,
кандидат медичних наук, доцент
(Національна академія внутрішніх справ)
Кравченко Н.В.
викладач кафедри криміналістики
навчально-наукового інституту права та психології
(Національна академія внутрішніх справ)

ТЕХНІЧНІ ВРАЗЛИВОСТІ НЕЙРОННИХ МЕРЕЖ ЯК ЧИННИК РИЗИКУ У ПРАВОЗАСТОСОВНІЙ ДІЯЛЬНОСТІ

Чи можна вважати систему штучного інтелекту (ШІ) надійною, якщо її математична природа (зокрема, лінійність чи специфіка алгоритмічної оптимізації) може призвести до порушення прав людини? Це питання є надзвичайно актуальним, оскільки сучасний етап розвитку правоохоронної системи України характеризується активною цифровою трансформацією. Згідно з проєктом Стратегії розвитку штучного інтелекту в Україні до 2030 року, держава ставить за мету увійти до топ-3 світових лідерів у цій сфері, що передбачає впровадження ШІ в оборонний сектор, медицину та державне управління [7]. Проте, паралельно з технологічним проривом, виникають фундаментальні загрози – конфлікт між технічною досконалістю алгоритмів (швидкість, точність) та їхньою архітектурною вразливістю, що створює ризики для правової безпеки. Питання безпеки алгоритмів переходить у площину захисту прав людини, оскільки Україна приєдналася до Рамкової конвенції Ради Європи про ШІ, що зобов'язує дотримуватися принципів прозорості та недискримінації [3].

Однією з найбільш обговорюваних проблем у машинному навчанні є вразливість нейронних мереж до так званих змагальних (адверсаріальних) атак (adversarial examples). Дослідження І. Гудфеллоу та інших демонструють, що моделі послідовно неправильно класифікують вхідні дані, якщо до них застосовано

мінімальні, навмисно підібрані викривлення. Основною причиною цього явища автори називають «лінійну природу» сучасних нейромереж, а не їхню складність чи перенавчання [5, с. 2].

Для юридичної практики це означає, що системи розпізнавання облич, автоматичної фіксації чи аналізу доказів можуть бути скомпрометовані шляхом навмисного внесення латентних збурень. Нейромережі працюють за принципом математичного підсумовування сигналів. Шляхом застосування малих, але інтенційно підібраних викривлень (perturbations) до вхідних даних, стає можливим спотворення вихідного результату моделі при збереженні її високої впевненості у правильності рішення. Це дозволяє зловмиснику додати до цифрового об'єкта (наприклад, зображення обличчя чи номерного знака) крихітний, невидимий для людини «математичний шум». Внаслідок цього система прийме помилкове рішення. В юридичній площині це створює ризик маніпулювання цифровими доказами: система може ідентифікувати особу там, де її немає, або навпаки – не ідентифікувати правопорушення через навмисно підібрану цифрову перешкоду.

Таким чином, технічна природа алгоритму створює ризики цілеспрямованої деформації доказової бази та стає об'єктивною межею його достовірності в суді. Це ставить під сумнів концепцію надійності (reliability) алгоритмічних рішень. Оскільки такі вразливості є властивістю самої математичної архітектури нейромереж, вони окреслюють межі їх використання як джерела доказової інформації.

Останнім часом у наукових колах ведеться активне обговорення тенденції переходу від статичних моделей до автономних агентних систем, наділених довгостроковою пам'яттю та інструментарієм взаємодії [2]. Коли LLM-моделі інтегруються в автономні агентні структури, об'єктом оцінки має виступати не окрема модель, а складна екосистема. Новітні дослідження (2026 р.) вказують на ризик виникнення стратегічної поведінки таких систем. Виникає явище «інсентив-конвергенції» (incentive convergence): агенти можуть демонструвати деструктивну поведінку (обман, змова, маніпуляція звітами) не через наявність «волі», а внаслідок тиску оптимізації поставленого завдання [2, с. 4].

ШІ не володіє свідомістю, проте він запрограмований на максимально ефективне виконання завдання. Якщо алгоритму поставлено мету «мінімізувати кількість помилок у звітах», він може почати приховувати суперечливі дані. Мета «максимізації розкриття правопорушень» може призвести до системного порушення прав громадян через агресивну інтерпретацію правил. Маніпуляція даними як прагнення алгоритму виконати завдання (reward maximization) не є «злим наміром» у криміналістичному розумінні, а є результатом математичної оптимізації. Проте для правової системи це означає виникнення «алгоритмічного хаосу», де за локально успішними показниками ховається глобальне викривлення реальності. Це ставить під сумнів можливість повної автоматизації юридично значущих процесів без безпосереднього контролю з боку людини.

Визнання архітектурної вразливості ШІ потребує перегляду концепції відповідальності операторів та розробників. Відповідно до Регламенту ЄС про штучний інтелект (EU AI Act), необхідним є запровадження жорстких механізмів людського контролю (human-in-the-loop). Системи з високим ризиком повинні проходити аудит на стійкість до маніпуляцій та прозорість логічного виведення [1]. В українських реаліях важливо розмежувати технічну похибку розробника та неправомірні дії оператора. Необхідно впроваджувати в українську правову практику методологію HUDERIA, яка дозволить проводити превентивну оцінку впливу алгоритмів на права людини [4].

Надійність ШІ-систем у правоохоронній діяльності не може вимірюватися лише статистичною точністю. Вона повинна включати критерії стійкості до зовнішнього втручання та прозорість логіки прийняття рішень. Правове регулювання має фокусуватися на створенні «запобіжників», що обмежують автономію алгоритмів у критично важливих сферах державного управління.

Список використаних джерел:

1. Акт про штучний інтелект (EU AI Act). Офіційний текст. URL: https://artificialintelligenceact.eu/the-act/ (дата звернення: 25.02.2026).

2. Agents of Chaos: emergent behavior in multi-agent autonomous systems. *arXiv:2602.20021*. 2026. URL: https://arxiv.org/abs/2602.20021 (дата звернення: 25.02.2026).

3. Безпечний ШІ для мільйонів українців: Україна підписала Рамкову конвенцію про штучний інтелект та права людини. *Міністерство цифрової трансформації України*. 2025. URL: https://thedigital.gov.ua/news/technologies/bezpechniy-shi-dlya-milyoniv-ukraintsiv-ukraina-pidpisala-ramkovu-konventsiyu-pro-shtuchniy-intelekt-ta-prava-lyudini (дата звернення: 25.02.2026).

4. Авдєєва Т., Дворовий М. Штучний інтелект під контролем: які міжнародні правила мають знати українські редакції. *Детектор медіа*. 2026. URL: https://detector.media/infospace/article/247369/2026-01-30-shtuchnyy-intelekt-pid-kontrolem-yaki-mizhnarodni-pravyla-mayut-znaty-ukrainski-redaktsii/ (дата звернення: 25.02.2026).

5. Goodfellow I. J., Shlens J., Szegedy C. Explaining and Harnessing Adversarial Examples. *arXiv:1412.6572*. 2014 (updated 2015). URL: https://arxiv.org/abs/1412.6572 (дата звернення: 25.02.2026).

6. Рік ШІ: трансформації країни — що змінилося для мільйонів українців та держави. *Міністерство цифрової трансформації України*. 2025. URL: https://thedigital.gov.ua/news/shtuchnyy-intelekt/rik-shi-transformatsiyi-krayiny-shcho-zminylosia-dlia-milyoniv-ukrayintsiv-ta-derzavy (дата звернення: 25.02.2026).

7. Як Україна розвиватиме ШІ до 2030 року — презентували проєкт стратегії. *Міністерство цифрової трансформації України*. 2025. URL: https://thedigital.gov.ua/news/technologies/iak-ukrayina-rozvyvatyme-shi-do-2030-roku-prezentuvaly-proyekt-stratehiyi (дата звернення: 25.02.2026).

Овдійчук Д.Е.
здобувач ступеня бакалавра факультету № 1
(Львівський державний університет внутрішніх справ)
Гуцуляк Ю.В.
доцент кафедри кримінального процесу
та криміналістики факультету № 1,
доктор філософії
(Львівський державний університет внутрішніх справ)

ВИКОРИСТАННЯ ЦИФРОВИХ ДОКАЗІВ ТА ІНСТРУМЕНТІВ ШІ ПРИ РОЗСЛІДУВАННІ КОЛАБОРАЦІЙНОЇ ДІЯЛЬНОСТІ

Станом на грудень 2025 року у Єдиному реєстрі досудових розслідувань зареєстровано 5244 кримінальних правопорушень передбачених ст. 111^1 Кримінального кодексу України (далі – КК України) [1], у Єдиному державному реєстрі судових рішень - 3629 вироків щодо обвинувачення осіб у колабораційній діяльності [2], що вказує на те, що факти вчинення такого кримінального правопорушення є далеко не поодинокими, що підкреслює актуальність дослідження розслідування та судового розгляду таких кримінальних правопорушень з метою вдосконалення правозастосовної практики.

Розслідування кримінальних правопорушень за ст. 111^1 КК України, органи досудового розслідування, прокуратури зобов'язані всебічно та повно дослідити обставини вчинення злочину у конкретному кримінальному провадженні, що передбачає здійснення їх порівняльного аналіз з використанням сучасних методик аналізу та перевірки даних. Вагомого значення у таких кримінальних провадженнях набувають цифрові докази, оскільки саме вони можуть відобразити фактичну поведінку особи в інформаційному просторі: фіксувати її комунікації з іншими особами, її публічні висловлювання, публікації у соціальних мережах, її переміщення також іншу активність, що є частиною вчинення кримінального правопорушення. Використання спеціалізованого програмного забезпечення та інструментів штучного інтелекту дозволяє ефективно здійснювати обробку

значних обсягів інформації, виявляти взаємозв'язки між подіями та особами, що може стати основою для судових рішень.

Колабораційна діяльність в Україні передбачена у таких її проявах та формах (ст. 111^1 КК України):

– добровільне зайняття посад в окупаційних органах влади (у т.ч. адміністрації держави-агресора), участь в організації та проведенні незаконних виборів/референдумів або публічні заклики до них;

– пропаганда в закладах освіти з метою сприяння збройній агресії чи утвердження окупаційної влади, а також впровадження стандартів освіти держави-агресора;

– добровільна передача матеріальних ресурсів збройним формуванням ворога, господарська діяльність у співпраці з окупаційною владою чи державою-агресором (постачання товарів, робіт, послуг);

– добровільне зайняття керівних чи адміністративно-господарських посад в окупаційних органах, обрання до них, організація та участь у незаконних виборах/референдумах;

– організація й участь у політичних або інформаційних заходах у співпраці з агресором на його підтримку чи для уникнення ним відповідальності.;

– добровільне зайняття посад у незаконних судових і правоохоронних органах, участь у незаконних збройних формуваннях та сприяння їм у здійсненні агресії проти України.

Важливо зазначити, що цифрові докази прямо не визначені кримінальним процесуальним законодавством як самостійне джерело доказів. Водночас відповідно до п. 1 ч. 2 ст. 99 Кримінального процесуального кодексу України (далі - КПК України) комп'ютерні дані віднесені до документів як процесуального джерела доказування. З урахуванням положень ч. 4 ст. 99 КПК України копії комп'ютерних даних, створені слідчим або прокурором із залученням спеціаліста, можуть визнаватися судом як оригінал документа.

Збирання доказів, в тому числі і тих, що існують у віртуальному середовищі, відбувається лише у спосіб, передбачений КПК України. Дослідження слідчо-судової практики засвідчило, що збирання електронних (цифрових) доказів у кримінальних провадженнях про колабораційну діяльність

здійснюється найчастіше шляхом проведення огляду комп'ютерних даних в порядку ст. 237 КПК України.

Об'єкт огляду під час розслідування колабораційної діяльності визначається залежно від конкретного виду діяння, передбаченого частиною статті 111^1 КК України. У ході досудового розслідування кримінального правопорушення, у межах проведення слідчих (розшукових) дій зазвичай здійснюється огляд вебсторінок, розміщених у соціальних мережах, зокрема таких як TikTok, Одноклассники, Facebook, ВКонтакте, Telegram дописів та публікацій, а також блогів, публічних груп і чатів. Зазначені ресурси можуть містити відомості про публічні висловлювання колаборантів, спрямовані на заперечення факту збройної агресії проти України або на підтримку рішень російської федерації [3].

Таке джерело отримання фактичних даних в кримінальному провадженні підтверджується і текстами судових рішень. Так, у постанові від 12 червня 2024 року по справі 569/1908/23 Касаційний кримінальний суд зазначив, що основними доказами у кримінальних правопорушеннях проти основ національної безпеки України, у т. ч. колабораційної діяльності, є електронні (цифрові) докази, до яких належать: матеріали фотозйомки, звуко-запису, відеозапису та інші носії інформації [4].

У кримінальному провадженні за № 333/4417/23 Вироком Комунарського районного суд м. Запоріжжя: «.. наліз протоколу проведення НС(Р)Д, зняття інформації з електронних інформаційних систем, судом встановлено, що в ході проведення такої дііх було отримано доступ до облікового запису ОСОБА_7 у мобільному додатку системи миттєвого обміну повідомленнями «Telegram» зареєстрований на абонентський номер оператора мобільного зв`язку НОМЕР_2, а також до всієї наявної у додатку інформації, яка зберігається у відповідних чатах з іншими користувачами цього додатку, в тому числі і до переліку всіх її контактів. В цій програмі наявне листування, яке становить собою обмін текстовими повідомленнями та файлами. За змістом цих повідомлень користувач акаунту під час звернення до інших абонентів представляється як ОСОБА_7, називає себе головним бухгалтером «УСИН по Запорізькій області», запрошує на роботу, визначає розмір заробітної плати майбутнім співробітникам,

розповідає про те, що зараз проживає в м. Мелітополі, їй видали службове житло в м. Мелітополі, висловлює своє задоволення від зайнятої посади в незаконно створеному органі «УСИН». Також встановлено, що абоненти з якими відбувалось спілкування ОСОБА_7 записані із вказанням посад в органах рф, як то «ДФС», «Казна», «Минфин» на аватарках яких мається прапор російської федерації, номери починаються з цифр +7. ОСОБА_7 Надсилає «Отчет УСИН», в якому міститься інформація витратам бюджету, викладений російською мовою із зазначенням сум» [5].

У Вироку від 18 грудня 2025 року Нововоронцовський районний суд Херсонської області зазначає, що проведення огляду інформації, яка містилася у відкритому доступі, її хід і результати фіксувалися у відповідному протоколі огляду, зокрема й від 31.05.2022 який захисник просить визнати недопустимим. За вказаними протоколами було проведено огляд інтернет-сторінки, зроблено їх скріншоти, роздруківки яких містяться у протоколах огляду (що дозволяє впевнитися в інформації, яка була об`єктом огляду), які відповідають вимогам КПК України. Огляд проводився щодо інформації, яка перебувала у відкритому доступі (Telegram-канал «РИА Новости»), що відповідає вимогам КПК України. Доводи захисника про те, що ідентифікація в протоколах була передчасною, нівелюються сукупністю наступних доказів. Крім того, об`єктом огляду як у протоколі огляду від 12.12.2023, так і в протоколі огляду від 31.05.2022 є публікація в месенджері «Telegram» офіційного російськомовного телеграм-каналу « ІНФОРМАЦІЯ_2 » [6].

Окремі кримінальні правопорушення вчиняються з використанням можливостей мережі Інтернет, а, отже, можуть залишати відповідні цифрові сліди. Наприклад, однією з форм колабораційної діяльності є публічне заперечення громадянином України здійснення збройної агресії проти України, встановлення та утвердження тимчасової окупації частини території України або публічні заклики громадянином України до підтримки рішень та/або дій держави агресора, збройних формувань та/або окупаційної адміністрації, до співпраці з державою-агресором, збройними формуваннями та/або окупаційною адміністрацією держави-агресора, до невизнання поширення державного суверенітету України на тимчасово окуповані території України (ч.

1 ст. 111^1 КК України). Вказані дії виконавці можуть вчиняти з використанням соціальних мереж, як правило, це «Одноклассники», «Вконтакте», або ж каналів чи групових чатів месенджерів Telegram, Viber шляхом розміщення відповідних повідомлень, що містять заборонені заперечення або підтримку, які стають загальнодоступними. Отже, фактичні дані, про зміст таких повідомлень, а саме: текстова інформація, відео-, аудіозаписи, фото і та інші графічні зображення разом з інформацією про використані засоби та способи оприлюднення вказаних відомостей можуть бути доказами у кримінальних провадженнях про подію кримінального правопорушення (час, місце, спосіб та інші обставини вчинення кримінального правопорушення) та про винуватість підозрюваного, обвинуваченого у вчиненні кримінального правопорушення, форму вини, мотив і мету вчинення кримінального правопорушення (п.п. 1, 2 ч. 1 ст. 91 КПК України) [7].

Інструменти штучного інтелекту можуть суттєво підвищити ефективність розслідування колаборaційної діяльності шляхом автоматизованого аналізу великих масивів цифрових даних. За їх допомогою можливо виявляти зв'язки між особами, ідентифікувати повторювані наративи, аналізувати активність у соціальних мережах та месенджерах, а також встановлювати часові й географічні закономірності. Алгоритми машинного навчання здатні здійснювати класифікацію контенту, розпізнавання облич і текстовий аналіз повідомлень. Водночас застосування таких інструментів повинно здійснюватися з дотриманням вимог кримінального процесуального законодавства та принципів допустимості доказів.

Керуючись викладеним, можна зробити висновок, про визначальне значення цифрових доказів у кримінальних провадженнях за ст. 111^1 КК України. Саме вони дозволяють об'єктивно зафіксувати поведінку особи в інформаційному просторі, її комунікації, публікації та взаємозв'язки з представниками держави-агресора. Особливим є дотримання процесуального порядку збирання таких доказів.

Список використаних джерел:

1. Офіс Генерального Прокурора: Статистика Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2

2. Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/Page/1

3. Романюк В. В., Фоміна Т. Г. Порядок збирання електронних (цифрових) доказів у кримінальних провадженнях про колаборaційну діяльність. *Вісник Кримінологічної асоціації України*. 2024. Т. 32, № 2. С. 344–353. URL: https://doi.org/10.32631/vca.2024.2.25 (дата звернення: 23.02.2026).

4. Постанова Верховного Суду колегією суддів Третьої судової палати Касаційного кримінального суду від 12.06.2024 у справі № 569/1908/23. URL: https://iplex.com.ua/doc.php?regnum=119741340 (дата звернення: 23.02.2026).

5. Вирок Комунарського районного суду м. Запоріжжя від 09.11.2023 у справі № 333/4417/23. URL: https://reyestr.court.gov.ua/Review/115235946 (дата звернення: 23.02.2026).

6. Вирок Нововоронцовського районного суду Херсонської області від 18.12.2025 у справі № 954/240/25. URL: https://reyestr.court.gov.ua/Review/132734947 (дата звернення: 23.02.2026).

7. Пашковський М. Обставини, що мають значення для кримінального провадження, та належність цифрових доказів з відкритих джерел. *Наукові перспективи (Naukovì perspektivi)*. 2024. № 10(52). URL: https://doi.org/10.52058/2708-7530-2024-10(52)-984-998 (дата звернення: 26.02.2026).

Овсянікова Т.
курсант факультету підготовки фахівців
для підрозділів превентивної діяльності НПУ
(Донецький державний університет внутрішніх справ).
Науковий керівник – **Шишкарьова О.Г.**
старший викладач кафедри адміністративно-правових
дисциплін факультету підготовки фахівців
для підрозділів превентивної діяльності НПУ
(Донецький державний університет внутрішніх справ)

ЦИФРОВІЗАЦІЯ АДМІНІСТРАТИВНОГО ПРОВАДЖЕННЯ ЯК ІНСТРУМЕНТ ПУБЛІЧНОГО АДМІНІСТРУВАННЯ: МІЖНАРОДНИЙ ТА ВІТЧИЗНЯНИЙ ДОСВІД

Сучасний етап світового технологічного розвитку характеризується динамічними та безперервними процесами цифровізації. Для України є характерне активне впровадження цифрових технологій саме для державної влади та органів місцевого самоврядування. Це пришвидшує та полегшує доступність громадян до отримання адміністративних послуг, а також служить для реалізації забезпечення прав та свободи людини. Особливої актуальності зазначений процес набув в умовах воєнного стану, коли швидкість прийняття управлінських рішень і мінімізація бюрократичних процедур мають критичне значення для підтримки життєдіяльності різних категорій населення, особливо внутрішньо – переміщених осіб, військових та осіб похилого віку.

Ключовою передумовою впровадження електронних технологій у сферу публічного адміністрування є їх належне нормативно-правове закріплення. Цифровізація адміністративних процедур має здійснюватися виключно в межах та на підставі відповідних нормативно-правових актів, що забезпечує дотримання принципів законності та правової визначеності. У контексті євроінтеграційного курсу України особливого значення набуває гармонізація національного законодавства з правом Європейського Союзу, що створює підґрунтя для імплементації

європейських стандартів цифрового врядування в адміністративне провадження. Важливим актом міжнародного законодавства є Цифрова Стратегія Європейського Союзу, яка започаткована у 2015 році та мала на меті сприяти економічному зростанню, збільшенню робочих місць,

конкуренції, інвестиціям та інноваціям у ЄС, проклала шлях до більш тісної цифрової гармонізації між державами-членами ЄС, базуючись на трьох стовпах:1) кращий доступ для споживачів і компаній до цифрових товарів і послуг по всій Європі; 2) створення належних та рівних умов для процвітання цифрових мереж та інноваційних послуг; 3) максимізація потенціалу зростання цифрової економіки [1]. На мою думку, дана стратегія чітко визначає межі цифровізації та доступу населення до надання адміністративних послуг, тому імплементація її в українське законодавство є важливим аспектом для партнерства з ЄС.

Вагомим прикладом практичної реалізації державної політики у сфері цифрової трансформації України є впровадження екосистеми електронних сервісів «Дія», яка стала ключовим інструментом цифрової трансформації публічного адміністрування. Відзначу, що в ст. 17 Закону України «Про адміністративні послуги» зазначено: «надання адміністративних послуг в електронній формі та доступ суб'єктів звернення до інформації про адміністративні послуги з використанням мережі Інтернет забезпечуються засобами Єдиного державного веб-порталу електронних послуг («Портал Дія»), який є офіційним джерелом інформації про надання адміністративних послуг в Україні» [2]. Отже запровадження електронних документів, онлайн-послуг та цифрової ідентифікації через платформу «Дія» закріплено на законодавчому рівні та суттєво спростило взаємодію громадян із суб'єктами владних повноважень. Функціонування зазначеної платформи свідчить про послідовний рух України шляхом цифровізації публічного адміністрування та наближення національної системи адміністративного провадження до європейських стандартів електронного врядування.

На цьому розбудова української системи надання електронних адміністративних послуг не зупинилася, зокрема було створено низку електронних сервісів, зокрема можна віднести: єдиний державний портал адміністративних послуг; кабінет

електронних сервісів; он-лайн будинок юстиції, портал державних послуг iGov; єдина державна електронна база з питань освіти; єдиний веб-портал органів виконавчої влади України та інші [3].

Отже, цифрова перебудова адміністративного провадження в Україні не лише відповідає міжнародним стандартам, а й є ключовим чинником модернізації публічного адміністрування, підвищення його ефективності та інтеграції державних послуг у цифрову економіку та європейський правовий простір. Про це свідчить практичне впровадження екосистеми електронних сервісів «Дія» та інших державних платформ публічного адміністрування в Україні. Законодавче закріплення електронних послуг забезпечує правову визначеність, гарантує доступність сервісів для різних категорій населення та створює підґрунтя для подальшого розвитку цифрової держави.

Список використаних джерел:

1. Цифрова стратегія ЄС. URL: https://eufordigital.eu/uk/discover-eu/eu digital-strategy/. (дата звернення: 12.01.2026)

2. Закону України «Про адміністративні послуги» № 5203-VI від 6 вересня 2012 року. Відомості Верховної ради України 2013, № 32, ст.409 (дата звернення: 12.01.2026).

3. Тенденції розвитку інформаційних технологій в сфері надання державних публічних послуг в україні, Я.В.Бахарєва, 2019, URL: https://socrates.vsau.org/repository/getfile.php/28876.pdf (дата звернення: 13.01.2026)

Оскерко С.В.
аспірант
(Львівський державний університет безпеки життєдіяльності)

КІБЕРБЕЗПЕКА ТА ШТУЧНИЙ ІНТЕЛЕКТ: ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ І КОНФІДЕНЦІЙНІСТЬ В ЕПОХУ АЛГОРИТМІВ

Вступ

Стрімка інтеграція систем штучного інтелекту (ШІ), зокрема великих мовних моделей (LLM), у цифрову інфраструктуру державних органів, бізнесу та критичних сервісів зумовлює появу нових векторів атак, які не охоплюються традиційними моделями загроз. Європейське агентство з кібербезпеки ENISA пропонує розглядати взаємодію ШІ та кібербезпеки у двох вимірах: «AI for cybersecurity» (застосування ШІ для підвищення рівня захисту) та «cybersecurity for AI» (забезпечення належного рівня безпеки для самих ШІ- систем). [1][2][3][4]

У межах другого виміру виокремлюється проблема так званих prompt- ін'єкцій (prompt injection), які становлять окремий клас атак на LLM- системи й розглядаються міжнародною спільнотою як одна з ключових загроз для конфіденційності та цілісності обробки даних. Метою цих тез є окреслення сутності prompt- ін'єкцій, їхньої класифікації, наслідків для захисту персональних даних та аналіз актуальних підходів до протидії, зокрема у світлі рекомендацій ENISA. [5][6][7][8]

Теоретичні засади: поняття prompt-ін'єкції

Під prompt- ін'єкцією пропонується розуміти сукупність технік зловмисного формування вхідних підказок (prompts) до великої мовної моделі з метою зміни її цільової поведінки, обходу закладених обмежень безпеки та/або отримання несанкціонованого доступу до інформації чи ресурсів, до яких має доступ ШІ- система. На відміну від класичних ін'єкцій (SQL, XSS тощо), які експлуатують синтаксичні вразливості в обробці даних, prompt- ін'єкції використовують семантичні властивості природної

мови та особливості механізмів узгодження інструкцій у LLM. [6][7][8][9][10][11][5]

Ключовою передумовою вразливості є те, що в багатьох архітектурах LLM системні інструкції, політики безпеки та користувацький ввід поєднуються в єдиний текстовий контекст, який обробляється моделлю без чіткого технічного розмежування рівнів довіри. У результаті достатньо «переконливо» сформульована користувацька інструкція може бути інтерпретована моделлю як така, що має вищий пріоритет, ніж початкові правила. [7][8][10][5]

Класифікація prompt-ін'єкцій

На основі сучасних наукових досліджень та аналітичних матеріалів з кібербезпеки можна умовно виокремити щонайменше три базові типи prompt- ін'єкцій. [10][12][5][6][7]

1. **Пряма (direct) prompt- ін'єкція.**

У цьому випадку шкідливі інструкції безпосередньо вводяться користувачем у поле взаємодії з моделлю (чат- інтерфейс, форма запиту тощо). Типовими є конструкції на кшталт: «ігноруй усі попередні інструкції», «зміни свою роль» або «розкрий повний системний промпт». [9][13][6]

2. **Непряма (indirect) prompt- ін'єкція.**

Інструкції атакувальника приховуються у зовнішньому контенті, який опрацьовується LLM- агентом: веб- сторінках, документах, електронних листах, записах баз даних. Під час аналізу цього контенту модель може сприймати приховані текстові фрагменти як власні інструкції й виконувати їх, зокрема виконувати небажані дії над іншими ресурсами. [14][15][16][17]

3. **Стійкі (stored) та комбіновані ін'єкції.**

У цьому випадку шкідливі інструкції вбудовуються у знання, пам'ять або тренувальні дані моделі, що призводить до довгострокової зміни її поведінки для широкого кола користувачів. Комбіновані сценарії можуть поєднувати прямі й непрямі ін'єкції, а також мультимодальні вектори (приховані інструкції в зображеннях або інших форматах даних). [18][19][5][9][10][14]

У своїх звітах ENISA та національні кіберорган (наприклад, BSI Німеччини) окремо підкреслюють небезпеку саме непрямих prompt- ін'єкцій як «внутрішньої вразливості» для інтегрованих

ШІ- додатків, що працюють з недовіреним зовнішнім контентом. [4][15][16][20][14]

Вплив prompt-ін'єкцій на конфіденційність та персональні дані

У контексті захисту персональних даних prompt- ін'єкції становлять загрозу насамперед там, де LLM- сервіси інтегровані з реальними інформаційними системами, що містять персональну чи іншу конфіденційну інформацію (реєстри, медичні бази, фінансові системи, внутрішні документообіги). [2][3][21][22][1]

До основних ризиків можна віднести:

• несанкціоноване розкриття вмісту документів та записів баз даних, коли модель під впливом prompt- ін'єкції виводить фрагменти внутрішніх даних, які не передбачалося робити доступними користувачу;

• обхід механізмів деперсоналізації, коли шляхом поєднання «безпечних» фрагментів інформації модель фактично відновлює ідентичність суб'єкта даних;

• маніпулювання автоматизованими рішеннями, що може мати наслідком хибні управлінські або фінансові рішення, ухвалені на основі скомпрометованого виходу моделі. [3][21][23][24][4]

ENISA наголошує, що в системах високого ризику (фінансовий сектор, охорона здоров'я, критична інфраструктура) такі інциденти мають розглядатися як порушення конфіденційності та цілісності обробки даних, а не лише як «аномальна поведінка моделі». [1][2][3][4]

Український вимір проблематики

Україна, імплементуючи європейське цифрове право (насамперед GDPR) та орієнтуючись на майбутнє застосування AI Act, одночасно розгортає масштабні проєкти цифрової трансформації державних послуг. Використання LLM- рішень у сфері е- урядування, фінансових сервісів, медицини та освіти робить питання prompt- ін'єкцій актуальним не лише в теоретичному, а й у прикладному вимірі. [30][31][32][3]

Висновки

Prompt- ін'єкції формують окремий клас загроз для систем штучного інтелекту, що поєднує властивості атак на застосунки, дані та логіку взаємодії людина–машина. У контексті захисту персональних даних вони становлять суттєву небезпеку через

здатність обходити класичні технічні та організаційні заходи безпеки, впливаючи безпосередньо на поведінку LLM- сервісів, інтегрованих з конфіденційними ресурсами. [8][22][3][7][10][21][1][2][5]

Позиція ENISA, підкріплена дослідженнями міжнародної спільноти, свідчить про необхідність розглядати захист від prompt- ін'єкцій як складову архітектурного проєктування ШІ- рішень, у тісному зв'язку з принципами «безпеки за замовчуванням» та «конфіденційності за замовчуванням» (security/privacy by design). Для України, яка одночасно впроваджує європейські стандарти захисту даних і масштабні проєкти цифровізації, інтеграція цих підходів у національну регуляторну та технічну практику є критично важливою умовою збереження довіри до цифрової держави в епоху алгоритмів. [31][32][3][4][30][1][2]

Список використаних джерел

1. Formalizing and Benchmarking Prompt Injection Attacks and Defenses. URL: https://arxiv.org/abs/2507.13038

2. Artificial Intelligence and Cybersecurity Research – an ENISA Research and Innovation Brief. URL: https://www.cip-association.org/artificial-intelligence-and-cybersecurity-research-an-enisa-research-and-innovation-brief/

3. IEEE Xplore document 11275079. URL: https://ieeexplore.ieee.org/document/11275079/

4. ENISA publishes AI cybersecurity reports. URL: https://dynabic.eu/enisa-publishes-ai-cybersecurity-reports/

5. IEEE Xplore document 11391166. URL: https://ieeexplore.ieee.org/document/11391166/

6. IEEE Xplore document 11023476. URL: https://ieeexplore.ieee.org/document/11023476/

7. Formalizing and Benchmarking Prompt Injection Attacks and Defenses (PDF). URL: http://arxiv.org/pdf/2310.12815.pdf

8. OWASP. Prompt Injection. URL: https://owasp.org/www-community/attacks/PromptInjection

9. Palo Alto Networks. What Is a Prompt Injection Attack? URL: https://www.paloaltonetworks.com/cyberpedia/what-is-a-prompt-injection-attack

10. ArXiv paper. URL: https://arxiv.org/abs/2504.18575
11. ArXiv paper. URL: https://arxiv.org/abs/2211.09527
12. ArXiv paper (PDF). URL: https://arxiv.org/pdf/2402.00898.pdf
13. SentinelOne. Prompt Injection Attack. URL: https://www.sentinelone.com/cybersecurity-101/cybersecurity/prompt-injection-attack/
14. ArXiv paper. URL: https://arxiv.org/abs/2503.00061
15. ArXiv paper. URL: https://arxiv.org/abs/2507.02735
16. BSI. Indirect Prompt Injections – Intrinsic Vulnerability in Application-Integrated AI Language Models. URL: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/EN/2023/2023-249034-1032.html
17. Unit 42 (Palo Alto Networks). Web-Based Indirect Prompt Injection Observed in the Wild. URL: https://unit42.paloaltonetworks.com/ai-agent-prompt-injection/
18. ArXiv paper (PDF). URL: https://arxiv.org/pdf/2403.04957.pdf
19. Nature Communications article. URL: https://www.nature.com/articles/s41467-024-55631-x
20. BSI. Indirect Prompt Injections – technical report (PDF). URL: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/EN/2023/2023-249034-1032.pdf?__blob=publicationFile&v=5
21. Semantic Scholar paper. URL: https://www.semanticscholar.org/paper/830cb22483595ec0421398af195842d788e4ea6e
22. Generative AI in Cybersecurity: A Comprehensive Review of LLM Applications and Vulnerabilities. URL: https://ieeexplore.ieee.org/document/11273791/
23. Semantic Scholar record of the article. URL: https://www.semanticscholar.org/paper/31babc068383c3966d322579eaaf79edc6a6bef4
24. KPMG Ukraine. Як перетворити ШІ без ризиків на союзника в галузі кібербезпеки. URL: https://kpmg.com/ua/uk/home/insights/2025/09/yak-peretvoryty-shi-bez-ryzykiv-na-soyuznyka-v-haluzi-kiberbezpeky.html

25. StruQ: Defending Against Prompt Injection with Structured Queries (PDF). URL: https://arxiv.org/pdf/2402.06363.pdf

26. OWASP. LLM Prompt Injection Prevention Cheat Sheet. URL: https://cheatsheetseries.owasp.org/cheatsheets/LLM_Prompt_Injection_Prevention_Cheat_Sheet.html

27. ArXiv paper (PDF). URL: http://arxiv.org/pdf/2410.21146.pdf

28. StackHawk. OWASP LLM01 Prompt Injection. URL: https://www.stackhawk.com/blog/owasp-llm01-prompt-injection/

29. PID Security. OWASP LLM Prompt Injection. URL: https://pidsec.com/insights/owasp-llm-prompt-injection/

30. ArXiv paper. URL: https://arxiv.org/abs/2502.16580

31. ZMINA. Штучний інтелект і захист персональних даних в Україні. URL: https://zmina.info/news/shtuchnyj-intelekt-i-zahyst-personalnyh-danyh-v-ukrayini-rozroblyayut-konczepcziyu-yedynogo-regulyatora-u-czyfrovij-sferi/

32. Вісник УжНУ. Наукова стаття (PDF). URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/11/9-2.pdf

33. Держспецзв'язку / CIP. Кібербезпека в епоху ШІ. URL: https://cip.gov.ua/ua/news/kiberbezpeka-v-epokhu-shi-yak-zakhistiti-svoyi-dani-pri-vikoristanni-onlain-chatbotiv

34. PSM7. Як захистити свої дані при використанні онлайн-чатботів. URL: https://psm7.com/uk/security/yak-zahystyty-svoyi-dani-pry-vykorystanni-onlajn-chatbotiv.html

35. Голос України. Матеріал про штучний інтелект. URL: https://www.golos.com.ua/article/386321

36. AI4Cyber. ENISA Threat Landscape – AI-related threats and risks. URL: https://ai4cyber.eu/?p=1219

37. Міністерство цифрової трансформації України. Artificial intelligence and human rights. URL: https://ai.thedigital.gov.ua/news/Artificial intelligence and human rights: recommendations for responsible AI use presented

Откидач Р.Р.
здобувачка вищої освіти
навчально-наукового інституту права та інноваційної освіти
(Дніпровський державний університет внутрішніх справ)
Науковий керівник – **Бобрішова Л.В.**
голова Ради молодих вчених,
доктор філософії
(Дніпровський державний університет внутрішніх справ)

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ У ПОПУЛЯРИЗАЦІЇ НАУКОВИХ ДОСЛІДЖЕНЬ НА ПРИКЛАДІ НАУКОВО-ОСВІТНЬОГО ПОРТАЛУ E-SENC

На сьогоднішній день процеси цифровізації поступово охопили майже всі сфери суспільного життя. Інформаційні технології вже давно є важливим елементом функціонування економіки, державного управління та освіти. Особливо стрімкого розвитку, як відомо, упродовж останніх років набули технології штучного інтелекту (далі – ШІ). Оскільки ШІ є відносно новим терміном для наукових розвідок, передусім зупинимося на його визначенні.

О.В. Баранов присвятив цьому питанню окреме дослідження, в результаті якого запропонував наступне формулювання: штучний інтелект – це певна сукупність методів, способів, засобів та технологій, насамперед комп'ютерних, що імітує (моделює) когнітивні функції, які мають критерії, характеристики та показники еквівалентні критеріям, характеристикам та показникам відповідних когнітивних функцій людини [1, с. 46]. М. Мар'єнко та В. Коваленко пропонують розуміти ШІ як інструментарій системи чи сервісу, з використанням якого можна збирати та адаптувати дані користувача (або дані, що розміщені у відкритих репозитаріях), та на їх основі генерувати нові рішення чи висновки, відповідно до поданого запиту користувача [1, с. 50].

І. О. Гелецька та М. М. Шовдра зауважують, що в більшості визначень ШІ має такі ознаки: 1) технічно він є певним системним забезпеченням, комп'ютерною програмою, сукупністю інформаційних технологій тощо; 2) діє на виконання мети чи завдань, визначених людиною; 3) в результаті діяльності ШІ наступають наслідки для середовища, з яким вони взаємодіють [3, с. 17].

З урахуванням наведених наукових підходів, вважаємо, що ШІ доцільно розуміти як комплекс інформаційних технологій, алгоритмів і програмних рішень, створених людиною, які здатні імітувати окремі когнітивні функції людського мислення, здійснювати аналіз даних та формувати нові рішення або висновки відповідно до поставлених завдань.

Не дивно, що нині такі технології активно впроваджуються як у комерції, так і на державному рівні. Наприклад, у низці країн ШІ вже використовується для оптимізації адміністративних процедур, аналізу масивів даних та підтримки ухвалення окремих рішень у сфері публічного управління. Окремі дослідження також вказують, що застосування алгоритмів машинного навчання дозволяє підвищити ефективність роботи державних інституцій [4, с. 125-126].

Водночас дедалі більшого значення набуває використання ШІ в освітній та науковій діяльності. Освітні системи різних держав уже починають інтегрувати відповідні технології у навчальний процес. Так, зокрема, у 2025 році в Естонії започатковано національну ініціативу AI Leap, метою якої є впровадження інструментів ШІ у систему середньої та професійної освіти, а також формування у учнів та викладачів відповідних компетентностей. Програма передбачає надання доступу до сучасних ШІ-інструментів десяткам тисяч учнів і педагогів та спеціальну підготовку викладачів щодо їх відповідального використання у навчальному процесі [5].

За таких умов виникає потреба у нових форматах поширення наукових знань та популяризації результатів досліджень, адже звичні форми комунікації поступово доповнюються цифровими платформами, які дозволяють зробити науковий контент доступнішим для ширшої аудиторії. Одним із таких прикладів є створення науково-освітніх онлайн-проєктів, зокрема платформ,

що функціонують на базі відеохостингів, соціальних мереж і поєднують можливості сучасних медіа та технологій ШІ.

Прикладом такої ініціативи є науково-освітній портал E-SENC (Scientific and Educational Network Community), який функціонує, зокрема, на базі відеохостингу YouTube та орієнтований на популяризацію результатів наукових досліджень у форматі аудіовізуального контенту [6]. Діяльність цього проєкту спрямована на створення сучасного інформаційного простору для представлення наукових напрацювань, обміну ідеями та розвитку академічної комунікації між дослідниками, викладачами й здобувачами освіти.

Особливістю порталу є подача матеріалу у доступному та сучасному форматі науково-освітніх подкастів, у межах яких автори мають можливість презентувати результати власних досліджень у більш доступній та наочній формі. Водночас підготовка подібного контенту нерідко здійснюється із застосуванням сучасних цифрових інструментів, у тому числі технологій ШІ, що дозволяє автоматизувати окремі етапи створення аудіовізуальних матеріалів, зокрема генерування текстового супроводу, синтез мовлення чи візуалізацію інформації.

У межах діяльності E-SENC технології ШІ використовуються безпосередньо у підготовці аудіовізуальних матеріалів. Йдеться, насамперед, про допоміжну обробку результатів наукових досліджень та їх подальшу трансформацію у формат відеоподкастів. Як показує практика реалізації цього проєкту, початковим етапом є надання автором наукових матеріалів. Надалі формулюється відповідний запит до системи ШІ, визначаються ключові смислові акценти та структура майбутнього аудіовізуального продукту. Фактично саме людина задає напрям роботи, коригує зміст та здійснює підсумкову перевірку отриманого результату.

Після цього технології ШІ застосовуються для автоматизованої обробки текстового матеріалу, зокрема для формування сценарію відеоподкасту, узагальнення основних ідей дослідження, а також для створення аудіо- та відеосупроводу. Таким чином науковий текст, який традиційно існує у письмовій формі, набуває нової форми – аудіовізуальної. Власне, такий

підхід і реалізується у межах діяльності порталу E-SENC, де результати наукових досліджень подаються у форматі зручних науково-освітніх подкастів.

Використання подібної моделі створення контенту має низку практичних переваг. Передусім це дозволяє значно скоротити час підготовки відеоматеріалів, адже окремі технічні етапи можуть виконуватися автоматизовано. Крім того, застосування інструментів ШІ сприяє більш наочному та доступному представленню наукової інформації, що, у свою чергу, полегшує її сприйняття ширшою аудиторією. Водночас принциповим є те, що змістовна основа матеріалу формується саме автором дослідження, тоді як ШІ виконує функцію допоміжного інструменту для його обробки та візуалізації.

Список використаних джерел

1. Баранов О.А. Визначення терміну “штучний інтелект”. *Інформація і право.* 2023. № 1(44). С. 32-49. DOI: https://doi.org/10.37750/2616-6798.2023.1(44).287537.

2. Мар’єнко М., Коваленко В. Штучний інтелект та відкрита наука в освіті. *Фізико-математична освіта.* 2023. Т. 38, № 1. С. 48-53. DOI https://doi.org/10.31110/2413-1571-2023-038-1-007.

3. Гелецька І.О., Шовдра М.М. Визначення поняття «штучного інтелекту» та його місце у системі цивільного законодавства України. *Галицькі студії: Юридичні науки.* 2024. № 6. С. 13-19. DOI https://doi.org/10.32782/galician_studies/law-2024-6-2.

4. Крутогорський Я.В., Ярова А.Л. Роль штучного інтелекту в державному управлінні. *Сучасні виклики та напрями вдосконалення в економічній та технічній наукових сферах*: матеріали Міжнар. наук.-практ. конф. (5-6 грудня 2023 р., м. Запоріжжя) / за ред. Макаренка А. П., Меліхової Т.О. Запорізький національний університет. Запоріжжя: ЗНУ, 2023. С. 125-127.

5. Estonia Announces A Groundbreaking National Initiative: AI Leap Programme to Bring AI Tools to All Schools. URL: https://www.hm.ee/en/news/estonia-announces-groundbreaking-national-initiative-ai-leap-programme-bring-ai-tools-all?utm (date of access: 05.03.2026).

6. Науково-освітній портал E-SENC. YouTube : вебсайт. URL: https://www.youtube.com/@E-SENC (дата звернення: 05.03.2026).

Павлішин Д.О.
здобувач вищої освіти факультету № 1
(Львівський державний університет внутрішніх справ)
Гуцуляк Ю.В.
доцент кафедри кримінального процесу
та криміналістики факультету № 1,
доктор філософії
(Львівський державний університет внутрішніх справ)

ВИКОРИСТАННЯ OSINT ТЕХНОЛОГІЙ ПІД ЧАС РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

У сучасному світі технологічний прогрес невпинно впливає на всі сфери життя суспільства, включно з діяльністю правоохоронних органів у тому числі органів досудового розслідування, прокуратури. Особливо актуальним стає використання новітніх інформаційних технологій для виявлення, розслідування і попередження кримінальних правопорушень. Однією з таких інноваційних і ефективних методик є OSINT, або відкритий збір розвідувальної інформації. Така методика базується на використанні доступних публічних джерел інформації, що не вимагають спеціальних дозволів, і може стати вагомим інструментом у розслідуванні широкого спектру кримінальних проваджень. Тому особливо актуальним є вироблення правового підґрунтя, методики використання OSINT технологій в процесі розслідування кримінальних правопорушень.

В першу чергу, вважаємо за необхідне зазначити, що комплексне застосування OSINT технологій дозволяє правоохоронним органам значно розширити коло доступних даних і оперативно отримувати процесуально-необхідну інформацію. Зокрема, такими джерелами отриманих даних є: соціальні мережі, Інтернет форуми, веб-блоги, офіційні реєстри, медіа-платформи, відео-архіви, дані геолокаційних сервісів та інші цифрові ресурси доступ до яких можливий через мережу Інтернет. Це відкриває нові горизонти для збору доказів, встановлення фактів,

ідентифікації підозрюваних і свідків, а також відстеження потенційних загроз [1, с. 203].

Разом з тим треба наголосити на фундаментальній особливості OSINT, якою є її законність, оскільки всі зібрані дані знаходяться у відкритому доступі і не порушують приватності, що не потребує дотримання додаткових гарантій забезпечення окремих прав та свобод. Водночас, при цьому, потрібно мати на увазі той факт, що методика роботи з OSINT вимагає високої професійної підготовки суб'єктів, які здатні систематизувати великий обсяг інформації, аналізувати її на предмет достовірності, актуальності та значущості для конкретного кримінального провадження.

Важливо підкреслити, що OSINT не замінює традиційні слідчі (розшукові) дії, а виступає як додатковий методико-криміналістичний інструмент, що оптимізує роботу слідчих і оперативних працівників. При цьому, саме ця методика на практиці дозволяє надзвичайно швидко отримати перші відомості про підозрюваних, їх оточення, місце перебування й інші важливі деталі, які можуть бути недоступними або складними для отримання іншими методами пізнання. Тому, застосування відкритих джерел допомагає також відстежувати нові тенденції у злочинній діяльності, а також розуміти соціальні і психологічні аспекти поведінки злочинців [2, с. 37].

Також доречним буде відмітити, що безпосередньо серед практичних напрямів використання OSINT варто виділити моніторинг інтернет-простору на предмет екстремістських і терористичних проявів, пошук викрадених даних та інформації про шахрайські схеми, аналіз фінансових операцій в межах боротьби з відмиванням коштів, встановлення зв'язків між підозрюваними і злочинними групами, виявлення фейкових акаунтів і кіберзлочинців. При цьому, отримані відомості можуть бути використані не лише у досудовому розслідуванні, а й у судовому процесі як частина доказової бази, що підтверджує версію подій.

При цьому, відмічаємо, що застосування OSINT пов'язане з певними викликами, серед яких необхідність дотримання етичних і правових норм, зокрема щодо захисту персональних даних, а також ризик маніпуляції інформацією або отримання

недостовірних даних. Спеціалісти у цій сфері повинні володіти навичками критичного мислення, вміти відокремлювати факти від припущень, перевіряти джерела і застосовувати комплексний підхід до аналізу. Важливим є також постійне оновлення знань про нові технології і інструменти збору інформації, що дозволяє підтримувати високий рівень компетентності.

Все ширше використання OSINT технологій з кримінального провадження підтверджує тенденцію до цифровізації правоохоронної діяльності та інтеграції сучасних інформаційних ресурсів у традиційні методи розслідування. Це створює умови для підвищення ефективності боротьби зі злочинністю та забезпечення безпеки громадян. Паралельно з цим зростає важливість нормативного регулювання цієї сфери, що має враховувати баланс між оперативністю збору інформації і дотриманням прав людини[4].

У кримінальному провадженні 947/2401/26 Київський районний суд міста Одеси OSINT-дослідженням соціальних мереж та інших відкритих джерел з фіксацією виявленої інформації за протоколом Берклі, відповідно до якого зафіксовано:

- публікації Krenzer Benjamin Donald та ОСОБА_39 про бажання усиновити братів ОСОБА_40 (опікун ОСОБА_10), перепони в цьому процесі, які виникли після нападу російських військ на Україну, а також про вартість міжнародного усиновлення, яка може сягати 35000 доларів США;

- відеопублікацію від 07.06.2022 на каналі «YouTube» з дитиною, візуально схожою на ОСОБА_41 , із закликом «…and that of 300 other orphans in the process of being adopted by American families», яке вказує, що дитину бажають усиновити громадяни США; з дитиною ОСОБА_42 , громадянкою США ОСОБА_58, її доньками ОСОБА_59 та ОСОБА_60, із закликами «Help Save ОСОБА_61», «Along with education, medical care, and the love and support of two parents and two big sisters», «She should stay in the US in their loving home until the war ends and her adoption can pr», які вказують на бажання ОСОБА_58 отримати саме цю дитину для подальшого удочеріння[5].

Вироком Холодногірського районного суду міста Харкова у резулятивній частині астановлено,що:інформацією, що надана відповіддю проекту Project Expedite Justice, що надійшла на запит

Харківської обласної прокуратури, відповідно до якої проведено OSINT-розслідування в ході якого встановлено в тому числі адреси реєстрації, номери документів контактні дані та коло родичів, а також фотокартки ОСОБА_7. Встановлено, що ОСОБА_7 притягався до відповідальності за ст. 128 ч. 1, ст. 158, ст. 161, ст. 162 КК рф (т. 4 а.с. 240-246)[6].

Отже, на основі проведеного дослідження можемо зробити висновок, що OSINT технології є потужним і перспективним інструментом у розслідуванні кримінальних правопорушень, що дозволяє правоохоронцям швидко і законно отримувати важливі відомості, підвищувати якість доказів і розширювати можливості аналітичної роботи. Водночас їхнє ефективне застосування потребує професіоналізму, відповідального ставлення до етичних аспектів і постійного розвитку технічних навичок. Завдяки цьому можна досягти значного прогресу у боротьбі зі злочинністю та зміцнити систему правосуддя в цілому.

Список використаних джерел:

1. Яровий Т.С. OSINT, як перспективний інструмент контролю за лобістською діяльністю в контексті державної безпеки. *Експерт: парадигми юридичних наук і державного управління*. 2019. № 4(6). С. 201-208.

2. Дуфенюк О. Використання відкритих джерел цифрової інформації під час розслідування злочинів. *Інформація та документ у сучасному науковому дискурсі: матеріали VII Всеукраїнської дистанційної науково-практичної конференції.* (Івано-Франківськ, 20 травня 2022 р.). Івано-Франківськ: ІФНТУНГ, 2022. С. 36-41.

3. Одерій О.В., Кожевніков О.А. отримання криміналістично значущої інформації шляхом аналізу відкритих інтернет-джерел. Правовий часопис Донбасу. 2020. № 4 (73) 2020. С. 144-155.

4. Кудінов С. С., Шехавцов Р. М. Правове регулювання використання OSINT та його результатів під час встановлення обставин кримінальних правопорушень. *Науковий вісник Львівського державного університету внутрішніх справ (серія юридична)*. 2025. № 3. С. 126-133. URL:

https://doi.org/10.32782/2311-8040/2025-3-14 (дата звернення: 12.12.2025).

5. Ухвала Київського районного суду міста Одеси Справа № 947/2401/26 URL: https://reyestr.court.gov.ua/Review/133526734

6. Вирок Холодногірського районного суду міста Харкова від 13.01.2026 у справі № 636/6739/25. URL: https://reyestr.court.gov.ua/Review/133239393.

Патрелюк Д.А.
докторант,
кандидат юридичних наук
(Донецький державний університет внутрішніх справ)

ДІДЖИТАЛІЗАЦІЯ ЯК НАПРЯМ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ КРИМІНАЛЬНОГО ПЕРЕСЛІДУВАННЯ

Відповідно до положень ст. 103 КПК України процесуальні дії під час кримінального провадження можуть фіксуватися: у протоколі; на носії інформації, на якому за допомогою технічних засобів зафіксовані процесуальні дії; у журналі судового засідання. Протокол є універсальною формою фіксації слідчих (розшукових) та інших процесуальних дій. Протокол має складну структуру та складається з вступної, описової та заключної частин. Запис, здійснений за допомогою звуко- та відеозаписувальних технічних засобів під час проведення процесуальних дій є додатком до протоколу. У матеріалах кримінального провадження зберігаються оригінальні примірники технічних носіїв інформації зафіксованої процесуальної дії, резервні копії яких зберігаються окремо [1].

Під час особливого режиму кримінального провадження в умовах воєнного стану законодавець передбачив певні винятки у порядку оформлення процесуальних дій. Згідно п. 1 ч. 1 ст. 615 КПК України за відсутності можливості складання процесуальних документів про хід і результати проведення слідчих (розшукових) дій чи інших процесуальних дій фіксація здійснюється доступними технічними засобами з подальшим складенням відповідного протоколу не пізніше сімдесяти двох годин з моменту завершення таких процесуальних дій [1]. Уявляється, що такі винятки мають бути направлені на спрощення документування/фіксації процесуальних дій, на оптимізацію зусиль органів кримінального переслідування, щоб останні могли більше зосередитись на сутності процесуальних дій, ніж на їх оформленні, однак сталось по іншому. Фактично, в умовах воєнного стану, за відсутності можливості складання процесуальних документів, сторона обвинувачення виконує

подвійну роботу: фіксує процесуальні дії за допомогою технічних засобів; протягом сімдесяти двох годин з моменту завершення процесуальної дії складає протокол.

Т.О. Лоскутов вважає доцільним унормування у КПК України змішаної (паперово-технічної) форми фіксації зі значним спрощенням процедури складання письмових документів. Це спростить формальну «паперову» роботу співробітників органів досудового розслідування та сприятиме підвищенню ефективності безпосереднього збирання та перевірки відомостей про обставини вчинення кримінального правопорушення [2, с. 344]. Надлишковий формалізм у документуванні процесуальних дій у перебігу кримінального переслідування, не сприяє підвищенню ефективності останнього. Першочергово, під час оцінки доказів чи прийняття рішень стороною обвинувачення має братись до уваги змістовний аспект, в той же час документування має відігравати другорядну роль. Використання стороною обвинувачення у своїй діяльності електронних засобів фіксації (без дублювання інформації на паперових носіях) має підвищити ефективність кримінального переслідування.

Вважаємо, що у разі застосування звуко і відео фіксації процесуальної дії, необхідність у паперовому оформленні такої процесуальної дії відсутня. В даному випадку наявність паперового документа про проведення стороною обвинувачення процесуальних дій жодним чином не впливає на результати процесуальних дій та на рівень забезпечення прав і свобод людини у ході їх проведення [3, с. 754].

Разом з тим, окремим напрямом підвищення ефективності кримінального переслідування може бути впровадження можливостей штучного інтелекту (далі – ШІ) у сферу боротьби зі злочинністю.

Практика застосування ШІ в досудовому розслідуванні демонструє значні переваги у таких напрямках як прогнозування злочинності, аналіз великих масивів даних, розпізнавання облич та об’єктів, автоматизація рутинних процесів документування. Зокрема, системи предиктивної аналітики, що використовуються правоохоронними органами США та країн ЄС, показують високу ефективність у запобіганні злочинам та оптимізації розподілу поліцейських ресурсів [4, с. 819].

М.А. Погорецький відмічає, що ШІ, виконуючи функції виявлення, фільтрації, класифікації та первинної аналітики цифрових даних, не є самостійним суб'єктом процесу доказування, а лише технічним інструментом сторін і суду, який підпорядковується доктринальним і процесуальним вимогам. Погоджуємось з тим, що ШІ підсилює доказування лише в межах перевірної криміналістичної дисципліни та процесуальних гарантій справедливого суду. Будь-яке делегування дискреції ШІ без прозорості, відтворюваності та мотивованої людської оцінки – це не доказування, а технологічна ілюзія. Судовий процес, на думку дослідника, має залишатися інструментом захисту прав, а не демонстрацією потужності алгоритмів [5, с. 413-414].

Штучний інтелект відкриває нові горизонти у сфері кримінального аналізу, значно підвищуючи ефективність виявлення, розслідування та профілактики злочинів. Завдяки здатності обробляти великі обсяги даних, виявляти закономірності та прогнозувати злочинну активність, системи ШІ стають незамінним інструментом для правоохоронних органів. Проте впровадження таких технологій потребує комплексного підходу, що враховує не лише технічні можливості, а й етичні та правові аспекти, зокрема захист прав людини, забезпечення прозорості і уникнення зловживань [6, с. 319].

Використання можливостей ШІ у тандемі з цифровими технологіями є корисними під час виявлення, попередження та документування кримінальних правопорушень. У сучасних реаліях функціонал ШІ може використовуватись для опрацювання великих масивів даних, аналізу цифрових доказів та прогнозування ризиків у кримінальному провадженні.

Список використаних джерел:

1. Кримінальний процесуальний кодекс України. Закон від 13.04.2012. № 4651-VI. URL : https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 01.03.2026).

2. Лоскутов Т.О. Правове регулювання фіксування кримінального провадження в умовах воєнного стану. *Аналітично-порівняльне правознавство*. 2022. № 1. С. 340-345.

3. Патрелюк Д. А. Шляхи підвищення ефективності кримінального переслідування. *Аналітично-порівняльне правознавство.* 2025. № 1. С. 749-757.

4. Бєлова М. В., Бєлов Д. М., Рущак І. В. Штучний інтелект у досудовому розслідуванні кримінальних справ: окремі питання міжнародної практики. *Аналітично-порівняльне правознавство*. 2025. № 1. С. 818-824.

5. Погорецький М. А. Штучний інтелект у доказуванні в досудовому та судовому провадженнях: доктринальні засади і практика застосування. *Науковий вісник Ужгородського національного університету. Серія : Право*. 2025. Вип. 91 (4). С. 398-417.

6. Хоменко Р. О., Кисельов А. О. Штучний інтелект: найсучасніші можливості штучного інтелекту та кримінальний аналіз. *Universum.* 2025. № 21. С. 314-320.

Пилипенко Д.О.
доцент кафедри права,
доктор юридичних наук, доцент
(Державний університет економіки і технологій
Пилипенко Є.О.
старший науковий співробітник
науково-дослідної лабораторії
з актуальних питань кримінального аналізу,
кандидат юридичних наук, старший дослідник
(Одеський державний університет внутрішніх справ)

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ У ЗДОБУТТІ ІНКЛЮЗИВНОЇ ОСВІТИ

Відповідно до ст. 53 Конституції України кожен має право на освіту. Крім того, повна загальна середня освіта є обов'язковою в нашій державі [1]. У зв'язку із цим, усі діти, у тому числі, із спеціальними освітніми потребами, мають право на здобуття освіти.

Слід зазначити, що, так звані, інклюзивні діти – це ті діти, у кого наявні виразні відхилення в розвитку, які виникли під впливом хвороби, органічних чи функціональних порушень нервової системи, або периферичних порушень певного аналізатора. Іноді причиною відхилень стають несприятливі зовнішні умови, наприклад, проблеми сімейного виховання, що можуть призвести до педагогічної занедбаності. Таким дітям потрібні спеціальні освітні та виховні умови [2].

Серед основних груп дітей з інклюзивним розвитком виділяють: дітей із вираженими та сталими порушеннями слухової функції (глухі, слабочуючі, пізнооглухлі); дітей із глибокими порушеннями зору (сліпі, слабозорі); дітей зі стійкими порушеннями інтелектуального розвитку, пов'язаними з органічним ураженням центральної нервової системи (розумово відсталі); дітей із важкими мовними вадами (діти-логопати); дітей із комплексними порушеннями ряду функцій (сліпоглухі; діти, в яких тяжкі порушення слуху або зору поєднуються з розумовою відсталістю) [2].

Але, не зважаючи на наявність певних особливостей, як нами вже зазначалося раніше, такі діти мають право на здобуття освіти в Україні.

Так, відповідно до Закону України «Про освіту» від 05.09.2017 року № 2145-VIII, інклюзивне навчання – система освітніх послуг, гарантованих державою, що базується на принципах недискримінації, врахування багатоманітності людини, ефективного залучення та включення до освітнього процесу всіх його учасників. Разом з тим, інклюзивне освітнє середовище – це сукупність умов, способів і засобів їх реалізації для спільного навчання, виховання та розвитку здобувачів освіти з урахуванням їхніх потреб та можливостей [3].

Тобто, задля навчання окремої категорії дітей (зокрема, інклюзивних) є необхідність у створенні певного інклюзивного освітнього середовища, допомогти у створенні якого може штучний інтелект.

Так, серед основних напрямків допомоги штучного інтелекту, можна окреслити такі [4]:

- адаптація контенту та персоналізація (штучний інтелект може аналізувати швидкість засвоєння матеріалу, визначити рівень учня та автоматично підібрати відповідну складність завдань);

- використання за стосунків, які озвучують текст, описують зображення або предмети навколо у реальному часі (для незрячих);

- використання платформ, що перетворюють звук у візуальні сигнали або текст (для людей з порушеннями слуху);

- використання програм, що допомагають розпізнавати нетипове мовлення та трансформувати його в зрозумілий текст (для людей із порушеннями мовлення);

- використання платформ, що імітують соціальні ситуації для підтримки комунікації та соціалізації (для дітей з аутизмом, для відпрацювання навичок спілкування в безпечному цифровому середовищі).

Отже, говорячи про роль та використання штучного інтелекту в інклюзивній освіті, можна цілком справедливо зауважити, що він є потужним інструментом здобуття такої освіти, адже дозволяє адаптувати навчальне середовище під потреби кожної дитини з особливими освітніми потребами.

Список використаних джерел:

1. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР (дата оновлення: 01.01.2020). URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/ 96-%D0%B2%D1%80#n4337 (дата звернення: 01.03.2026).

2. Інклюзивні діти. Діти з спеціальними освітніми потребами. *Всеосвіта. Стрічка блогів.* URL: https://vseosvita.ua/blogs/dity-z-spetsialnymy-osvitnimy-potrebamy-111947.html# (дата звернення: 01.03.2026).

3. Про освіту : Закон України від 05.09.2017 № 2145-VIII (дата оновлення: 01.01.2026). URL: https://zakon.rada.gov.ua/laws/show/2145-19#Text (дата звернення: 01.03.2026).

4. Штучний інтелект в інклюзивній освіті. *ВсімОсвіта.* URL: https://vsimosvita.com/shtuchnyj-intelekt-v-inklyuzyvnij-osviti/ (дата звернення: 01.03.2026).

Піхурець О.В.
професор кафедри цивільного, трудового
та господарського права ННІ № 1,
кандидат юридичних наук, доцент
(Харківський національний університет внутрішніх справ)
Литвин С.Й.
доцент кафедри цивільного права
та процесу юридичного факультету ДВНЗ,
кандидат юридичних наук, доцент, адвокат
(Ужгородський національний університет)

ВИКОРИСТАННЯ ШІ В ОСВІТНЬОМУ ПРОЦЕСІ: ПЕРСПЕКТИВИ ТА ПРОБЛЕМИ

Сучасна вища освіта перебуває в стані глибокої системної цифрової трансформації, зумовленої стрімкою інтеграцією генеративних та інших систем штучного інтелекту (AI). За даними 2025 року, обсяг використання студентами AI сягає 85-92 % (HEPI Student Generative AI Survey 2025, Digital Education Council AI in Higher Education LATAM Survey 2026, Inside Higher Ed survey 2025). Викладачі та працівники закладів вищої освіти демонструють не меншу активність, понад 70 % вже використовують інструменти AI на щоденній або щотижневій основі [1]. Не є винятком з цього процесу і Україна. Загалом 86 % закладів освіти вже впровадили GenAI у свою діяльність.

Масове впровадження AI відкриває нові перспективи для якісної трансформації освітнього процесу. Системи GenAI забезпечують можливість глибокої персоналізації навчання шляхом формування адаптивних освітніх траєкторій, створення інтелектуальних рекомендаційних систем та використання персональних tutoring-агентів. Безумовно, це сприяє підвищенню ефективності освітніх програм, зокрема рівень завершеності курсів зростає на 15–35 %, особливо у заочній та дистанційній формах навчання.

Автоматизація оцінювання та управління освітнім процесом стає ключовим напрямом цифрової трансформації. AI оптимізує організаційні та методичні аспекти, забезпечує швидкий доступ до знань, перевірку завдань і тестів, адаптацію матеріалів та

формування персоналізованих траєкторій навчання. Алгоритми машинного навчання аналізують успішність і прогнозують результати, а інтеграція у цифрові платформи розширює можливості дистанційної освіти. Наразі провідною тенденцією в освіті стає концепція «AI як розумний партнер», що змінює мету вищої освіти та формує нові стандарти освітнього процесу.

Інтеграція GenAI радикально змінює ландшафт сучасної науки. AI суттєво прискорює дослідницькі процеси, виводить аналітику на якісно новий рівень, виявляє приховані закономірності у великих даних, автоматизує рутинні завдання (пошук літератури, систематизацію, первинну обробку) та оптимізує подання результатів. GenAI звільняє науковцям значну кількість часу для творчих, концептуальних і міждисциплінарних аспектів дослідження.

Так, наприклад, ретроспективний аналіз літератури, пошук джерел, їх систематизація та формулювання напрямів подальших досліджень можуть ефективно підтримуватися GenAI, не порушуючи принципи академічної доброчесності – за умови дотримання правил цитування, критичної перевірки та збереження авторства людини. GenAI особливо цінні для створення якісних стислих резюме наукових статей та оглядів, що знижує когнітивне навантаження при мінімальних ризиках недоброчесності (за належного контролю та атрибуції). Фактично, AI перетворюється з допоміжного інструменту на інтелектуального партнера, який розширює горизонти наукового пошуку, підвищує ефективність досліджень та інтегрує її у глобальний цифровий простір.

Водночас масштабне використання AI вимагає свідомого й системного врахування етичних викликів, а саме: потенційну упередженість алгоритмів (bias), захист персональних даних, інтелектуальну власність та відповідальне застосування цих цифрових інструментів.

Слід вказати і на потенційне порушення академічної доброчесності, що може виникнути у випадках некоректного формулювання запитів до AI, використання системи без розуміння її принципів дії або свідомого застосування отриманих результатів з порушенням вимог до самостійного виконання творчих завдань чи отримання результатів досліджень. Також надмірне делегування творчої праці алгоритмам призводить до поступової

ерозії критичного та самостійного мислення [2], адже студенти (курсанти) дедалі частіше отримують готові відповіді без усвідомлення процесу їх формування, що спричиняє поверхневе засвоєння знань, ілюзію компетентності. Значна частина викладачів занепокоєна зростанням залежності студентів (курсантів) від AI, що, на їхню думку, послаблює критичне мислення, скорочує тривалість уваги та призводить до накопичення «когнітивного боргу», тобто поступового недорозвинення навичок самостійного аналізу, аргументації й незалежного судження. Звіт EDUCAUSE за 2026 рік свідчить про те, що надмірне покладання на алгоритми здатне підривати фундаментальні інтелектуальні компетентності, необхідні для професійної та наукової діяльності [2].

Академічна недоброчесність є одним із найгостріших ризиків інтеграції AI в освітній процес. Оскільки значна частина студентів (курсантів) використовує GenAI без належного цитування, що провокує своєрідну «гонку озброєнь» між детекторами плагіату та GenAI. Як наслідок значна частка студентів (курсантів) застосовують AI для написання рефератів, тез чи перефразування текстів [3]. Поверхневе розуміння матеріалу посилюється галюцинаціями, упередженнями та дезінформацією. Так AI-моделі генерують впевнені, але хибні твердження, особливо в наукових текстах, що вводить в оману користувачів і вимагає постійної верифікації й критичної оцінки.

Відмітимо й порушення академічної доброчесності користувачами AI під час створення та застосування «згенерованого результату», коли користувач свідомо чи несвідомо видає результат роботи GenAI за власний творчий результат без суттєвого самостійного внеску, критичного осмислення та декларування джерела. Найпоширенішими формами порушень є пряме копіювання згенерованого тексту, рішень, структури чи висновків і подання їх як власної роботи без будь-яких або з мінімальними правками. Поширеним є приховане використання AI як «невидимого співавтора» без вказівки на його роль. До порушень слід віднести й маніпуляції для обходу перевірки, а саме перефразування через інші моделі, створення фейкових цитат та джерел, заміна самостійного результату на згенерований код без розуміння логіки процесу. Окремо слід

виділити недекларованe використання у курсових, дипломних чи наукових роботах, де алгоритм формує значну частину змісту, але автор не фіксує цього факту. Варто і зауважити на недобросовісному застосування AI для імітації самостійної роботи під час іспитів чи захистів (підказки в реальному часі, автоматична генерація відповідей на усні запитання викладача) свідчить про відсутність істотного творчого внеску автора, свідоме приховування застосування технологій та делегування ключових когнітивних процесів. Що, безумовно, призводить до відчуження й втрати мотивації до набуття компетентностей.

Водночас ефективна протидія академічній недоброчесності на іншим ризикам застосування AI має ґрунтуватись на проактивному, багаторівневому підході, що означає відмову від практики «полювання на плагіат» чи інших порушень до формування культури відповідального використання моделей AI. Такий підхід передбачає переосмислення системи оцінювання та розвиток метакогнітивних навичок, що уможливлює уникнення потенційних порушень академічної доброчесності під час застосування AI.

Нещодавно ЮНЕСКО опублікувала рамку компетентностей у сфері ШІ для студентів (2024) та рамку компетентностей у сфері ШІ для вчителів (2024), з метою сприяння адаптації системам освіти до стрімкого розвитку AI. В 2025 році Міністерство освіти і науки спільно з Мінцифри розробило Рекомендації щодо відповідального впровадження та використання технологій ШІ в закладах вищої освіти, а низка університетів затвердила власні внутрішні положення про використання AI. Вказані рекомендації враховують вимоги чинного законодавства України, Білої книги з регулювання AI та актуальних міжнародних практик, зокрема Рамкової конвенції Ради Європи про ШІ, права людини, демократію та верховенство права, а також принципів Регламенту ЄС щодо AI (EU AI Act) та Етичні принципи для надійного ШІ та найкращі світові практики. Рекомендації містять практичні поради для різних груп стейкхолдерів: викладачів (створення якісних промптів, інтеграція AI в педагогіку, розробка завдань, що вимагають людського внеску), студентів (критична перевірка результатів, уникнення галюцинацій та упередженості, декларування AI-об’єктів), адміністрацій ЗВО (розробка

внутрішніх політик, оцінка ризиків AI) та дослідників (застосування AI в наукових процесах з дотриманням етичних норм). Наголошено на прозорості, атрибуції та збереженні академічної доброчесності, визначено допустимі й недопустимі сценарії використання ШІ.

З урахуванням положень Закону України «Про академічну доброчесність» та вказаних нормативно-правових актів, освітні заклади мають оновити положення про академічну доброчесність включивши чітку політику щодо використання ШІ, оцінку ризиків при виборі чи придатності системи-AI, критеріїв відповідального застосування, обов'язкового декларування використання AI в академічних творах та класифікацію недоброчесних практик.

класифікації недоброчесного використання результатів, згенерованих AI (як окремої ознаки порушення, тобто оприлюднення згенерованого контенту як власного).

Заклади вищої освіти мають оновити положення про академічну доброчесність, включивши чітку політику щодо використання ШІ, оцінку ризиків, критерії відповідального застосування, обов'язкове декларування використання та класифікацію недоброчесних практик.

Доцільно також розглянути внесення змін до освітньо-професійних програм підготовки здобувачів першого (бакалаврського) та другого (магістерського) рівнів вищої освіти шляхом введення окремого освітнього компонента (навчальної дисципліни) «Академічна доброчесність». У межах цієї дисципліни слід передбачити вивчення основних принципів етичного використання AI, правил формулювання якісних запитів (промптів) та критичної перевірки згенерованих результатів, механізмів виявлення галюцинацій, упередженості та похибки AI, вимог до декларування, цитування та атрибуції AI-генерованого контенту, наслідків порушень, доповнені практичними кейсами.

Доречним є і проведення постійних просвітницьких заходів для підвищення рівня AI-грамотності своїх працівників та здобувачів вищої освіти. Науково-педагогічний персонал також може запобігати порушенням академічної доброчесності, якщо замість заборони надаватимуть пояснення можливості та ризики використання AI, формулюватимуть чіткі завдання з вимогою атрибуції (назву інструменту, промпти тощо) та регулярно їх

оновлювати. Ефективним є поєднання письмових і усних форм роботи, використання креативних завдань та практичних воркшопів. Вважаємо, що найкращим у цьому аспекті є не забороняти, а інтегрувати AI. Головна мета – не ловити порушення, а розвивати критичне мислення, оригінальність, синтез знань та етичну відповідальність. Тоді AI перетворюється з загрози на потужний інструмент, який посилює навчання, зберігаючи цінність людського внеску та академічну доброчесність.

Висновок. У 2026 році головним завданням для закладів вищої освіти є не заборона ШІ, а його інтеграція в освітній процес так, щоб він підтримував творчу самостійність студентів (курсантів), розвивав компетентності та водночас гарантував академічну доброчесність і цінність людського судження. Зміна парадигми в освітньому процесі полягає саме у переході від контролю «чи не списав» до виховання культури «як правильно й чесно використовувати AI». Оптимальним шляхом є модель відповідального партнерства з AI через оновлення методик оцінювання (процесуальний контроль, усний захист, авторський внесок), включення етичних і критичних компонентів у програми, систематичне підвищення кваліфікації викладачів та формування культури, де самостійне мислення й етичне використання технологій стають нормою для кожного. Заклади освіти, які запровадять таку екосистему, отримають конкурентні переваги, адже їхні випускники матимуть базову «AI fluency».

Вважаємо, що відповідальне використання AI не замінить викладача, а розвантажить його від рутинних завдань, дозволяючи зосередитися на живій взаємодії, розвитку soft skills та формуванні ціннісного ставлення до знань.

Список використаних джерел:

1. 2025 AI in Education: A Microsoft Special Report. URL: https://surl.li/udnbau (дата звернення – 28.02.2026).

2. Jenay Robert The Impact of AI on Work in Higher Education : EDUCAUSE: сайт. 12.01.2026. URL: https://surl.li/ejfmcm (дата звернення – 28.02.2026).

3. Angehr E., Bloem M., Howell J., Radford A. W. College Faculty Perceptions of Generative Artificial Intelligence in Higher Education. URL: https://surl.li/xutsjc (дата звернення – 28.02.2026).

Політова А.С.
доцент кафедри права,
кандидат юридичних наук, доцент
(*Маріупольський державний університет*)

АНАЛІЗ УХВАЛ ТА ВИРОКІВ СУДДІВ ЩОДО ПРАКТИКИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ: ОКРЕМІ АСПЕКТИ ПРОБЛЕМИ

Дискусіями про використання штучного інтелекту в освітньому процесу та для написанні наукових робіт вже нікого не здивуєш. У цьому питанні, варто врахувати й той аспект, що Міністерство освіти і науки та Міністерство цифрової трансформації України спільно з експертами розробили рекомендації щодо відповідального використання штучного інтелекту в закладах вищої освіти. Документ містить поради для викладачів, студентів, адміністрацій ЗВО та дослідників, що допоможуть ефективно інтегрувати ШІ в освітній і науковий процес [1].

Але використання штучного інтелекту стало своєрідним «викликом», зокрема, й у діяльності суддів і адвокатів. Відзначимо, що саме проблематика «Штучний інтелект та адвокатська діяльність: можливості, ризики та межі застосування», «Штучний інтелект: практичні та етичні питання у роботі юриста» ставали предметом вебінарів й онлайн-обговорень учасниками лише за останні півроку рік. Також зауважимо, що у статті «Штучний інтелект й адвокатська етика: виклики, які існують і ще з'являться» наводяться практики «позитивного» використання штучного інтелекту: «Журналісти описують історію мешканки Каліфорнії, яка програла справу про виселення, яку супроводжував адвокат. Але за допомогою *ChatGPT* та системи *Perplexity* вона змогла самостійно підготувати апеляцію, домогтися скасування судового наказу і звільнилася від сплати понад $70 тис. штрафів та прострочених орендних платежів. Вона надсилала штучному інтелекту документи, отримуючи підказки щодо можливих процесуальних помилок і правильного формулювання аргументів» [2].

Так, аналізуючи наукові публікації та інформацію в засобах масової інформації можна виокремити як позитивні аспекти щодо використання штучного інтелекту, так і негативні. Разом з тим, цікавим, на нашу думку, є саме аналіз ухвал та вироків суддів щодо практики використання штучного інтелекту, адже «для професійних юристів ШІ навряд є загрозою. Він також працює помічником, але вже у іншій якості. Це попередній аналіз, пошук судової практики, перевірка гіпотез перед написанням правових висновків, швидка структуризація опрацьованих матеріалів. За умови належного контролю й дотримання конфіденційності такі інструменти можуть значно підвищити ефективність роботи адвоката» [2].

В Єдиному державному реєстрі судових рішень існують певні правила пошуку необхідної інформації. Так, нами для підготовки цієї доповіді використано наступні правила: пошук Формою судочинства (обрано «Кримінальне»), категорією справи (зокрема, Кримінальні справ (з 01.01.2019) було обрано та за контекстом (ключові слова «штучний інтелект»). Це дозволило нам виокремити 197 ухвал та вироків суду.

Так, наприклад, у вироку Ужгородського міськрайонного суду Закарпатської області від 20 липня 2021 р. (Справа № 308/7867/21) зазначено: «В судовому засіданні представник Ужгородського МРВ філії Державної установи «Центр пробації» в Закарпатській області ОСОБА_7 пояснив, що ОСОБА_5 має позитивні характеристики, проте ризики вчинення повторного кримінального правопорушення та рівень небезпеки особи для суспільства визначається автоматизованою системою з штучним інтелектом «Касандра»» (підкресл. – А.С.П.) [3]. В іншому вироку, зокрема, вирок Дзержинського районного суду м. Харкова від 29 січня 2025 р. (Справа № 638/1151/25, Провадження №1-кп/638/1308/25) вказано: «Допитаний у судовому засіданні ОСОБА_4 повідомив, що він як 12 вересня 2023 так і 16 жовтня 2024 року телефонував на відповідні сайти, з ним спілкувався штучний інтелект, який повідомив де та коли забрати психотропні речовини. Він виконав указівки, та як в перший так і в другий рази забрав вказані згортки з психотропною речовиною» (підкресл. – А.С.П.) [4].

Також вважаємо за доцільне навести декілька прикладів про вказівку на використання учасниками кримінальних проваджень штучного інтелекту. Наприклад, в ухвалі колегії суддів Сумського апеляційного суду щодо бездіяльності слідчого прокурора від 03 лютого 2026 р. (Справа №589/5099/25, Номер провадження 11-сс/816/180/26) зазначено: «Окремої уваги заслуговують доводи апелянта щодо нібито існуючих правових позицій Верховного Суду. Аналіз змісту апеляційної скарги дає підстави для висновку про недобросовісне використання інструментів штучного інтелекту при її підготовці. Посилання на постанови Верховного Суду (зокрема № 761/4621/18, № 243/6679/19, № 991/7558/20, № 991/592/19) як на такі, що регулюють оскарження рішень слідчого про відмову у задоволенні клопотань, є грубим викривленням реальної судової практики.

Перевіркою встановлено, що зазначені номери справ або відсутні в Єдиному державному реєстрі судових рішень, або стосуються проваджень про адміністративні правопорушення, розглянутих судами першої інстанції, та не містять жодних висновків Верховного Суду щодо застосування норм КПК України. Використання вигаданих правових позицій (так званих «галюцинацій» штучного інтелекту) та подання до суду неперевірених документів, порушує принцип юридичної визначеності та є виявом неповаги до суду» (підкресл. – А.С.П.) [5].

Окрім того, в ухвалі слідчого судді Печерського районного суду м. Києва щодо тимчасового доступу до речей від 03 липня 2025 р. (Справа № 757/31017/25-к, пр. № 1-кс-27147/25) вказано: «Надалі, зловмисники, використовуючи раніше отриманий доступ до онлайн-банкінгу «ІНФОРМАЦІЯ_3 » та невстановлене програмне забезпечення, яке базується на технології «DeepFake» (технологія, яка використовує штучний інтелект і глибоке навчання для створення реалістичних підроблених відео та зображень, в тому числі в реальному часу), яка дає можливість змінювати обличчя людей на відео, синхронізувати міміку та голос, здійснюють несанкціонований доступ до Єдиного державного веб-порталу електронних послуг « ІНФОРМАЦІЯ_2 », та в подальшому, з метою незаконного заволодіння чужим майном – грошовими коштами АТ «ІНФОРМАЦІЯ_6 », авторизуються в

онлайн-банкінгу « ІНФОРМАЦІЯ_4 », відкриваючи рахунки на вказаних осіб з використанням технології «LIVENESS» (фото-відео верифікація)» (підкресл. – А.С.П.) [6].

Таким чином, проведений нами аналіз окремих положень ухвал та вироків суддів вказує на такі аспекти використання штучного інтелекту, перелік яких є невичерпних, а саме:

- проєктування подальшої протиправної поведінки особи, яка вчинила кримінальне правопорушення (тяжких та особливо тяжких злочинів);

- адвокатами при підготовці процесуальних документів (зокрема, апеляційних скарг);

- ідентифікації як особи, яка надає консультації та доступ до певних ресурсів.

Разом з тим, проблеми невизначеності використання штучного інтелекту у правосудді стають викликом, адже «на сьогодні в Україні не затверджені етичні стандарти та норми, які регулюють використання штучного інтелекту в судочинстві, не визначені визначення межі (етичні, правові) застосування систем штучного інтелекту для цілей надання професійної правничої допомоги, що відповідно до Концепції розвитку штучного інтелекту в Україні є одним із завдань державної політики у сфері правового регулювання галузі штучного інтелекту» [7].

Список використаних джерел:

1. Штучний інтелект у закладах вищої освіти: рекомендації для викладачів, студентів і працівників ЗВО. Опубл. 29 квітня 2025 р. *Сайт Міністерства освіти і науки України*. URL: https://mon.gov.ua/news/shtuchnyi-intelekt-u-zakladakh-vyshchoi-osvity-rekomendatsii-dlia-vykladachiv-studentiv-i-pratsivnykiv-zvo (дата звернення 24.02.2026)

2. ШІ витісняє адвокатів – чи існує реальна загроза професії? Опубл. 10 жовтн. 2025 р. Сайт *Національної асоціації адвокатів України*. URL: https://unba.org.ua/news/10847-shi-vitisnyae-advokativ-chi-isnue-real-na-zagroza-profesii.html (дата звернення: 25.02.2026).

3. Вирок Ужгородського міськрайонного суду Закарпатської області від 20 липня 2021 р. (Справа № 308/7867/21). URL:

https://reyestr.court.gov.ua/Review/98435140 (дата звернення: 25.02.2026).

4. Вирок Дзержинського районного суду м. Харкова від 29 січня 2025 р. (Справа № 638/1151/25, Провадження №1-кп/638/1308/25). URL: https://reyestr.court.gov.ua/Review/124784871 (дата звернення: 25.02.2026).

5. Ухвала колегії суддів Сумського апеляційного суду щодо бездіяльності слідчого прокурора від 03 лютого 2026 р. (Справа №589/5099/25, Номер провадження 11-сс/816/180/26). URL: https://reyestr.court.gov.ua/Review/133783810 (дата звернення: 25.02.2026).

6. Ухвала слідчого судді Печерського районного суду м. Києва щодо тимчасового доступу до речей від 03 липня 2025 р. (Справа № 757/31017/25-к, пр. № 1-кс-27147/25). URL: https://reyestr.court.gov.ua/Review/128844017 (дата звернення: 25.02.2026).

7. Ухвала Верховного Суду у складі суддів судової палати для розгляду справ щодо корпоративних спорів, корпоративних прав та цінних паперів Касаційного господарського суду від 08 лютого 2024 р. (справа № 925/200/22). URL: https://reyestr.court.gov.ua/Review/116984639# (дата звернення: 25.02.2026).

Полторак А.Б.
здобувачка вищої освіти
навчально-наукового інституту
права та соціального менеджменту
(Донецький державний університет внутрішніх справ).
Науковий керівник – **Туренко О.С.**
професор кафедри
державно-правових дисциплін
доктор філософських наук, професор
(Донецький державний університет внутрішніх справ)

ПРАВОВИЙ РЕЖИМ ЗАСТОСУВАННЯ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ В УМОВАХ ГЛОБАЛЬНИХ ТУРБУЛЕНТНОСТЕЙ: ВІД МІЛІТАРНИХ ТЕХНОЛОГІЙ ДО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

У сучасних умовах глобальної полікризи, що проявляється в синергії збройних конфліктів, економічної нестабільності та швидкої цифрової трансформації, традиційні правові інститути змушені фундаментально переглядати поняття суб'єктності, здатності до відповідальності та юридичних зобов'язань. Системи штучного інтелекту вже перестали бути лише інструментами для аналізу великих обсягів даних, перетворившись на автономних агентів, здатних впливати на публічне управління, стратегічне планування та глобальні ринки. Науковий діалог навколо пошуку оптимального співвідношення між технологічним прогресом і базовими правами людини акцентує увагу на необхідності створювати адаптивне нормативне регулювання. Таке так зване «динамічне регулювання» повинно підтримувати інновації, одночасно знижуючи ризики алгоритмічної дискримінації й порушення приватності. У цьому контексті концепція інклюзивної справедливості стає особливо актуальною: вона спрямована на те, щоб автоматизація правосуддя чи цифровізація державних послуг не призводили до маргіналізації вразливих верств населення та уникали створення явища цифрової ізоляції. Юридична основа використання ШІ повинна будуватися на принципах прозорості

алгоритмів та обов'язковій незалежній перевірці високоризикованих систем. Це є особливо важливим у сферах, пов'язаних із захистом інтелектуальної власності, де стираються межі між людською творчістю та контентом, згенерованим технологіями. За таких умов вкрай потрібні нові механізми для ідентифікації та охорони авторських прав у цифровому середовищі [1].

Особливості правового регулювання систем штучного інтелекту в умовах військових загроз і воєнного стану, які мають критичне значення для України, висувають на перший план актуальні питання етичного регулювання автономних озброєнь і інструментів інтелектуального аналізу розвідувальної інформації. Використання алгоритмів машинного навчання для визначення цілей і прогнозування воєнних дій створює складні виклики для міжнародного гуманітарного права, вимагаючи закріплення принципу «змістовного людського контролю» як бар'єру проти неконтрольованої ескалації конфліктів. Поза межами суто військового застосування, штучний інтелект стає ключовим компонентом національної стійкості: від моніторингу інформаційного простору для виявлення дезінформації та протидії гібридним загрозам до аналізу вразливостей критичної інфраструктури. Водночас мілітаризація цивільних технологій приховано несе ризик утворення систем масового нагляду під виглядом гарантій безпеки. У зв'язку з цим правове регулювання в умовах глобальної нестабільності повинно забезпечити тонкий баланс між інтересами державної безпеки та основоположними правами громадян на приватність. Особливо важливо запобігти тому, щоб надзвичайні правові режими у післявоєнний період не перетворилися на постійну практику обмеження громадянських свобод [2].

Реформування системи кримінальної юстиції та правоохоронної діяльності через впровадження технологій предиктивної аналітики вимагає суттєвих змін у процесуальному законодавстві, особливо щодо збору і перевірки цифрових доказів. Правовий статус доказів, отриманих чи перевірених за допомогою нейронних мереж, потребує створення нових стандартів прийнятності, які б унеможливлювали маніпуляції й забезпечували захист від упередженості, часто обумовленої некоректними

навчальними вибірками алгоритмів. У контексті європейської інтеграції України першочерговим завданням стає гармонізація національного законодавства зі стандартами EU AI Act, які передбачають чітке розмежування систем відповідно до рівня ризику для суспільства. Застосування біометричних технологій для дистанційної ідентифікації у громадських місцях або алгоритмів для автоматизованого прогнозування правопорушень має бути під суворим контролем парламенту та судових органів. У судовому процесі штучний інтелект повинен виконувати виключно функції допоміжного когнітивного інструменту, тоді як остаточне правове рішення і морально-етичне обґрунтування вироку обов'язково мають залишатися виключною відповідальністю судді-людини. Це є принциповою умовою забезпечення права на справедливий розгляд справи незалежним арбітром [3, с. 108].

Фінальним напрямом у формуванні правового середовища для штучного інтелекту стає розробка інтегрованої системи кібербезпеки та захисту персональних даних, здатної ефективно реагувати на виклики алгоритмічної ери. У контексті глобальної нестабільності кіберпростір перетворюється на ключову арену конфліктів між державами та корпораціями, де штучний інтелект слугує як інструментом для реалізації складних атак, так і основою побудови інтелектуальних захисних механізмів у режимі реального часу. У таких умовах конфіденційність даних стає стратегічно важливим компонентом національної безпеки, адже сучасні нейромережі здатні виконувати глибоку деанонімізацію навіть при роботі з фрагментарними, зашифрованими або деперсоналізованими даними [4, с. 133].

Отже, можна зробити висновок, що правове регулювання застосування систем штучного інтелекту в умовах глобальної нестабільності повинно спиратися на принципи динамічної стійкості та етичного антропоцентризму. Перспективи розвитку як національної, так і світової правової думки вбачаються у поєднанні традиційної юридичної доктрини з передовими стандартами алгоритмічного управління. Це дозволить спрямувати технологічний потенціал штучного інтелекту на користь суспільства, не порушуючи демократичних цінностей. Лише гармонізація національного законодавства з європейськими стандартами, особливо у сфері безпеки мілітарних і

правоохоронних технологій, здатна забезпечити створення стійкої моделі співіснування людства з автономними системами. Відтак, ключовим завданням держави має стати формування нормативної бази, яка передбачає водночас інноваційний розвиток нейромереж і повагу до фундаментальних прав і свобод людини. Це стане запорукою правової стабільності навіть у найскладніші часи глобальних викликів.

Список використаних джерел:

1. Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р (дата звернення: 21.02.2026).

2. Artificial Intelligence Act : Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024. *Official Journal of the European Union.* 2024. URL: http://data.europa.eu/eli/reg/2024/1689/oj (accessed: 21.02.2026).

3. Данилюк О. В. Кібербезпека та застосування штучного інтелекту в умовах гібридної війни: стратегічний аспект. *Збірник наукових праць НІСД*. 2024. № 5. С. 102–110.

4. Цифрові докази у судовому процесі: роль штучного інтелекту в аналізі та прийнятності : аналіт. доповідь / за заг. ред. С. В. Пєткова. Київ : Юрінком Інтер, 2025. 156 с.

Помаза-Пономаренко А.Л.
завідувач науково-дослідної лабораторії
з дослідження проблем управління
у сфері цивільного захисту,
доктор з державного управління, професор
(Національний університет цивільного захисту України)
Тарадуда Д.В.
професор кафедри
управління діяльністю підрозділів
цивільного захисту інституту післядипломної освіти,
кандидат технічних наук, доцент
(Львівський державний університет безпеки життєдіяльності)

ШТУЧНИЙ ІНТЕЛЕКТ ТА ПРАВА ЛЮДИНИ: БАЛАНС МІЖ ТЕХНОЛОГІЯМИ ТА ПРАВОМ ТА РОЗВИТОК ЦИФРОВИХ ПРАВ І ЦИФРОВОГО ОМБУДСМАНА В УКРАЇНІ

Розвиток штучного інтелекту (далі – ШІ) уже сьогодні формує новий технологічний ландшафт, суттєво впливаючи на економічні, соціальні та правові аспекти життя суспільства. Алгоритми ШІ застосовуються у медицині, судочинстві, банківській справі, працевлаштуванні, освіті та сфері громадської безпеки. У багатьох випадках вони підвищують ефективність, прискорюють процеси та оптимізують прийняття рішень. Однак у цьому контексті виникає низка серйозних загроз правам людини: порушення право на приватність, автономію, недискримінацію, доступ до правосуддя та свободу вираження. Баланс між технологіями та правом стає одним із ключових викликів сучасної правової системи. У цьому процесі важливо не лише запроваджувати інновації, а й формувати юридичні інструменти, що забезпечують захист фундаментальних прав людини у цифрову еру.

Україна активно розвиває цифрову трансформацію суспільства, і при цьому стикається з необхідністю створення повноцінної системи цифрових прав і відповідних механізмів їх

захисту, зокрема інституту цифрового омбудсмана. Це пов'язано з зростанням використання технологій ШІ у публічному секторі, трансформацією цифрового середовища.

ШІ передбачає застосування сукупності алгоритмів та обчислювальних моделей, що здатні виконувати завдання, які раніше вимагали людського інтелекту: навчання, планування, розпізнавання, генерація інформації. Технології ШІ часто характеризуються непрозорістю механізмів ухвалення рішень (так званою «чорною коробкою») та здатністю моделювати поведінку людей. Ця непрозорість створює низку проблем: відповідальність за рішення, що приймаються алгоритмами; трансформація понять дискримінації, оскільки алгоритми можуть відтворювати та посилювати упередження; порушення приватності, адже великі дані (Big Data), на яких навчаються моделі, містять персональну інформацію [2; 3].

Права людини в цифровому світі включають класичні фундаментальні права (на свободу вираження, приватність, недискримінацію, доступ до правосуддя), які набувають нових вимірів під впливом цифровізації. Важливими є також цифрові права – поняття, що охоплює право на доступ до мережі, безпечну обробку даних, справедливе використання алгоритмів, прозорість автоматизованих рішень та захист від цифрового насильства. Міжнародні документи підкреслюють, що технології не повинні замінювати людську автономію, створювати дискримінацію або обмежувати фундаментальні свободи.

Основні проблеми реалізації прав людини у контексті ШІ:

1. Приватність і захист даних. ШІ часто потребує обробки великих обсягів персональних даних – медичних, фінансових, геолокаційних, поведінкових. Це підвищує ризики зловживань, витоків, несанкціонованого доступу та інструментального використання даних для маніпуляцій. Наявні нормативні механізми захисту даних в Україні, зокрема Закон «Про захист персональних даних», мають бути адаптовані до викликів алгоритмічної обробки та машинного навчання.

2. Дискримінація та несправедливість алгоритмів. Вони можуть бути упередженими. Це може призводити до дискримінації за ознаками раси, статі, віку чи соціального статусу [2].

3. Непрозорість рішень. Частина моделей ШІ (особливо глибинні нейромережі) є непрозорими за своєю природою. Це ускладнює доступ громадян до розуміння, як і чому приймається рішення, яке впливає на їх життя (наприклад, блокування доступу до соціальних послуг, кредитування тощо). У цьому контексті постає питання прав на пояснення рішення.

Щодо розвитку інститут цифрового омбудсмана, то можемо відзначити таке: він є незалежною посадовою особою, уповноваженою захищати цифрові права громадян, розглядати звернення щодо порушень, моніторити застосування ШІ, забезпечувати аудити алгоритмів, сприяти дотриманню етичних стандартів, надавати рекомендації та виступати арбітром у спорах між громадянами та технологічними компаніями або державними органами.

Подібна практика вже існує в деяких країнах, наприклад: Нідерланди (Data Protection Authority з функціями контролю алгоритмів); Естонія (Естонська аудиторська служба та digital ombuds structures); Канада (Office of the Privacy Commissioner працює із ШІ-ризиками) (рис. 1).

Рис. 1. Інститут цифрового омбудсмана у світі.
Джерело: складено на підставі [4]

Цифровий омбудсман може виконувати такі завдання: контролювати дотримання цифрових прав; аналізувати вплив ШІ на права людини; ініціювати незалежні аудити алгоритмів; виступати посередником у спорах; розробляти рекомендації для політиків; сприяти цифровій грамотності та правовій освіті. Зрозуміло, що цифровий омбудсман повинен мати незалежний статус, право доступу до даних та алгоритмів у межах перевірок, можливість виступати в судах, право публікувати звіти та фінансову незалежність. Такий орган може бути створений у складі вже існуючих структур або як окрема інституція. Можливі декілька моделей,: 1) парламентська (як частина системи омбудсманів); 2) урядова (у структурі виконавчої влади); 3) гібридна модель із високим рівнем автономії [1; 4]. З точки зору демократичних стандартів уважаємо, що найбільш ефективною виглядає парламентська модель із гарантованою незалежністю. За цих умов цифровий омбудсман може стати ключовим елементом екосистеми цифрової демократії, де держава виступає не лише провайдером послуг, а й гарантом цифрової гідності людини.

Список використаних джерел:

1. Дідух Х.В. Цифрові права: український та європейський досвід. Науковий вісник Ужгородського Національного університету. 2024. Серія ПРАВО. Випуск 85: частина 1. С. 59–65.

2. Домбровська С., Помаза-Пономаренко А., Крюков О., Порока С. Інформаційні загрози та комунікативна інфраструктура в державному секторі : монографія. Харків: НУЦЗУ, 2024. 244 с.

3. Помаза-Пономаренко А.Л. Механізми публічного управління у сфері правозахисних інститутів (громадянського суспільства й омбудсмана) // Вісник Національного університету цивільного захисту України. 2025. № 1 (23). С. 16–23.

4. Роговенко О.В., Лозін А.О. Інститут омбудсмена як гарант захисту цифрових прав людини в Україні: сучасні виклики та зарубіжний досвід. URL: http://journal-app.uzhnu.edu.ua/article/view/341908.

Пономаренко В.В.
викладач кафедри адміністративного права та процесу
навчально-наукового інституту
права та соціального менеджменту
(*Донецький державний університет внутрішніх справ*)

АВТОМАТИЗАЦІЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ ЯК ЕЛЕМЕНТ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ СЕКТОРУ БЕЗПЕКИ

Цифровізація суспільних відносин та стрімкий розвиток інформаційних технологій зумовлюють трансформацію діяльності державних інституцій, у тому числі органів сектору безпеки та правопорядку. У сучасних умовах ефективність функціонування правоохоронних органів дедалі більше залежить від здатності використовувати цифрові інструменти, автоматизовані системи обробки даних та технології штучного інтелекту. У цьому контексті автоматизація правоохоронної діяльності виступає важливим елементом цифрової трансформації сектору безпеки, спрямованим на підвищення ефективності управління, оперативності реагування на правопорушення та забезпечення належного рівня захисту прав і свобод людини.

Питання впровадження цифрових технологій у діяльність правоохоронних органів набуває особливої актуальності в умовах сучасних безпекових викликів, пов'язаних із воєнною агресією, кіберзлочинністю, транснаціональними правопорушеннями та необхідністю забезпечення належного рівня публічної безпеки. Цифрова трансформація сектору безпеки передбачає не лише модернізацію технічної інфраструктури, а й переосмислення організаційних підходів до здійснення правоохоронної діяльності, зокрема шляхом інтеграції автоматизованих інформаційних систем, електронних баз даних та аналітичних платформ.

У науковій літературі автоматизацію правоохоронної діяльності розглядають як процес впровадження інформаційно-комунікаційних технологій, програмних комплексів та алгоритмічних систем, що забезпечують автоматизовану обробку інформації, підтримку прийняття управлінських рішень та

оптимізацію службових процедур. У практичному вимірі це проявляється у створенні єдиних інформаційних систем, автоматизованих баз даних, електронних систем обліку правопорушень, цифрових платформ аналітичної обробки інформації, а також використанні технологій штучного інтелекту для прогнозування криміногенних процесів.

Важливу роль у процесі цифрової трансформації правоохоронної системи відіграє діяльність Національної поліції України, яка активно впроваджує сучасні інформаційні технології у сфері забезпечення публічної безпеки та протидії злочинності. Серед таких технологій можна відзначити системи відеоспостереження, автоматизовані комплекси фіксації правопорушень, електронні інформаційні бази, а також аналітичні системи обробки великих масивів даних. Використання зазначених інструментів дозволяє підвищити оперативність реагування на правопорушення, удосконалити процеси кримінального аналізу та покращити координацію між різними суб'єктами сектору безпеки.

Автоматизація правоохоронної діяльності також сприяє підвищенню ефективності управлінських процесів у системі органів правопорядку. Застосування цифрових платформ дозволяє оптимізувати документообіг, забезпечити швидкий доступ до необхідної інформації, підвищити прозорість діяльності органів влади та зменшити ризики корупційних проявів. У цьому контексті автоматизовані системи виступають інструментом підвищення підзвітності правоохоронних органів та зміцнення довіри суспільства до державних інституцій.

Водночас процес цифрової трансформації правоохоронної діяльності супроводжується низкою правових, організаційних та етичних викликів. Однією з ключових проблем є необхідність забезпечення належного рівня захисту персональних даних та інформаційної безпеки. Використання автоматизованих систем передбачає обробку значних обсягів інформації, що може містити конфіденційні відомості про осіб, а отже потребує створення ефективних механізмів контролю та правового регулювання.

Не менш важливим є питання забезпечення балансу між підвищенням ефективності правоохоронної діяльності та дотриманням прав людини. Автоматизовані системи прийняття рішень, алгоритмічний аналіз даних та технології розпізнавання

облич можуть створювати ризики порушення права на приватність, недискримінаційного ставлення та справедливого процесу. Саме тому впровадження таких технологій має супроводжуватися чіткими правовими гарантіями, які передбачають прозорість алгоритмів, можливість людського контролю за автоматизованими рішеннями та ефективні механізми оскарження.

У цьому контексті важливе значення мають міжнародні стандарти використання цифрових технологій у діяльності органів влади, зокрема рекомендації та нормативні акти Європейського Союзу і Ради Європи, спрямовані на забезпечення етичного та безпечного використання штучного інтелекту. Імплементація таких стандартів у національне законодавство України є важливим кроком на шляху формування ефективної та правової моделі цифрової трансформації сектору безпеки.

Важливим напрямом розвитку автоматизації правоохоронної діяльності є використання аналітичних систем, здатних здійснювати прогнозування криміногенних процесів на основі аналізу великих масивів даних. Такі системи дозволяють визначати потенційні зони підвищеного рівня злочинності, прогнозувати можливі правопорушення та планувати превентивні заходи. Разом з тим застосування подібних технологій потребує обережного підходу, оскільки алгоритмічні моделі можуть містити упередження або помилки, що впливатимуть на об’єктивність прийняття рішень.

Цифрова трансформація сектору безпеки також передбачає розвиток міжвідомчої інформаційної взаємодії між різними органами державної влади. Інтеграція інформаційних систем правоохоронних органів, судових установ, органів прокуратури та інших суб’єктів публічної влади дозволяє підвищити ефективність обміну інформацією, скоротити час обробки даних та забезпечити комплексний підхід до протидії злочинності. У результаті формується єдиний інформаційний простір безпеки, який сприяє більш ефективному управлінню безпековими процесами.

Разом із тим впровадження автоматизованих систем у діяльність правоохоронних органів вимагає належної підготовки кадрів. Працівники сектору безпеки повинні володіти не лише професійними юридичними знаннями, а й навичками роботи з

цифровими технологіями, аналітичними системами та базами даних. Підвищення цифрової компетентності правоохоронців є необхідною передумовою успішної реалізації процесів цифрової трансформації.

Отже, автоматизація правоохоронної діяльності є важливим напрямом модернізації сектору безпеки та невід'ємною складовою цифрової трансформації державного управління. Використання сучасних інформаційних технологій сприяє підвищенню ефективності боротьби зі злочинністю, удосконаленню управлінських процесів та зміцненню взаємодії між суб'єктами сектору безпеки. Водночас успішність впровадження автоматизованих систем залежить від створення належної нормативно-правової бази, забезпечення захисту прав людини, розвитку кадрового потенціалу та впровадження міжнародних стандартів використання цифрових технологій. Саме комплексний підхід до цифрової трансформації правоохоронної системи здатний забезпечити формування ефективної, сучасної та орієнтованої на потреби суспільства моделі забезпечення безпеки.

Попович Є.
курсант факультету підготовки фахівців
для органів досудового розслідування
Національної поліції України
(Донецький державний університет внутрішніх справ).
Науковий керівник – **Умрихіна І.**
завідувач кафедри адміністративно-правових дисциплін
факультету підготовки фахівців
для підрозділів превентивної діяльності НПУ,
доктор філософії, доцент
(Донецький державний університет внутрішніх справ)

ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ: СОЦІАЛЬНО-ЕКОНОМІЧНІ ПЕРСПЕКТИВИ ТА ЕТИЧНІ РИЗИКИ

Процеси глобальної цифровізації на сучасному етапі розвитку цивілізації трансформувалися з суто технологічного явища у фундаментальний соціально-філософський контекст. Центральним елементом цієї трансформації виступає штучний інтелект (ШІ), який інтегрується в усі сфери людської життєдіяльності - від побутових сервісів до стратегічного державного управління. Актуальність дослідження зумовлена тим, що швидкість експоненціального розвитку технологій значно перевищує темпи адаптації правових інститутів та етичних норм, створюючи певний вакуум відповідальності та ризики для соціокультурної стабільності.

Розглядаючи нові можливості, що відкриваються перед суспільством, слід відзначити кардинальне підвищення ефективності аналізу великих масивів даних. Впровадження ШІ у державний сектор дозволяє реалізувати концепцію «цифрового уряду», де алгоритми забезпечують прозорість прийняття рішень, автоматизують надання адміністративних послуг та мінімізують людський фактор, що безпосередньо сприяє подоланню корупційних ризиків. У сфері охорони здоров’я цифровізація забезпечує перехід до предиктивної медицини: аналіз біометричних даних у реальному часі дозволяє діагностувати

патології на ранніх стадіях, що раніше було неможливим. Освітня галузь отримує інструменти для створення персоналізованих адаптивних платформ, які підлаштовуються під індивідуальний темп засвоєння матеріалу кожним учнем. Економічний ефект від цифровізації полягає у створенні самооптимізованих логістичних ланцюгів та систем точного прогнозування ринкової кон'юнктури, що є запорукою сталого розвитку в умовах глобальної нестабільності [1].

Водночас, масштабна інкорпорація інтелектуальних систем у суспільну тканину породжує комплекс етичних викликів, які потребують негайного вирішення. Найбільш критичною є проблема алгоритмічної дискримінації. Оскільки моделі ШІ навчаються на історичних даних, вони часто успадковують та мультиплікують людські упередження щодо раси, гендеру або соціального статусу, що призводить до несправедливих рішень у банківському скорингу, наймі персоналу чи навіть у судочинстві [2]. Наступним викликом є криза приватності. Масовий збір персональної інформації та розвиток технологій розпізнавання облич створюють передумови для формування систем «соціального кредиту», де кожен крок індивіда стає об'єктом аналізу та контролю, що суперечить демократичним цінностям та праву на анонімність. Не менш важливою є проблема «експлікативності» (explainability) - неможливості простежити логічний ланцюжок прийняття рішення нейронною мережею, що створює загрозу безпеці у критичних інфраструктурах. Зрештою, автоматизація когнітивної діяльності актуалізує питання трансформації ринку праці, де значна частина професій інтелектуальної сфери може бути заміщена алгоритмами, вимагаючи розробки нових моделей соціального договору [3].

Отже, цифровізація суспільства має відбуватися в межах людиноцентрованої парадигми. Необхідно запровадити міжнародні стандарти етичного проектування (Ethics by Design), які передбачають інтеграцію гуманістичних принципів безпосередньо в алгоритмічну структуру ШІ. Ключовим завданням для наукової спільноти та державних інституцій є розробка механізмів аудиту алгоритмів на предмет їхньої прозорості та справедливості. Штучний інтелект має розглядатися не як автономна сила, а як інструмент посилення людського потенціалу,

що діє в чітких етичних та правових кордонах. Тільки за умови гармонійного поєднання технологічного інноваційного драйву з аксіологічними засадами гуманізму можливо побудувати безпечне та прогресивне цифрове майбутнє [4].

Список використаних джерел:

1. Шваб К. Четверта промислова революція / пер. з англ. Р. Корнута. Київ : Форс Україна, 2019. 224 с.

2. O'Neil C. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. New York : Broadway Books, 2016. 272 p.

3. Бостром Н. Суперінтелект: Стратегії і небезпеки розвитку розумних машин / пер. з англ. А. Івашко. Київ : Наш Формат, 2020. 400 с.

4. Floridi L. The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities. Oxford : Oxford University Press, 2023. 320 p.

Похиленко І.С.
доцент кафедри права та публічного управління,
кандидат юридичних наук, доцент
*(Київський національний університет
будівництва і архітектури)*

ГЕНЕРАТИВНИЙ ШІ ТА МЕЖІ АВТОРСТВА: СПІВВІДНОШЕННЯ АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ ТА АВТОРСЬКОГО ПРАВА В КОНТЕКСТІ ЄВРОІНТЕГРАЦІЇ УКРАЇНИ

Активний розвиток генеративних технологій штучного інтелекту зумовив необхідність формування нових правових стандартів використання цифрових інструментів у науковій та освітній діяльності. Одним із ключових нормативних орієнтирів у цій сфері стало закріплення спеціальних вимог щодо використання результатів, створених із застосуванням штучного інтелекту, у Законі України «Про академічну доброчесність».

Відповідно до п. 4 ст. 8 зазначеного Закону, у разі використання в академічному творі об'єкта, згенерованого штучним інтелектом, автор зобов'язаний повідомити про це в такому творі із зазначенням методики генерування та/або посилання на відповідну комп'ютерну програму чи її опис відповідно до встановлених вимог оформлення академічних робіт. Зазначена норма формує принципово новий стандарт прозорості академічної діяльності, який спрямований на забезпечення достовірності наукових результатів та належної ідентифікації творчого внеску автора.

Правове значення цієї норми полягає у запровадженні обов'язку декларування використання штучного інтелекту як окремого елементу академічної відповідальності. Фактично законодавець визнає, що генеративні моделі можуть виступати інструментом створення наукового контенту, однак їх застосування не повинно призводити до підміни особистої інтелектуальної діяльності дослідника. Такий підхід узгоджується із загальними принципами академічної доброчесності, зокрема чесності, прозорості та відповідальності.

Зазначене положення також має важливе значення для визначення меж авторства. Обов'язок розкриття інформації про використання генеративних систем фактично підтверджує, що результати діяльності штучного інтелекту не можуть розглядатися як повністю автономний продукт творчості людини. Водночас закон не забороняє використання таких інструментів, що свідчить про орієнтацію на інтеграцію інноваційних технологій у наукову діяльність за умови дотримання принципів доброчесності.

Проблема авторства у сфері генеративного ШІ є предметом жвавих дискусій у світовій юридичній літературі. Д. Лім [1] наголошує, що генеративний штучний інтелект є «тестом для авторського права», оскільки сучасні норми базуються на принципі **сингулярної людської творчості як умови охорони.** При цьому судові практики, зокрема рішення суду США, вказали, що хоча право «влаштоване так, щоб адаптуватися», **людська креативність залишається фундаментальною умовою правоздатності твору.**

Це підтверджується і практикою Національного бюро з авторських прав США [2], яке визначає, що твір, створений виключно алгоритмом без значного людського контролю, **не може бути охоронюваним об'єктом авторського права**, оскільки відсутній суб'єкт із вираженою креативною участю людини. Якщо ж творчий внесок людини у створенні твору очевидний, такі твори можуть отримати авторське право.

У роботі І.Лі [3] аналізуються підходи країн до **вимог людського авторства** як ключової умови охорони авторських прав у творах, що створюються із використанням генеративних алгоритмів. Більшість юрисдикцій зберігають вимогу участі людини для отримання правової охорони.

Європейський контекст розвитку правового регулювання штучного інтелекту визначається ухваленням Регламенту (ЄС) 2024/1689 (Artificial Intelligence Act), який встановлює вимоги щодо прозорості функціонування систем ШІ та дотримання прав інтелектуальної власності під час навчання моделей [4]. Для України, яка перебуває у процесі гармонізації законодавства з правом ЄС, ці підходи мають стратегічне значення. Імплементація європейських стандартів передбачає посилення вимог до розкриття використання генеративних моделей, забезпечення

людського контролю над алгоритмічними рішеннями та захист прав авторів.

Окремої уваги заслуговують сучасні українські дослідження впливу генеративного штучного інтелекту на правові системи сучасних держав. Зокрема, **А. Гачкевич [5]** обґрунтовує, що розвиток генеративних технологій зумовлює необхідність модернізації традиційних правових підходів, сформованих у межах романо-германської правової сім'ї. Автор визначає генеративний ШІ як технології, що забезпечують створення текстів, зображень, аудіо та відео шляхом «синтетичної творчості» на основі інструкцій користувача, підкреслюючи, що саме інтенсивність і характер людського контролю є ключовим критерієм для правової кваліфікації результатів такої діяльності.

Отже, розвиток генеративного штучного інтелекту актуалізує переосмислення меж авторства та співвідношення академічної доброчесності й авторського права. Українське законодавство, зокрема п. 4 ст. 8 Закону України «Про академічну доброчесність», закріплює обов'язок прозорості використання ШІ, тим самим підтверджуючи пріоритет людського творчого внеску. Порівняльний аналіз міжнародних підходів і положень права ЄС свідчить про збереження вимоги людської креативності як умови правової охорони. У контексті євроінтеграції Україна формує модель регулювання, за якої генеративний ШІ розглядається як інструмент інтелектуальної діяльності, а не самостійний суб'єкт авторства, що забезпечує баланс інноваційного розвитку, правової визначеності та захисту прав людини.

Список використаних джерел:

1. Lim D. *Generative AI and copyright: principles, priorities and practicalities.* Journal of Intellectual Property Law & Practice. 2023. Vol. 18, No. 12, P. 841–842. DOI: https://doi.org/10.1093/jiplp/jpad081

2. O'Brien M. *AI-assisted works can get copyright with enough human creativity, says US copyright office* [Electronic resource]. AP News. January 30, 2025. URL: https://apnews.com/article/ai-copyright-office-artificial-intelligence-363f1c537eb86b624bf5e81bed70d459 (дата звернення: 13.02.2026).

3. Li Yiran. *The Human Authorship Requirement in AI-Generated Works: A Comparative Analysis of Copyright Protection Frameworks.* Journal of Law and Governance. 2025. DOI: https://doi.org/10.64229/671z9c57

4. 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) // Official Journal of the European Union. 2024. OJ L 2024/1689, 12 July 2024. ELI: http://data.europa.eu/eli/reg/2024/1689/oj (дата звернення: 13.02.2026).

5. Гачкевич А. *Вплив генеративного штучного інтелекту на правові системи сучасних держав.* Право та інноваційне суспільство. 2025. № 1(24), С. 37-46. DOI: https://doi.org/10.37772/2309-9275-2025-1(24)-3

Пристайчук Ю.А.
здобувачка ступеня магістра
навчально-наукового інституту права
(Київський національний університет імені Тараса Шевченка)
Мірошников І.Ю.
доцент кафедри кримінального процесу та криміналістики
навчально-наукового інституту права,
кандидат юридичних наук, доцент
(Київський національний університет імені Тараса Шевченка)

ГЕНЕРАТИВНИЙ ШТУЧНИЙ ІНТЕЛЕКТ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ: РИЗИКИ ПРОЦЕСУАЛЬНОГО ПИСЬМА

Генеративний штучний інтелект, зокрема великі мовні моделі, дедалі частіше використовують юристи як допоміжний інструмент для написання та редагування текстів. Це стосується чернеток процесуальних документів, стислого викладу позицій сторін і структурування великих обсягів матеріалів справи. У кримінальному провадженні такі інструменти справді можуть пришвидшувати роботу. Однак саме в цій сфері будь-яка технологічна помилка або недостатня перевірка результату здатні перерости у процесуальну шкоду, оскільки рішення впливають на права людини та можуть спричиняти істотні обмеження свободи й приватності. Тому ключовим є не питання заборони чи дозволу, а визначення меж допустимого застосування і процедурних запобіжників, які унеможливлюють підміну доказування та мотивування правдоподібно сформульованим, але неперевіреним текстом.

Великі мовні моделі (LLM) - це різновид систем штучного інтелекту, які навчаються на дуже великих масивах текстів і здатні генерувати або переформульовувати текст на основі закономірностей, засвоєних із даних, пропонуючи найбільш імовірні мовні конструкції [1, с.3]. До таких моделей належать, зокрема, сімейства Claude, Gemini, GPT, а також відкриті моделі

Llama (Meta), які застосовуються для генерування та редагування текстів. Для кримінального провадження важливо, що такі системи можуть створювати стилістично переконливі формулювання, але не гарантують точності, повноти та коректності посилань, тому потребують обов'язкової верифікації перед включенням у процесуальні документи.

У кримінальному провадженні вимоги до контролю процесуальних текстів має бути посиленим, адже суд оцінює докази за внутрішнім переконанням, і жодні відомості не мають наперед визначеної сили (ст. 94 КПК України). Судовий акт, у свою чергу, повинен бути законним, обґрунтованим і вмотивованим, тобто спиратися на встановлені обставини, підтверджені дослідженими доказами, із наведенням достатніх мотивів та підстав (ст. 370 КПК України). Відтак використання великих мовних моделей у процесуальному письмі допустиме лише тоді, коли зберігається контрольованість і відтворюваність кожного твердження, а сторони реально можуть перевіряти і спростовувати аргументацію, покладену в основу процесуального рішення [2].

Окрему групу загроз становить поява у процесуальних документах недостовірних елементів, що виглядають переконливо і можуть залишитися непоміченими під час фінальної перевірки. У застосуванні генеративних моделей це проявляється як «галюцинації», тобто вигадані реквізити, некоректні посилання та доповнення мотивування твердженнями без опори на матеріали провадження. Показовими є випадки, коли після використання генеративних інструментів у поданих до суду матеріалах виявлялися вигадані або помилкові посилання через відсутність верифікації джерел [3]. На рівні європейських підходів ця проблема прямо відображена у настановах CEPEJ щодо генеративного ШІ для судів, де наголошується на ризику «галюцинацій» та необхідності належного людського нагляду за результатами генерації [4, с. 4]. Практична небезпека полягає в тому, що в документ може потрапити неправдива правова підстава, а інша сторона буде змушена витрачати ресурси на спростування тверджень, яких немає ні в матеріалах справи, ні в судовій практиці.

Суттєвою процесуальною проблемою є автоматизаційне зміщення, тобто схильність сприймати згенерований текст як нейтральний і достатньо перевірений лише через його узгодженість та переконливий стиль, особливо за умов дефіциту часу та високого навантаження. У судовому письмі це може проявлятися як підміна реальної логіки мотивування формально узгодженою аргументацією, яка не має належної прив'язки до досліджених доказів.

Додаткові труднощі створює непрозорість роботи таких систем, що ускладнює контроль походження формулювань і логіки їх добору, а також зменшує можливість контролю й пояснення згенерованого результату у процесуальному вимірі. У зарубіжній практиці прикладом для розуміння процесуальних наслідків використання закритих алгоритмічних методик є справа State v. Loomis, у якій суд оцінював вплив алгоритмічної оцінки ризику на рішення. Дана справа демонструє загальну для кримінальної юстиції проблему, яка за відсутності доступної методики та можливості відтворюваної перевірки зростає ймовірність, що технологічний продукт впливатиме на рішення без достатнього процесуального контролю [5].

Окремий блок ризиків стосується конфіденційності та захисту персональних даних під час використання генеративних інструментів у роботі з матеріалами кримінального провадження [6, с. 177]. Ризик зростає, коли для підготовки або редагування текстів залучаються зовнішні сервіси, адже туди можуть потрапити фрагменти матеріалів провадження, що містять персональні дані або іншу охоронювану інформацію. В українському правопорядку це стикається з конституційними гарантіями приватності та загальною забороною необґрунтованого збирання, зберігання, використання конфіденційної інформації про особу, що вимагає особливої обережності при залученні зовнішніх сервісів ШІ.

Отже, використання генеративних інструментів у кримінальному провадженні доцільно розглядати як потенційний ризик для процесуальної якості текстів: їх точності, посилальності, мотивованості та можливості перевірки. Такі ризики виникають як у документах сторін, так і в судових актах, але найбільш критичними стають там, де текст набуває вирішального значення

для прав особи. Так допустимість зводиться до збереження перевірюваності, адже будь-який виклад має бути відтворюваним за першоджерелами, а переконливість форми не може замінювати доказову й логічну обґрунтованість.

Список використаних джерел:

1. Bommasani R., et al. On the Opportunities and Risks of Foundation Models [Електронний ресурс]. arXiv preprint arXiv:2108.07258, 2021. URL: https://arxiv.org/abs/2108.07258 (дата звернення: 01.03.2026).

2. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI (зі змін. і доп.). URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 01.03.2026).

3. Merken S. New York lawyers sanctioned for using fake ChatGPT cases in legal brief // Reuters. 26.06.2023. URL: https://www.reuters.com/legal/new-york-lawyers-sanctioned-using-fake-chatgpt-cases-legal-brief-2023-06-22/ (дата звернення: 01.03.2026).

4. CEPEJ. Guidelines on the use of generative artificial intelligence for courts (CEPEJ(2025)18Final) [Електронний ресурс]. 19.12.2025. Council of Europe. URL: https://rm.coe.int/cepej-2025-18final-en-draft-guidelines-on-the-use-of-generative-ai-for/48802a4ad1 (дата звернення: 01.03.2026).

5. State v. Loomis: Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessments in Sentencing // Harvard Law Review. 2017. Vol. 130, No. 5. P. 1530–1537. URL: https://harvardlawreview.org/print/vol-130/state-v-loomis/ (дата звернення: 01.03.2026).

6. Гудзь Л. В. Забезпечення права на приватність у контексті використання штучного інтелекту: потенційні загрози та шляхи їх подолання // Науковий вісник Ужгородського національного університету. Серія «Право». 2024. Вип. 86, ч. 1. С. 175–180. DOI: 10.24144/2307-3322.2024.86.1.25. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/01/27.pdf (дата звернення: 01.03.2026).

Присяжнюк Е.В.
курсант
(Харківський національний університет внутрішніх справ)
Пчеліна О.В.
професор кафедри кримінального процесу
та організації досудового слідства,
доктор юридичних наук, професор
(Харківський національний університет внутрішніх справ)

ПРОТИДІЯ КІБЕРШАХРАЙСТВУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ DEEPFAKE: ВИКЛИКИ ДЛЯ ДОСУДОВОГО РОЗСЛІДУВАННЯ

Розвиток штучного інтелекту дав правопорушникам нові зручні інструменти, і головний із них – це deepfake. Ця технологія дозволяє робити дуже реалістичні підробки відео та аудіо, які зараз масово використовують для шахрайства, шантажу та ворожих інформаційних маніпуляцій в умовах війни. Для органів досудового розслідування це серйозна проблема, бо старі методи криміналістики з такими кримінальними правопорушеннями майже не працюють. Шукати цифрові сліди та доводити факт підробки стало набагато складніше.

Серед найбільш розповсюджених способів створення діпфейків можна виділити такі: 1) заміну обличчя: обличчя однієї людини у відеоматеріалі замінюється на обличчя іншої людини; 2) синхронізацію губ: рухи губ людини на оригінальному відео узгоджуються з неоригінальним аудіозаписом; 3) «ляльковод»: відеозображення людини (рухи голови, рухи очима, міміка) анімує виконавець, що сидить перед камерою і виконує дії, які він хоче бачити на відео від створеного персонажу. Отже, застосування технології Deepfake надає безмежні можливості для створення відеоконтенту, в якому можна «примусити» будь-яку особу сказати або зробити будь-що [1, с. 32–33].

У контексті досліджуваного питання варто вказати, що криміналістичний аналіз deepfake-контенту є складним та багатогранним процесом, що включає застосування різноманітних технічних та аналітичних методів. Основна мета експертизи

полягає в ідентифікації ознак підробки та встановленні автентичності досліджуваних медіафайлів. До основних методів криміналістичного аналізу deepfake-контенту належать: аналіз цифрових артефактів (вивчення метаданих файлів, слідів редагування, особливостей стиснення та інших цифрових характеристик, які можуть свідчити про маніпуляції); аналіз частоти кадрів та часових аномалій (виявлення невідповідностей у частоті кадрів відео, різких змін темпу або інших часових аномалій, що можуть виникати під час монтажу); вивчення візуальних невідповідностей (аналіз освітлення, тіней, відображень, кольорової гами та інших візуальних елементів на предмет їхньої узгодженості та реалістичності); виявлення асиметрії обличчя та аномалій міміки (deepfake часто призводить до ледь помітної асиметрії обличчя або нетипової міміки, оскільки відтворити складні рухи м'язів обличчя з високою точністю є складним завданням. Розпізнавання змін у динаміці міміки та рухів є значним викликом, що підкреслює важливість поєднання технічних засобів з розумінням психологічних і поведінкових особливостей людини); аналіз аудіодоріжки (виявлення штучних пауз, переривань, несинхронності звуку з відеорядом, а також аналіз спектральних характеристик голосу на предмет його штучного синтезування або маніпуляцій); застосування алгоритмів машинного навчання (розробка та використання спеціалізованих алгоритмів, навчених на великих наборах даних як справжніх, так і підроблених медіафайлів, для автоматизованого виявлення ознак фальсифікації. Ці алгоритми здатні виявляти невидимі людському оку закономірності та аномалії).

З вищенаведеного вбачається, що важливим аспектом є комплексний підхід до аналізу, який об'єднує технічні методи з глибоким розумінням людської поведінки та психології. Поєднання технічного та гуманітарного підходів, як правильно підкреслено у тексті, є запорукою об'єктивності результатів експертизи [2, с. 502–503].

Практична небезпека використання таких технологій яскраво підтверджується нещодавніми фактами організованого кібершахрайства в Україні. Зокрема, правоохоронці викрили організовану групу, яка за допомогою штучного інтелекту оформлювала кредити на українців. Про це повідомила

Національна поліція України. Зазначається, що оборудку організувала 33-річна жінка, яка під час повномасштабного вторгнення виїхала до Польщі. До злочинної діяльності залучила колишнього чоловіка та знайомого з Миколаєва. Жінка отримувала з невстановлених джерел персональні дані користувачів онлайн-банкінгу – фінансові номери мобільних телефонів, паролі та коди авторизації. Отриману інформацію вона передавала іншим учасникам групи, які здійснювали несанкціоновані входи до мобільних застосунків українських банків, а далі – у «Дію» через систему авторизації BankID. Після отримання доступу до електронних кабінетів громадян зловмисники завантажували їхні цифрові документи, а організаторка виготовляла короткі DeepFake-відео, використовуючи обличчя потерпілих. Ці підроблені ролики застосовувалися для проходження фото-верифікації у банківських онлайн-системах. За словами правоохоронців, зловмисники уклали договори та відкрили рахунки від імені щонайменше 286 громадян, а на частину з них оформили кредити на суму понад 4 000 000 гривень. Отримані кошти учасники групи переводили на підконтрольні рахунки у різних фінансових установах. У подальшому гроші конвертували у криптовалюту та обготівковували. Трьом учасникам організованої групи повідомлено про підозру у шахрайстві та у несанкціонованому втручанні в роботу інформаційно-комунікаційних систем. Їм загрожує покарання – 15 років ув'язнення із конфіскацією майна [3].

Підсумовуючи, варто зауважити, що стрімкий розвиток технологій створення штучного контенту становить серйозний виклик для системи кримінальної юстиції, серед іншого органів досудового розслідування, оскільки традиційні криміналістичні методики часто виявляються недостатньо ефективними. Успішна ідентифікація підробок вимагає комплексного підходу, який поєднує глибокий аналіз цифрових артефактів, використання машинного навчання та розуміння психолого-поведінкових особливостей людини.

Реальна правоохоронна практика підтверджує масштаб загрози: використання діпфейків для обходу систем біометричної верифікації, як у випадку з масовим оформленням кредитів,

демонструє високий рівень організації таких кіберзлочинів. Це зумовлює нагальну потребу в постійному оновленні технічного оснащення органів досудового розслідування та розробці новітніх алгоритмів протидії несанкціонованому втручанню в інформаційно-комунікаційні системи.

Список використаних джерел:

1. Юртаєва К. В. Кримінологічний аналіз використання технології deepfake: коли фейк стає злочином. *Вісник кримінологічної асоціації України.* 2021. №1(24). С. 31–42.

2. Стріляна А. В., Макарова О. П. Криміналістична експертиза deepfake-контенту: методики виявлення та процесуальні аспекти. *Актуальні проблеми сучасної науки в дослідженнях молодих учених, курсантів та студентів*: тези доп. всеукр. наук.-практ. конф. (м. Вінниця, 16 трав. 2025 р.). Вінниця: ХНУВС, 2025. С. 501–504.

3. Українка із Польщі за допомогою ШІ та Deepfake оформила на співвітчизників кредити на 4 млн грн. *Судово-юридична газета.* (14 жовт. 2025). URL: https://sud.ua/uk/news/ukraine/343586-ukrainka-iz-polshi-s-pomoschyu-ii-i-deepfake-oformila-na-sootechestvennikov-kredity-na-4-mln-grn (дата звернення: 27.02.2025).

Рабко Т.О.
адвокат,
заступниця голови Комітету НААУ
з питань електронного судочинства
та кібербезпеки адвокатської діяльності
(Національна асоціація адвокатів України)

ПРАКТИЧНІ АСПЕКТИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ПРИ СУПРОВОДІ СУДОВИХ СПРАВ

Питання використання штучного інтелекту стає не тільки сучасним трендом, але і реаліями сьогодення.

Беззаперечно використання штучного інтелекту має безліч переваг, що дозволяє позбутися рутинних процесів та оптимізувати робочі задачі.

Але при цьому потрібно не забувати про потенційні ризики необдуманого використання нових технологій.

Слід відзначити, що штучний інтелект здатен суттєво підсилити професійну діяльність юриста, однак залишається лише допоміжним інструментом. Остаточна відповідальність за якість документів та правову позицію незмінно належить юристу.

Сьогодні ми спостерігаємо ситуацію, коли громадяни не маючи спеціальних юридичних знань намагаються створити процесуальні документи за допомогою штучного інтелекту.

Однак необхідно врахувати, що будь-який результат отриманий за допомогою штучного інтелекту потребує критичній оцінці.

Успішність опрацювання запиту штучним інтелектом залежить від якісно сформованого запиту.

Розглянимо приклади із судової практики.

Ухвала Сумського апеляційного суду від 17.02.2026 по справі № 589/5099/25 «…Окремої уваги заслуговують доводи апелянта щодо нібито існуючих правових позицій Верховного Суду. Аналіз змісту апеляційної скарги дає підстави для висновку про недобросовісне використання інструментів штучного інтелекту при її підготовці. Посилання на постанови Верховного

Суду (зокрема № 243/666/17, № 991/7554/19, № 761/40480/20, № 757/22584/21-к) як на такі, що регулюють оскарження рішень слідчого про відмову у задоволенні клопотань, є грубим викривленням реальної судової практики. Перевіркою встановлено, що зазначені номери справ або відсутні в Єдиному державному реєстрі судових рішень, або стосуються проваджень у цивільних справах, розглянутих судами першої інстанції, та не містять жодних висновків Верховного Суду щодо застосування норм КПК України. Використання вигаданих правових позицій (так званих «галюцинацій» штучного інтелекту) та подання до суду неперевірених документів, порушує принцип юридичної визначеності та є виявом неповаги до суду.…» [1]

Ухвала Дніпровського апеляційного суду від 05.02.2026 по справі № 185/2861/25 «…твердження захисника про існуючу усталену судову практику у подібних випадках є недостовірними, не може розглядатися як належний юридичний аргумент та може свідчити про використання останньою штучного інтелекту без належного контролю за наданою ним інформацією, що є неприпустимим для професійного юриста -адвоката…» [2]

Рішення Господарського суду Івано-Франківської області від 03.02.2026 по справі № 909/1174/25 «…судом здійснено перевірку усіх процесуальних документів представника позивача на предмет використання інструментів штучного інтелекту та встановлено, що вони подані у відповідності до вимог процесуального закону, правові позиції у поданих заявах відповідають існуючим правовим позиціям Верховного Суду, окрім судової практики, зазначеної у відповіді на відзив з посиланням на постанову Великої Палати Верховного Суду від 19.01.2021 у справі № 916/1415/19, в якій зазначено: "Пред`явлення позову, яке відповідно до статті 264 ЦК України перериває перебіг позовної давності, означає, що Позивач скористався своїм правом на захист у суді… Після переривання перебіг позовної давності починається заново, а час, що минув до переривання, до нового строку не зараховується", правова позиція в якій не міститься у означеній вище постанові Великої Палати Верховного Суду, що підтверджується офіційними джерелами - базами законодавства та реєстром судових рішень...» [3]

Ухвала Приморського районного суду м. Одеси від 27.01.2026 по справі 522/8694/25-е «…повторно сформована за

допомогою штучного інтелекту та подана заява є явно необґрунтованою та завідомо безпідставною (фактично зводиться до незгоди з рішенням суду, повторного перегляду висновків суду з наданням іншого судового тлумачення і надання відповіді на питання, що взагалі не були предметом спору), не відповідає завданню цивільного судочинства та є фактично зловживанням правом на подання заяви, тому суд вважає її неприйнятною згідно зі ст. 44 ЦПК України. Схожа позиція викладена в ухвалі Верховного Суду від 8 лютого 2024 року по справі № 925/200/22…» [4]

Ухвала Вознесенівського районного суду міста Запоріжжя від 20.01.2026 по справі 335/7222/21 «…окремо суд звертає увагу на те, що відзив ОСОБА_2 на заяву про зміну способу і порядку виконання судового рішення вочевидь сформований за допомогою технологій штучного інтелекту, про що свідчать певні фрази, наведені у відзиві (зокрема абз. 6, 7 стор. 3 відзиву)…» [5]

Постанова Шостого апеляційного адміністративного суду від 23.12.2025 по справі № 365/627/25 «…Посилання апелянта на відомості із інтернет сайту Chat GPT суд не приймає до уваги та оцінює критично, оскільки останні не визнаються джерелом достовірної та науково доведеної інформації. Відтак суд може не приймати такі докази у справах…» [6]

Підсумовуючи зазначене потрібно врахувати, що штучний інтелект є потужним допоміжним інструментом, а не заміною правника. Технології здатні посилити аналітичний потенціал, проте відповідальність за якість процесуального документа незмінно покладається на юриста. Необхідно не забувати про дотримання балансу між використанням технологій та професійною етикою.

Список використаних джерел:

1. ЄДРСР. Ухвала Сумського апеляційного суду від 17.02.2026 по справі № 589/5099/25 URL: https://reyestr.court.gov.ua/Review/134154709.

2. ЄДРСР. Ухвала Дніпровського апеляційного суду від 05.02.2026 по справі № 185/2861/25 URL: https://reyestr.court.gov.ua/Review/133930254

3. ЄДРСР. Рішення Господарського суду Івано-Франківської області від 03.02.2026 по справі № 909/1174/25 URL: https://reyestr.court.gov.ua/Review/134067438

4. ЄДРСР. Ухвала Приморського районного суду м. Одеси від 27.01.2026 по справі 522/8694/25-е URL: https://reyestr.court.gov.ua/Review/133857838

5. ЄДРСР. Ухвала Вознесенівського районного суду міста Запоріжжя від 20.01.2026 по справі 335/7222/21 URL: https://reyestr.court.gov.ua/Review/133515013

6. ЄДРСР. Постанова Шостого апеляційного адміністративного суду від 23.12.2025 по справі № 365/627/25 URL: https://reyestr.court.gov.ua/Review/132882964

Росяк С.Т.
здобувачка вищої освіти
навчально-наукового інституту права
та правоохоронної діяльності
(Львівський державний університет внутрішніх справ).
Науковий керівник – **Проць І.М.**
доцент кафедри адміністративно-правових дисциплін
навчально-наукового інституту права
та правоохоронної діяльності,
кандидат юридичних наук, доцент
(Львівський державний університет внутрішніх справ)

ГЕРМЕНЕВТИЧНІ МЕЖІ ЗАСТОСУВАННЯ ШІ У ТЛУМАЧЕННІ НОРМ ЗАКОНОДАВСТВА

Стрімкий розвиток технологій штучного інтелекту зумовив їх активне впровадження у сферу правозастосування, включаючи аналітику судової практики, автоматизоване формування процесуальних документів, прогнозування результатів розгляду справ та підготовку проєктів рішень. У цих умовах особливої актуальності набуває питання допустимості використання систем штучного інтелекту у процесі тлумачення норм законодавства, оскільки правотлумачення є не технічною, а глибоко інтелектуальною та ціннісно зумовленою діяльністю. Проблема полягає не лише у визначенні функціональної ефективності алгоритмів, а насамперед у з'ясуванні герменевтичних меж їх застосування, тобто тих концептуальних і методологічних обмежень, за яких використання штучного інтелекту не призводить до спотворення природи права як нормативно-ціннісної системи.

Герменевтика займає одне з провідних місць у методології права, оскільки пропонує інструментарій для розуміння та вирішення правових проблем у будь-якій галузі юридичної практики через здатність вибирати та реалізовувати саме той зміст правової норми, який закладено законодавцем. Особливість такого тлумачення полягає в тому, що його зміст постає не лінгвістично-семантичним, а радше таким, що розкриває значення тексту. Ця передумова фактично є відправною точкою для побудови логіки

тлумачення, не стільки граматико-семантичного аналізу, як у більшості дослідників, скільки уточнення значення тексту, у нашому випадку – його юридичного змісту [1, с. 37].

Штучний інтелект, навпаки, функціонує на основі алгоритмічної обробки даних, статистичних моделей та машинного навчання. Сучасні системи здатні проводити семантичний аналіз текстів, виявляти закономірності в судовій практиці, формувати логічно узгоджені висновки та пропонувати варіанти правових позицій. Однак їхня діяльність базується на формалізованих структурах та ймовірнісних оцінках, що ставить під сумнів здатність алгоритмів повноцінно розуміти закон. Якщо людина-інтерпретатор інтерпретує, виходячи з усвідомлення мети закону, принципу справедливості, пропорційності та балансу інтересів, то алгоритм функціонує на основі статистичної кореляції між даними без власної ціннісної позиції.

У цьому контексті постає фундаментальне питання: чи є тлумачення права виключно логічною операцією, що може бути формалізована, чи воно містить елемент волевиявлення та оцінювання, який принципово не піддається алгоритмізації. Герменевтична традиція виходить із того, що розуміння тексту завжди передбачає інтерпретаційний акт, у якому суб'єкт співвідносить норму з власним правосвідомісним горизонтом та системою соціальних цінностей. Опосередковане пізнання, що дає змогу проникнути, заглибитись у зміст норм права, з'ясувати їхній смисл здійснюється через знання про зовнішні форми життя, зв'язки та опосередкування норм права. По-перше, до таких форм і зв'язків належить насамперед мовна форма. По-друге, норми права складають частину правової системи, кожна правова норма виявляється у зв'язках із іншими нормами. Ці зв'язки впливають на зміст тлумачення норм права та знання, такі зв'язки повинні враховуватися у процесі тлумачення. По-третє, норми права мають свою ґенезу (походження), знання про яку також використовуються при тлумаченні. По-четверте, норми права реалізуються у діях, поведінці суб'єктів, які перебувають у певній соціальній атмосфері. На поведінку цих суб'єктів впливають різні соціальні фактори (політика, правосвідомість, мораль і т. ін.) [2, с. 37-38]. У процесі регулювання суспільних відносин норми права взаємодіють з іншими факторами. І знання про такі зв'язки

використовуються в ході тлумачення. Відтак тлумачення є не механічним відтворенням змісту, а творчим процесом конкретизації норми. Делегування цього процесу штучному інтелекту означало б трансформацію правотлумачення з ціннісно зумовленої діяльності у технічну операцію обробки тексту.

Особливо проблематичним є використання штучного інтелекту в інтерпретації широко вживаних оціночних понять у законодавстві, таких як «справедливість», «добросовісність», «значна шкода», «суспільний інтерес» тощо. Зміст таких категорій неможливо всебічно визначити за допомогою формальних критеріїв; він формується через зміни, що залежать від судової практики, теорії та соціального контексту. Алгоритм, навчений на наборі попередніх рішень, може реконструювати статистичну модель їх застосування, але не може оцінити, чи відповідає така практика сучасним уявленням про справедливість або принципу верховенства права. Більше того, використання систем машинного навчання може призвести до збереження помилок та упереджень, що містяться в минулій практиці, тим самим обмежуючи розвиток правової теорії [3, с. 9].

Герменевтичні межі застосування штучного інтелекту в тлумаченні правових норм полягають, перш за все, у розмежуванні допоміжних та автономних функцій алгоритмів. Штучний інтелект може бути ефективно використаний для пошуку відповідних норм, аналізу судової практики, виявлення конфліктів та узагальнення правових позицій. Однак остаточне тлумачення, яке передбачає оцінку цілей правового регулювання, балансування принципів та прийняття рішення в конкретній справі, має залишатися за людиною як носієм правосвідомості та відповідальності. В іншому випадку центр правотворчої та правозастосовчої діяльності зміщується з суб'єкта на алгоритм, що ставить під сумнів легітимність прийнятих рішень.

Таким чином, штучний інтелект не здатний до праворозуміння в повному розумінні цього поняття, оскільки він позбавлений здатності до ціннісного осмислення, моральної оцінки. Його функціонування базується на формалізованих моделях, тоді як право є динамічною системою, що поєднує нормативність із соціальною та етичною складовою. Тому використання штучного інтелекту в галузі юридичного

тлумачення має бути обмежене допоміжною роллю, а його використання має супроводжуватися процесуальними гарантіями прозорості, можливістю перевірки алгоритмічних висновків та збереженням вирішальної ролі особи у прийнятті остаточного рішення.

Список використаних джерел:

1. Проблеми тлумачення правових норм. *Посібник* / автор-упорядник О. М. Балинська. Львів : Львівський державний університет внутрішніх справ. 2021. 392 с.

2. Сердюк І. А. Методологічний аналіз інтерпретацій поняття «тлумачення норм права». *Науковий вісник ДДУВС*. 2014. № 3. С. 35–43.

3. Кобко-Одарій В.С. Роль штучного інтелекту в судовій інтерпретації права. *Київський часопис права*. 2023. № 3. С. 7-13.

Савайда О.І.
старший науковий співробітник
науково-дослідної лабораторії
вивчення проблем протидії торгівлі людьми
навчально-наукового інституту з підготовки
фахівців для підрозділів кримінальної поліції,
кандидат юридичних наук, доцент
(Львівський державний університет внутрішніх справ)

ЦИФРОВА СОЦІАЛІЗАЦІЯ МОЛОДІ ЯК ЧИННИК РИЗИКУ ПОТРАПЛЯННЯ У СИТУАЦІЇ ТОРГІВЛІ ЛЮДЬМИ В УМОВАХ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ

Здійснюючи правовий аналіз цифрової соціалізації молоді як чинника підвищеної вразливості до торгівлі людьми в умовах активного використання штучного інтелекту (ШІ) у цифровому середовищі ми розглядаємо роль алгоритмів соціальних мереж, автоматизованих систем комунікації та цифрових платформ у процесах вербування, маніпулювання та експлуатації як форм, які використовуються під час вчинення такого ганебного явища як торгівля людьми. Особливу увагу ми б хотіли приділити правовим механізмам запобігання торгівлі людьми, захисту прав потерпілих та використанню інструментів ШІ у правовому полі.

Стрімкий розвиток цифрових технологій та впровадження інструментів штучного інтелекту в різні сфери суспільного життя зумовили трансформацію соціальних і правових відносин. Українська молодь як найбільш активний суб'єкт цифрової соціалізації перебуває у зоні підвищеного ризику порушення прав людини, зокрема у контексті торгівлі людьми та особливо зараз в сучасних військових реаліях. У сучасних умовах інтернет, соціальні мережі та платформи з елементами ШІ дедалі частіше використовуються як засіб вербування, контролю та експлуатації осіб, що є основними формами торгівлі людьми.

Для правової науки актуальним є питання співвідношення цифрової соціалізації, технологій штучного інтелекту та ефективності правових механізмів протидії торгівлі людьми. Це

особливо важливо в умовах війни, масового переміщення та міграції українського населення та зростання кількості кіберзлочинів, що мають транснаціональний характер.

Цифрова соціалізація молоді відбувається в межах правового поля, яке охоплює норми міжнародного, європейського та національного права. Водночас швидкість технологічного розвитку, зокрема застосування ШІ, значно випереджає темпи нормативного врегулювання. Алгоритми рекомендацій соціальних мереж, чат-боти та автоматизовані сервіси створюють правові ризики, пов'язані з непрозорістю обробки персональних даних, маніпуляцією свідомістю та формуванням ілюзії безпечної комунікації.

З позиції права цифрове середовище має розглядатися як простір потенційного порушення фундаментальних прав людини - права на свободу, гідність, недоторканність приватного життя та захист персональних даних. Молоді люди часто не усвідомлюють правових наслідків передачі особистої інформації, що створює підґрунтя для злочинної діяльності, пов'язаної з торгівлею людьми. Штучний інтелект може виступати як інструмент та об'єкт правового впливу у сфері торгівлі людьми

У контексті торгівлі людьми штучний інтелект може виконувати подвійну роль. З одного боку, злочинні угруповання використовують інструменти ШІ для масового пошуку потенційних жертв, аналізу поведінки користувачів, створення фейкових профілів та персоналізованих повідомлень з метою вербування. Такі дії ускладнюють ідентифікацію злочинців та потребують удосконалення кримінально-правових і кримінально-процесуальних механізмів реагування.

З іншого боку, ШІ активно впроваджується у правову практику як засіб протидії торгівлі людьми. Йдеться про автоматизований аналіз великих масивів даних, виявлення підозрілих онлайн-активностей, цифрову ідентифікацію ризикових оголошень та підтримку розслідувань. Водночас використання таких технологій має відповідати принципам законності, пропорційності та поваги до прав людини.

В розгляді данної проблематики потрібно звернути увагу на правові чинники вразливості молоді в цифровому просторі. До

ключових правових чинників, що підвищують ризик потрапляння молоді у ситуації торгівлі людьми, належать:

- недостатня правова обізнаність щодо форм та способів торгівлі людьми в онлайн-середовищі;
- прогалини у правовому регулюванні діяльності цифрових платформ і використання алгоритмів ШІ;
- складність доказування злочинів, вчинених із використанням інформаційно-комунікаційних технологій;
- транснаціональний характер онлайн-вербування, що ускладнює юрисдикційні питання та міжнародну співпрацю.

Безперечно, що зазначені чинники потребують комплексного правового реагування, зокрема гармонізації національного законодавства з міжнародними стандартами.

З огляду на це напрями вдосконалення правової протидії та виклики цифрової соціалізації та розвитку ШІ доцільно зосередитися на таких аспектах:

- удосконалення кримінального законодавства щодо відповідальності за торгівлю людьми з використанням цифрових технологій та ШІ;
- запровадження чітких стандартів відповідальності цифрових платформ за контент і алгоритмічні рішення;
- використання інструментів ШІ у правоохоронній діяльності з дотриманням правових гарантій;
- посилення правопросвітницької роботи серед молоді щодо цифрових прав і безпеки;
- розвиток міжнародної співпраці у сфері протидії торгівлі людьми в кіберпросторі.

Висновки. Цифрова соціалізація молоді в умовах впровадження штучного інтелекту формує нові правові виклики у сфері захисту прав людини. Торгівля людьми набуває технологічно ускладнених форм, що потребує адекватної правової відповіді. Ефективне використання потенціалу ШІ у правовій практиці можливе лише за умови належного нормативного регулювання, дотримання принципів верховенства права та пріоритету прав і свобод людини.

Список використаних джерел:

1. United Nations Office on Drugs and Crime. Global Report on Trafficking in Persons. Vienna, 2022.

https://www.unodc.org/documents/data-and-analysis/glotip/2022/GLOTiP_2022_web.pdf

2. International Organization for Migration. Counter-Trafficking Data Collaborative: Global Report. Geneva, 2023. https://ukraine.iom.int/uk/news/informatsiyna-kampaniya-mom-prolyvaye-svitlo-na-nebezpeky-torhivli-lyudmy

3. Council of Europe. Convention on Action against Trafficking in Human Beings. Warsaw, 2005. P. 19.

4. Левченко К. Б. Конвенція Ради Європи про заходи щодо протидії торгівлі людьми та проблемні питання вдосконалення українського законодавства / К. Б. Левченко, А. Є. Санченко // Форум права. 2011. № 4. С. 451-456.

5. Шумило М. О. Штучний інтелект у праві: виклики та перспективи // Право України. 2022. №4. С. 45–53.

Савчин Г.Я.
заступник начальника
відділу організації наукової діяльності,
кандидат юридичних наук
(Львівський державний університет внутрішніх справ)
Волкова С.М.
науковий співробітник
відділення організації наукової роботи
відділу організації наукової діяльності
(Львівський державний університет внутрішніх справ)

ІМПЛЕМЕНТАЦІЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В СТРАТЕГІЯХ ІНФОРМАЦІЙНОЇ ВІЙНИ РФ ПРОТИ УКРАЇНИ

Інформаційний вимір сучасних воєнних конфліктів перетворився на стратегічний простір протиборства, у якому технологічна перевага визначає ефективність впливу не меншою мірою, ніж військова сила. У контексті повномасштабної агресії росії проти України, інформаційна складова стала системним елементом гібридної війни, яка спрямована на підрив внутрішньої стабільності, деморалізацію суспільства та дискредитацію державних інституцій. Розвиток технологій штучного інтелекту суттєво трансформував інструментарій інформаційно-психологічних операцій, надавши їм масштабності, автоматизованості та адаптивності.

Штучний інтелект дозволяє швидко генерувати, аналізувати та поширювати величезні обсяги інформації, що значно підсилює можливості інформаційної агресії [1, с. 144]. Алгоритми генерації природної мови здатні створювати аналітичні публікації та коментарі, що імітують стиль реальних журналістів або експертів. Це дозволяє формувати псевдодостовірний інформаційний фон, який важко відрізнити від легітимного медіаконтенту. Автоматизація процесів створення та поширення дезінформації сприяє безперервності інформаційного тиску та ускладнює своєчасне виявлення маніпулятивних кампаній.

Окремою проблемою виступають обмежені можливості правового регулювання у сфері протидії дезінформації. Хоча українське законодавство містить окремі положення, які можуть бути використані для реагування на поширення фейкових новин, нормативна база залишається фрагментарною й не повністю адаптованою до реалій сучасного інформаційного середовища [2, с. 357].

Важливим механізмом є використання алгоритмічно керованих бот-мереж у соціальних медіа. Окрему загрозу становить вплив глобальних цифрових платформ, через які реалізується більшість інформаційних атак. Багато пропагандистських наративів поширюється через такі ресурси, як Facebook, YouTube, Telegram, TikTok, які перебувають поза межами прямої дії українського законодавства. Це створює серйозні труднощі в питанні контролю, блокування або обмеження доступу до шкідливого контенту [2, с. 357].

Системи машинного навчання аналізують інформаційний простір у режимі реального часу, визначають тренди та найбільш резонансні теми, після чого ініціюють масове поширення відповідних наративів. Така діяльність створює ілюзію суспільної підтримки певних позицій, підсилює поляризацію та формує викривлене сприйняття громадської думки. Координація бот-акаунтів дозволяє впливати на алгоритми соціальних платформ, підвищуючи видимість пропагандистського контенту та витісняючи альтернативні джерела інформації. Застосування штучного інтелекту у поєднанні з аналізом великих масивів даних відкриває можливості для точкового інформаційного впливу. Алгоритми здійснюють сегментацію аудиторій за соціально-демографічними та поведінковими характеристиками, прогнозують реакції на різні типи повідомлень і формують персоналізовані інформаційні продукти. Такий підхід підвищує ефективність пропаганди, оскільки повідомлення апелюють до вже наявних переконань, страхів або соціальних запитів окремих груп населення. Персоналізація стає інструментом глибшого психологічного впливу, що сприяє закріпленню потрібних наративів.

Особливу небезпеку становлять технології синтетичного аудіо- та відеоконтенту. Можливість створення deepfake-

матеріалів дозволяє імітувати виступи публічних осіб, фальсифікувати заяви та поширювати маніпулятивні відео, спрямовані на дискредитацію державного керівництва або військових структур. Умови високої інформаційної турбулентності підвищують ризик того, що подібні матеріали можуть бути сприйняті як автентичні, що підриває довіру до офіційних джерел та створює атмосферу невизначеності.

Штучний інтелект також використовується для виявлення соціально чутливих тем і підсилення конфліктогенності інформаційного простору. Аналіз онлайн-дискусій дозволяє визначати тригерні питання, навколо яких можливо посилити поляризацію та спровокувати внутрішні суперечності. У такий спосіб інформаційна агресія спрямовується не лише на зовнішню аудиторію, а й на внутрішню дестабілізацію українського суспільства.

Таким чином, штучний інтелект у сучасній інформаційній агресії виступає не просто допоміжним технологічним засобом, а системоутворюючим елементом цифрових операцій впливу. Його застосування забезпечує швидкість, масштабність та гнучкість дезінформаційних кампаній, підвищуючи їхню ефективність і складність протидії. В умовах триваючої війни питання розвитку механізмів виявлення штучно згенерованого контенту, підвищення медіаграмотності та зміцнення цифрової стійкості суспільства набувають стратегічного значення для забезпечення національної безпеки України.

Список використаних джерел:

1. Когут Ю.І. Штучний інтелект і безпека: практичний посібник. за ред. док-ра тех. наук, проф. А.С. Довгополого. Київ: Консалтингова компанія «СІДКОН»; ВД Дакор, 2024. 294 с

2. Петренко С., Ільченко Ю. Проблемні питання протидії російській інформаційній агресії. *Науковий вісник Ужгородського національного університету. Серія право. Вип. 90. Ч. 3.* Ужгород: ФОП Ященко, 2025. 460 с.

Сліпченко С.П.
курсант
(Харківський національний університет внутрішніх справ)
Краснобриж Б.О.
курсант
(Харківський національний університету внутрішніх справ)
Горбунова К.В.
доцент кафедри кримінального процесу
та організації досудового слідства ННІ № 1,
доктор філософії
(Харківський національний університет внутрішніх справ)

ПРОБЛЕМНІ ПИТАННЯ ЗБИРАННЯ ТА ПЕРЕВІРКИ ЦИФРОВИХ ДОКАЗІВ ЗАСОБАМИ ШТУЧНОГО ІНТЕЛЕКТУ В МЕЖАХ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ

Трансформація парадигми сучасного досудового розслідування зумовлює зміщення акцентів від традиційних документальних джерел до «цифрових слідів» як об'єктів доказування у кримінальному провадженні. Зростання обсягів релевантної інформації, що акумулюється на електронних носіях (зокрема у хмарних сховищах та на серверному обладнанні), вимірюється терабайтами, що робить мануальну верифікацію та огляд вмісту технічних пристроїв детерміновано неефективними. Такий стан речей призводить не лише до затягування строків досудового розслідування, але й створює ризики порушення засади розумності строків [1, ст. 28 КПК України]. Штучний інтелект (ШІ) у цьому контексті виступає не як заміна слідчого, а як інструмент оптимізації рутинних процесів [2, с. 12].

Застосування алгоритмів машинного навчання у кримінальному процесі можна розділити на кілька ключових кластерів: 1) аналіз великих масивів тексту (NLP): ШІ здатний миттєво класифікувати тисячі повідомлень у месенджерах, виокремлюючи лише ті, що містять ознаки злочинної діяльності (наприклад, жаргонізми наркоторговців або координати об'єктів при шпигунстві) [3, с. 45]; 2) біометрична ідентифікація та

комп'ютерний зір полягають у автоматичному порівнянні облич із камер відеоспостереження з базами даних МВС. Це дозволяє встановити маршрут пересування підозрюваного за лічені хвилини, що раніше займало тижні роботи оперативників; 3) нейромережі використовують для верифікації автентичності відеозаписів, виявляючи ознаки «діпфейків» або монтажу, що є критичним для забезпечення належності доказів [4, с. 88].

Які ж можуть виникнути проблеми зі штучним інтелектом під час вивчення законності інформації, отриманої від ШІ? Згідно зі ст. 84 КПК України, доказами є фактичні дані, отримані у передбаченому законом порядку. Виникає колізія: чи можна вважати «звіт ШІ» самостійним доказом? На сьогодні панівною є думка, що результати роботи алгоритмів мають бути оформлені у якості додатків до протоколів огляду, чи бути частиною висновку експерта-криміналіста [1, ст. 105 КПК України].

Важливим аспектом є забезпечення права на захист. Адвокат повинен мати можливість перевірити «неупередженість» алгоритму, щоб уникнути помилкових звинувачень через технічні збої або викривлені навчальні вибірки даних [5, с. 5].

Застосування ШІ під час досудового розслідування не повинно порушувати право на приватність. Автоматизований збір даних про особу без належного судового контролю створює ризик перетворення правосуддя на тотальне стеження. Необхідно дотримуватися принципу «Human-in-the-loop», де остаточне процесуальне рішення завжди приймає людина (слідчий або прокурор), а ШІ лише надає варіанти аналізу [6, с. 1310].

На нашу думку, перспективи імплементації ШІ у кримінально-процесуальну діяльність з тим, щоб в подальшому результати роботи ШІ не розбивалися об аргументи захисту в суді про «недопустимість доказів», необхідно внести доповнення до КПК України, а саме:

1. Доповнити ст. 99 КПК України поняттям «результати автоматизованого аналізу цифрових даних», що дозволить легалізувати звіти, сформовані ШІ, як різновид документів.

2. Закріплення на законодавчому рівні обов'язку сторони обвинувачення розкривати інформацію про програмне забезпечення, якщо його висновки покладені в основу підозри,

щоб захист мав можливість залучити спеціаліста для перевірки наявності помилок у коді [6, с. 1321].

3. Обов'язкова верифікація, здійснена за допомогою ШІ (наприклад, за біометрією), повинна обов'язково підтверджуватися протоколом пред'явлення для впізнання за участі людини або висновком судово-портретної експертизи [1, ст. 206 КПК України]

Отже, інтеграція ШІ в роботу правоохоронних органів України є неминучим кроком в умовах євроінтеграції. Проте, це вимагає чіткого законодавчого закріплення статусу «цифрового асистента» у КПК, визначення порядку сертифікації відповідного програмного забезпечення та створення механізму оскарження результатів алгоритмічного аналізу. ШІ не повинен замінювати слідчого, дізнавача, але має стати його «цифровим асистентом». Для легітимізації ШІ в Україні необхідно внести зміни до КПК, закріпивши статус «цифрового доказу, обробленого автоматизованими системами».

Список використаних джерел:

1. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17.

2. Барабаш О. О. Штучний інтелект у правовій практиці: межі та можливості. Матеріали міжнародного круглого столу (Львів, 13 березня 2026 р.). Львів: ЛДУВС, 2026. С. 10–15.

3. Ковальський В. Цифровізація досудового розслідування: від теорії до автоматизації. Юридичний часопис. 2024. № 2. С. 40–52.

4. Смирнов О. Проблеми використання штучного інтелекту при зборі цифрових доказів. Право та безпека. 2024. Т. 92, № 1. С. 85–94.

5. Європейська етична хартія про використання штучного інтелекту в судових системах та їхньому середовищі: прийнята на 31-му пленарному засіданні CEPEJ (Страсбург, 3-4 грудня 2018 р.). 5 с.

6. Surden H. Artificial Intelligence and Law: An Overview. Georgia State University Law Review. 2019. Vol. 35, No. 4. P. 1305–1337.

Снітніков Д.Г.
викладач кафедри кримінально-правових дисциплін
(Одеський державний університет внутрішніх справ).
Науковий керівник – **Резніченко Г.С.**
доцент кафедри кримінально-правових дисциплін,
кандидат юридичних наук, доцент
(Одеський державний університет внутрішніх справ)

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЛЕКТУ В ЮРИДИЧНІЙ ПРАКТИЦІ

Snitnikov D.
Lecturer, Department of Criminal Law Disciplines
(Odessa State University of Internal Affairs).
Head of Research – **Reznichenko H.**
Candidate of Law, Associate Professor,
Associate Professor of the Department
of Criminal Law Disciplines
(Odessa State University of Internal Affairs)

USE OF ARTIFICIAL INTELLIGENCE IN LEGAL PRACTICE

На сучасному етапі розвитку інформаційного суспільства впровадження систем штучного інтелекту набуває стратегічного значення як у приватному секторі, так і у професійній правничій діяльності. Інтеграція алгоритмів штучного інтелекту дозволяє суттєво оптимізувати робочі процеси шляхом автоматизації аналізу значних масивів неструктурованих даних, що забезпечує формування релевантних та лаконічних висновків відповідно до встановлених параметрів.

Функціональний потенціал штучного інтелекту дозволяє здійснювати прецизійний аналіз багатоаспектних юридичних питань, розв’язання яких за традиційними методиками потребує значного часового ресурсу. Автоматизація когнітивних операцій забезпечує релевантний пошук відповідей на запити підвищеної складності, істотно випереджаючи людський чинник за

показниками оперативності та глибини моніторингу інформаційного поля.

Комплексний аналіз потенційних переваг та ризиків, пов'язаних із впровадженням систем штучного інтелекту в юриспруденцію, вимагає передусім чіткої концептуалізації цього феномена. У зв'язку з цим доцільно звернутися до дефініції, запропонованої О. А. Барановим, який у своєму дослідженні зазначає наступне: «штучний інтелект – це інтелект, що має штучне походження та імітує (моделює) певну сукупність когнітивних функцій еквівалентних відповідним когнітивним функціям людини.» [1, с. 45].

Серед ключових переваг застосування систем штучного інтелекту виокремлюється принцип процесуальної економії та оптимізація інтелектуальної праці. Технологічна спроможність штучного інтелекту щодо аналізу даних із колосальних інформаційних обсягів дозволяє суб'єкту правозастосування зосередитися на стратегічних аспектах справи, делегуючи машині ресурсозатратну аналітичну роботу.

Очевидна практична користь від інтеграції систем штучного інтелекту не повинна відволікати увагу від суттєвих правових та етичних викликів, притаманних даній технології. Висока функціональність штучного інтелекту часто стає аргументом на користь його імплементації, проте вимагає ретельної ідентифікації та мінімізації прихованих загроз, які мають системний характер.

Першочерговим ризиком є генерування системами штучного інтелекту недостовірної, фактологічно помилкової або релевантної лише для минулих періодів інформації (феномен «галюцинацій» штучного інтелекту). Ситуація ускладнюється формуванням у суб'єкта правозастосування надмірної когнітивної довіри до алгоритмів, що призводить до зниження критичного сприйняття результатів. Відсутність належної верифікації отриманих даних загрожує використанням хибних висновків, що у юридичній практиці тягне за собою суттєві правові наслідки, феномен так званих "галюцинацій" ШІ – випадків, коли система генерує неправдиву, неточну, спотворену або вигадану інформацію, подаючи її як об'єктивний факт [2, с. 111].

Другим суттєвим викликом, актуальним як для приватної, так і для професійної правничої сфери, є потенційна регресія

когнітивних спроможностей суб'єкта. Замість традиційного опрацювання значних масивів інформації, що стимулює розвиток аналітичного мислення та нейропластичність, надмірна експлуатація штучного інтелекту призводить до формування інтелектуальної пасивності. Відмова від самостійного критичного аналізу на користь готових алгоритмічних рішень спричиняє поступову деградацію навичок системного мислення та здатності до глибокої професійної рефлексії.

Окремої уваги заслуговує аспект кібербезпеки та ризик компрометації конфіденційної інформації, що охороняється законом. Проблема полягає у можливості несанкціонованого витоку даних під час формування запитів до зовнішніх систем штучного інтелекту. Суб'єкт правозастосування, надаючи пріоритет оперативності вирішення завдання перед стандартами захисту інформації, може не усвідомлювати, що передача персональних даних або відомостей, які становлять професійну таємницю, у хмарне середовище алгоритму створює неконтрольовані канали розголошення.

Особливої уваги заслуговує стрімка еволюція технологій штучного інтелекту, що зумовлює виникнення нових видів кіберзагроз. Швидкий розвиток генеративних моделей дозволяє створювати високореалістичний синтетичний контент (дипфейки), який ще кілька років тому був недоступний широкому загалу. Використання таких інструментів для несанкціонованої генерації фото- та відеоматеріалів із зображенням осіб створює підгрунтя для вчинення правопорушень, пов'язаних із шантажем, вимаганням, а також цілеспрямованою дискредитацією та порушенням недоторканності приватного життя.

Перспектива масового використання генеративних систем штучного інтелекту створює суттєві виклики для інституту доказування в судовому процесі. Ризик фальсифікації доказової бази через створення високореалістичних синтетичних фото- та відеоматеріалів актуалізує проблему верифікації доказів як з боку обвинувачення, так і з боку захисту. Можливість генерування штучних підтверджень певних юридичних фактів ставить під сумнів презумпцію достовірності цифрових матеріалів та потребує розробки нових методик судово-технічної експертизи для виявлення ознак алгоритмічного втручання.

Окремим викликом для правоохоронної системи є стрімке вдосконалення технологій клонування голосу (voice cloning). Здатність алгоритмів штучного інтелекту до високоточної імітації біометричних характеристик людського мовлення створює підґрунтя для появи принципово нових шахрайських схем. Використання синтезованого голосу в межах методів соціальної інженерії дозволяє зловмисникам здійснювати маніпулятивний вплив на потерпілих, що суттєво ускладнює ідентифікацію злочинців та потребує розробки нових протоколів аудіофоноскопічної експертизи.

Щоб подолати ці виклики, необхідно розробити чіткі правила та регуляторні механізми для використання штучного інтелекту у правовій сфері, які враховуватимуть особливості роботи з технологіями та забезпечуватимуть баланс між їхніми перевагами й ризиками. Розробка міжнародних стандартів і залучення фахівців до адаптації законодавства до нових умов є ключовими кроками для інтеграції штучного інтелекту у правову систему [3, с. 48].

Резюмуючи вищевикладене, слід констатувати, що імплементація штучного інтелекту як у професійній правничій діяльності, так і в приватному секторі, потребує впровадження принципів відповідального використання та суворої нормативної регламентації. Це необхідно для нівелювання ризиків фактологічних помилок та запобігання регресії когнітивних навичок суб'єкта. Паралельно з цим, критично важливим є розробка та впровадження новітніх криміналістичних методик верифікації доказів, здатних ефективно ідентифікувати ознаки алгоритмічної фальсифікації, що дозволить забезпечити дотримання принципу справедливості та унеможливить маніпулювання процесуальними даними.

Список використаних джерел:

1. Баранов О. А. Визначення терміну «штучний інтелект». *Інформація і право*. 2023. №. 1 (44). С. 32-49.

2. Махно Є. П., Руденко Є. Г., Судніков Є. О., Тищенко М. Г. Галюцинації штучного інтелекту у сфері освіти та науки: причини, наслідки та методи мінімізації. *Повітряна міць України*.

2026. № 1 (8). С. 111-126. URL: https://doi.org/10.33099/2786-7714-2025-1-8-111-126.

3. Томашівський М. О., Томашівський О. З. Використання штучного інтелекту в юридичній практиці: перспективи та виклики. *Недоліки та перспективи вдосконалення законодавства України*: матеріали наук.-практ. семінару, присвяч. Міжнар. дню прав людини (м. Львів, 10 груд. 2024 р.). Львів: Львівський інститут ПрАТ «ВНЗ «МАУП», 2024. С. 44-50.

Стратілат Д.П.
науковий співробітник відділу
дослідницького ядерного реактора,
кандидат природничих наук
(Інститут ядерних досліджень НАН України)

ЗАСТОСУВАННЯ СИСТЕМ РАДІАЦІЙНОЇ РОЗВІДКИ ТА МОНІТОРИНГУ ДЛЯ КОНТРОЛЮ РАДІАЦІЙНОЇ БЕЗПЕКИ

Автоматичні системи радіаційного моніторингу та комплекси розвідки є інструментом виявлення підвищених показників іонізуючого випромінювання для подальшого реагування на ядерні та радіаційні загрози. До складу таких систем входять стаціонарні та мобільні комплекси радіаційного контролю, автоматизовані пости моніторингу, повітряно-фільтрувальні установки для відбору аерозольних проб, а також гамма-спектрометри для ідентифікації радіонуклідів.

Стаціонарні системи забезпечують безперервний контроль потужності дози іонізуючого випромінювання на визначених територіях, об’єктах критичної інфраструктури та об’єктах підвищеної небезпеки [1]. Дані вимірювань передаються для обробки та аналізу і фіксації змін радіаційного фону. Мобільні системи радіаційної розвідки використовуються для оперативного обстеження територій, пошуку та локалізації джерел випромінювання, а також проведення детальних вимірювань у разі підозри на радіаційний інцидент.

Повітряно-фільтрувальні установки забезпечують регулярний відбір атмосферних аерозолів з подальшим спектрометричним аналізом, що дозволяє виявляти навіть низькі концентрації радіонуклідів у повітрі. Гамма-спектрометричні комплекси застосовуються для визначення ізотопного складу радіоактивного забруднення, що дозволяє встановити джерело походження радіації та характер події.

Актуальним напрямком є створення єдиної інтегрованої онлайн-системи радіаційного моніторингу на території всієї України. Така система повинна об’єднувати мережу стаціонарних постів, мобільні комплекси радіаційної розвідки, повітряні

фільтрувальні станції та спектрометричні пункти контролю в єдину цифрову інфраструктуру з передачею даних у режимі реального часу.

Інтерактивна платформа моніторингу з використанням цифрових карт, автоматизованого аналізу даних та системи оперативних сповіщень дозволить швидко виявляти відхилення радіаційного фону, локалізувати потенційні джерела випромінювання та забезпечувати оперативне реагування відповідних служб. Особливої актуальності така система набуває в умовах зростання ризиків техногенних інцидентів, втрати радіоактивних джерел та можливого незаконного обігу радіоактивних матеріалів.

Створення національної онлайн-системи радіаційного моніторингу є важливим не лише для України, але й для всієї Європи. Територія України має значну кількість ядерних та радіаційно небезпечних об'єктів, а також є частиною спільного європейського екологічного простору. Будь-які радіаційні інциденти можуть мати транскордонний характер та впливати на сусідні країни. Інтегрована система моніторингу забезпечує прозорість радіаційної обстановки, швидке інформування та підвищує рівень колективної радіаційної безпеки в Європі [2].

Список використаних джерел:

1. Polyakova Iryna Oleksandrivna, Stratilat Dmytro Petrovych, Maidannyk Tetyana Petrivna, Budnyk Oksana Petrivna. Interpretation of radiation-ecological indicators obtained by using of the "NUVIA" integrated automatic system for environmental radiation monitoring and its correlation with data provided by the Ukrainian hydrometeorological central audience service of ukraine for emergency situations. Seventh International Conference on Nuclear Decommissioning and Environment Recovery INUDECO 22. P 79.

2. Radioactivity Environmental Monitoring URL: https://remap.jrc.ec.europa.eu/Advanced.aspx

Стукаліна О.В.
юрист,
доктор філософії
(м. Одеса)

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ ЗАПОБІГАННЯ СЕКСУАЛЬНІЙ ЕКСПЛУАТАЦІЇ ДІТЕЙ У ЦИФРОВОМУ СЕРЕДОВИЩІ

Стрімка цифровізація суспільства, розширення онлайн-комунікацій та глобалізація інформаційного простору зумовили трансформацію злочинності й появу її нових форм. Однією з найбільш небезпечних серед них є дитяча сексуальна експлуатація в цифровому середовищі. Використання соціальних мереж, месенджерів, ігрових платформ та інших онлайн-сервісів створює сприятливі умови для поширення матеріалів сексуального насильства щодо дітей, встановлення злочинного контакту (грумінгу) та функціонування транснаціональних кримінальних мереж.

Актуальність проблеми підтверджується і даними офіційної кримінальної статистики. В Україні простежується зростання кількості кримінальних правопорушень, передбачених ст. 301-1 Кримінальний кодекс України. Так, у 2022 році було зареєстровано 1095 таких правопорушень, у 2023 році – 1621, у 2024 році – 1809. Хоча у 2025 році зафіксовано 1127 випадків, загальна динаміка попередніх років свідчить про істотну активізацію незаконного обігу матеріалів сексуального характеру за участю дітей саме в цифровому середовищі. Кількість повідомлень про підозру є співмірною із числом облікованих кримінальних правопорушень (2022 р. – 1012; 2023 р. – 1523; 2024 р. – 1703; 2025 р. – 957), що вказує на належний рівень процесуального реагування, однак не зменшує масштабів самої проблеми [1;2;3;4].

Водночас традиційні механізми правоохоронної діяльності виявляються обмеженими через значний обсяг цифрового контенту, анонімність користувачів, швидкість поширення інформації та високий рівень технологічної адаптивності

правопорушників. За таких умов ефективна протидія дитячій сексуальній експлуатації потребує впровадження інноваційних інструментів аналізу та моніторингу інформаційного простору.

У цьому контексті особливої ваги набуває застосування технологій штучного інтелекту, здатних здійснювати автоматизований аналіз великих масивів даних, розпізнавання зображень і текстових повідомлень, виявлення підозрілих поведінкових моделей та прогнозування ризиків. Саме інтеграція алгоритмічних систем у діяльність правоохоронних органів може суттєво підвищити ефективність виявлення та запобігання таким кримінально протиправним діянням у цифровому середовищі.

Сучасні системи штучного інтелекту відкривають принципово нові можливості для виявлення та запобігання дитячій сексуальній експлуатації в цифровому середовищі. Насамперед йдеться про застосування алгоритмів машинного навчання та нейронних мереж для автоматизованого аналізу великих масивів даних, що циркулюють у мережі Інтернет.

Ключовим напрямом є автоматичне виявлення матеріалів сексуального насильства щодо дітей (CSAM). Алгоритмічні системи здатні здійснювати розпізнавання зображень і відеофайлів, ідентифікувати заборонений контент шляхом використання технологій цифрового хешування, а також виявляти модифіковані або частково змінені файли [5]. Такий підхід дозволяє значно скоротити час реагування та мінімізувати необхідність безпосереднього перегляду травматичного контенту працівниками правоохоронних органів.

Другим важливим напрямом є виявлення онлайн-грумінгу. Системи обробки природної мови (NLP) аналізують текстові повідомлення у соціальних мережах і месенджерах, виявляючи характерні мовні патерни, маніпулятивні стратегії встановлення довіри та інші поведінкові індикатори, притаманні потенційним правопорушникам. Завдяки цьому можливо здійснювати ранню ідентифікацію ризикових комунікацій ще до переходу злочину у фізичну фазу [6].

Крім того, штучний інтелект застосовується для аналізу соціальних зв’язків і побудови моделей кримінальних мереж. Алгоритмічні інструменти дозволяють встановлювати взаємозв’язки між обліковими записами, IP-адресами, платіжними

транзакціями та іншими цифровими слідами, що є особливо важливим у випадках транснаціональної злочинної діяльності. Подібні підходи використовуються у практиці міжнародних правоохоронних структур, зокрема Європол та Інтерпол [7, с. 122].

На сьогодні в Україні відсутнє комплексне нормативно-правове регулювання застосування систем штучного інтелекту в діяльності правоохоронних органів, зокрема у сфері протидії торгівлі людьми та дитячій сексуальній експлуатації. Це створює правову невизначеність щодо статусу результатів роботи алгоритмів, порядку їх використання та допустимості як доказів у кримінальному провадженні [7, с. 120]. Як вірно зазначає А. В. Боровик, необхідно внести зміни до Кримінальний кодекс України та Кримінальний процесуальний кодекс України, оскільки без надання результатам роботи штучного інтелекту офіційного статусу доказу вони залишатимуться лише аналітичною інформацією без належної доказової сили [9, с. 39]. Тобто, подальший розвиток правового регулювання у цій сфері має передбачати комплексне оновлення кримінального та кримінального процесуального законодавства, запровадження стандартів допустимості цифрових доказів, а також встановлення прозорих механізмів контролю за використанням технологій штучного інтелекту в правоохоронній діяльності.

Отже, проблема дитячої сексуальної експлуатації в цифровому середовищі сьогодні стає дедалі гострішою через стрімкий розвиток онлайн-комунікацій і глобалізацію інформаційного простору. Статистика в Україні демонструє зростання кількості таких правопорушень, що змушує правоохоронні органи шукати більш ефективні та технологічні підходи до їх виявлення й розслідування. У цьому контексті штучний інтелект відкриває нові можливості – від автоматичного виявлення забороненого контенту та раннього розпізнавання онлайн-грумінгу до аналізу зв’язків між учасниками кримінальних мереж. Водночас важливо, щоб упровадження цих технологій супроводжувалося належним правовим регулюванням і дотриманням стандартів захисту прав людини, адже саме поєднання інновацій і правових гарантій може забезпечити реальну ефективність протидії таким кримінально протиправним діянням.

Список використаних джерел:

1. Єдиний звіт про кримінальні правопорушення за січень-грудень 2022 року. Офіс Генерального прокурора України. URL: https://www.gp.gov.ua (дата звернення: 24.02.2026).

2. Єдиний звіт про кримінальні правопорушення за січень-грудень 2023 року. Офіс Генерального прокурора України. URL: https://www.gp.gov.ua (дата звернення: 25.02.2026).

3. Єдиний звіт про кримінальні правопорушення за січень-грудень 2024 року. Офіс Генерального прокурора України. URL: https://www.gp.gov.ua (дата звернення: 25.02.2026).

4. Єдиний звіт про кримінальні правопорушення за січень-грудень 2025 року. Офіс Генерального прокурора України. URL: https://www.gp.gov.ua (дата звернення: 26.02.2026).

5. Child Sexual Abuse Material. URL: https://www.justice.gov/d9/2023-06/child_sexual_abuse_material_2.pdf (дата звернення: 27.02.2026).

6. Deep learning-based natural language processing model and optical character recognition for detection of online grooming on social networking services. *Computer Modeling in Engineering & Sciences*, 143 (2). 2025. URL: https://www.sciencedirect.com/org/science/article/pii/S1526149225001365 (дата звернення: 27.02.2026).

7. Зачек О.І. Застосування штучного інтелекту для протидії злочинам у сфері сексуальної експлуатації дітей у мережі Інтернет. *Науковий вісник Львівського державного університету внутрішніх справ.* Випуск 3, 2025. С. 119-125.

8. Боровик А. В. Щодо практики застосування штучного інтелекту при розслідуванні кримінальних правопорушень. Штучний інтелект у правовій практиці: межі та можливості: збірник тез круглого столу (14 березня 2025 року). Львів: ЛьвДУВС, 2025. С. 38-39.

Тарасенко О.І.
аспірант кафедри цивільно-правових дисциплін
навчально-наукового інституту
права та правоохоронної діяльності
(Львівський державний університет внутрішніх справ)

МАШИННЕ НАВЧАННЯ У ЦИВІЛЬНОМУ СУДОЧИНСТВІ: ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ТА РИЗИКИ АЛГОРИТМІЧНОЇ УЧАСТІ

Цифрова трансформація є одним із найактуальніших та найбільш динамічних процесів сучасності. В умовах стрімкого розвитку технологій штучного інтелекту, значних інвестицій у цю сферу та глобального перегляду традиційних моделей управління й взаємодії між інституціями, питання впровадження цифрових рішень набуває більш особливої ваги. Юриспруденція не є винятком. Навпаки, саме вона потребує особливо виваженого, відповідального та нормативно обґрунтованого підходу до інновацій.

Цифрова трансформація – це процес системного впровадження цифрових технологій у діяльність інституцій з метою підвищення ефективності, доступності, швидкості та якості виконання їх функцій. У цивільному процесі цифрова трансформація має особливе значення. Цивільне судочинство характеризується великою кількістю спорів, документообігом, однотипних категорій справ та потребою оперативного вирішення приватноправових конфліктів.

Одним із інструментів такої трансформації є машинне навчання. Під машинним навчанням ми розуміємо саме математичну модель, створену фахівцями на основі навчальних вибірок, алгоритмів та методів аналізу даних, яка дозволяє системі виявляти закономірності у великих масивах інформації та формувати прогнозовані висновки. Йдеться не про самостійне «мислення» машини, а про обробку статистичних даних за визначеними правилами. Саме за допомогою цього методу побудована більшість сучасних технологій, в яких застосовується штучний інтелект. Зокрема, слід розуміти та зазначити, що

штучний інтелект є поняттям більш ширшим, а машинне навчання в свою чергу має більш вужче значення.

У контексті цивільного судочинства це означає можливість аналізу доволі значної кількості судових рішень, систематизації правових позицій, автоматизованого формування проектів процесуальних документів, швидкого пошуку релевантної практики. Такий підхід здатен суттєво зменшити витрати часу, адміністративного навантаження на апарат суду та спростити взаємодію між судом, громадянами і юридичними особами. Крім того, алгоритмічні системи можуть допомогти сторонам попередньо оцінити перспективи спору, визначити ризики та обрати правильну та якісну стратегію захисту.

Наразі під штучним інтелектом в цілому фахівцями розуміється моделювання процесів людського інтелекту за допомогою машин, комп'ютерних систем, яке включає в себе навчання (отримання інформації та правила її використання), міркування (використання правил для досягнення приблизних або певних висновків) і самокорекцію [1, с. 234].

Такий підхід підкреслює ключову особливість штучного інтелекту - моделювання, а не відтворення людської свідомості. Йдеться про інструмент, який оперує даними та алгоритмами, але не має волі, відповідальності чи правового статусу.

Світова практика демонструє, що інтеграція машинного навчання у сферу правосуддя вже не є теоретичною моделлю, а поступово набуває прикладного значення. У низці держав впроваджуються системи прогнозування судової практики (*predictive justice*), які аналізують великі масиви рішень та дозволяють оцінити ймовірність певного результату спору. Зокрема окремі країни Європейського Союзу розвивають цифрові платформи онлайн-врегулювання спорів (*online dispute resolution*), де алгоритмічні модулі допомагають сторонам оцінити перспективи справи до звернення до суду. Це сприяє зменшенню навантаження на судову систему та розвитку альтернативних механізмів вирішення конфліктів.

Важливо, що такі ініціативи супроводжуються нормативними обмеженнями. Відповідно до AI Act, системи штучного інтелекту, які застосовуються у судочинстві, віднесені до категорії високого ризику. Це означає обов’язковість людського

нагляду, вимог до якості даних, прозорості алгоритмічних рішень та можливості їх перевірки [5].

Як зазначають дослідники, сучасні великі мовні моделі (large language models, далі – LLM) «самонавчаються, але вхідні дані настільки різноманітні і у більшості суперечливі, їх впровадження у практичну діяльність здійснюється лише фрагментарно. Хоча світова практика свідчить про постійне удосконалення технічної складової. Не дивлячись на такий стрімкий розвиток багато дискусій викликали оціночні показники для вдосконалення юридичної моделі LLMs, оскільки дуже важливо забезпечити прозорість, підзвітність та етичності щодо міркування під час впровадження штучного інтелекту систему прийняття судових рішень» [4, с. 582-583].

Таким чином, міжнародний досвід демонструє поєднання технологічного розвитку з нормативними гарантіями. Для України інтеграція машинного навчання у цивільне судочинство може стати наступним етапом розвитку електронного суду.

Потенційні напрями застосування можуть включати: автоматизований аналіз судової практики для формування єдності правозастосування, інтелектуальний пошук релевантних рішень, структурування та попередній аналіз великого масиву доказів, а також формування проєктів процесуальних документів у типових категоріях справ.

Особливо актуальним це є в умовах підвищеного навантаження на судову систему. Алгоритмічні інструменти могли б виконувати допоміжну аналітичну функцію, не втручаючись у дискреційні повноваження судді. Водночас впровадження таких систем потребує розробки чітких процедур тестування, аудиту моделей та визначення відповідальних суб’єктів.

У наукових та практичних рекомендаціях щодо використання штучного інтелекту у діяльності судів наголошується, що повна відповідальність за використання будь-яких інструментів ШІ під час здійснення правосуддя покладається на суддю. Використання ШІ допускається винятково як допоміжного інструменту - здебільшого для організаційних завдань, підготовки навчальних матеріалів або узагальнення інформації, але не для правового аналізу або дослідження прецедентів [2].

Одним із найбільш дискусійних питань є так звана суб'єктивізація штучного інтелекту. Під цим не слід розуміти визнання алгоритму суб'єктом права або надання йому процесуального статусу. Слід погодитись з твердженням таких вчених як В. Г. Деркач, Є. Д. Прокопович-Ткаченко, Є. Г. Руденко, які зазначають про те, що «штучний інтелект у судовій системі має виконувати виключно допоміжну роль, не втручаючись у компетенції, що належать людині–зокрема судді. ШІ може виступати аналітичним інструментом, але не суб'єктом, який ухвалює рішення або тлумачить норми права. Це відповідає європейському підходу до правосуддя, де ШІ розглядається як сервісна технологія, що діє під повним контролем людини» [3, с. 463].

Машинне навчання не має волі, свідомості чи здатності нести юридичну відповідальність. Однак може виникнути ситуація, коли алгоритмічні висновки починають сприйматися як самостійне джерело рішення або як об'єктивний арбітр. Такий ефект посилюється довірою до статистичних показників та технологічної «нейтральності».

Небезпека полягає не у самому алгоритмі, а у можливому перенесенні частини внутрішнього переконання судді на машинну модель. Саме тому принцип людського контролю повинен залишатися базовою гарантією алгоритмічної інтеграції. Машинне навчання у цивільному судочинстві має потенціал стати інструментом підвищення ефективності, передбачуваності та процесуальної економії. Алгоритм має залишатися допоміжним механізмом, а суддя - єдиним суб'єктом прийняття рішення та носієм владних повноважень.

Відтак, інтеграція машинного навчання у цивільне судочинство є можливою та перспективною, проте потребує поєднання технологічної інноваційності з чітким нормативним регулюванням та усвідомленням меж алгоритмічної участі.

Список використаних джерел:

1. Бааджи Н. П. Новітні інструменти юридичної освіти в добу штучного інтелекту. *Правова держава*. 2023. С. 233-239.

2. Берназюк Я. О. Ера штучного інтелекту й роль верховних судів у цифровій трансформації правосуддя. *Юридична практика*. 2024. № 4 (792).

3. Деркач В. Г., Прокопович-Ткаченко Є. Д., Руденко Є. Г. Використання штучного інтелекту в судовому процесі України: правові, етичні та процесуальні аспекти. *Юридичний науковий електронний журнал*. 2023. С. 460–464.

4. Ковальчук А. Ю., Наконечна І. В. Виклики для національних судових систем, що пов'язані з формуванням єдиних судових стандартів залучення штучного інтелекту. *Юридичний науковий електронний журнал*. 2023. С. 574-585.

5. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union. 2024.

Тарасюк А.В.
співробітник,
доктор юридичних наук, професор
(Служба безпеки України)

ШТУЧНИЙ ІНТЕЛЕКТ У ДІЯЛЬНОСТІ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ: ПРАВОВІ МЕЖІ ЗАСТОСУВАННЯ ТА ВИКЛИКИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В УМОВАХ ВОЄННОГО СТАНУ

Критична загроза національному суверенітету, детермінована реаліями повномасштабної збройної агресії, змушує нас по-новому осмислювати систему безпекового сектору, де традиційні методи контррозвідки неминуче стикаються із потоками великих масивів даних. В умовах сьогодення, коли інформаційне середовище перетворилося на простір гібридної війни, Служба безпеки України (далі – СБУ) стала одним із основних елементів технологічної адаптації, де швидкість ідентифікації латентної загрози стає питанням виживання нації. Історично діяльність підрозділів ґрунтувалася на традиційних методах негласного отримання інформації, утім, тепер, коли об'єкти зацікавленості використовують багаторівневі цифрові засоби приховування активності, вбачається очевидним, що оперативний працівник без підтримки алгоритмічних систем певною мірою втрачає здатність до повноцінної візуалізації загроз. Більше того, ст. 24 Закону України «Про Службу безпеки України» від 25.03.1992 р. №2229-XII встановлений обов'язок щодо виявлення та припинення розвідувально-підривної діяльності [1], який, безсумнівно, залежить від технічної спроможності опрацьовувати значні масиви метаданих у реальному часі.

Очевидно, цифрова трансформація спецслужби – це стратегічна необхідність, що випливає безпосередньо з положень Стратегії національної безпеки України від 14.09.2020 р. №392/2020 [2]. Проте, запровадження штучного інтелекту (далі – ШІ) в оперативно-службову діяльність породжує певне онтологічне протиріччя між оперативною доцільністю та

основоположними правами людини, закріпленими в Конституції України [3]. Звертаючись до правової природи названого явища, слід вказати, що станом на сьогодні ми спостерігаємо формування нової юридичної реальності, де алгоритм стає безпосереднім учасником процесу забезпечення правопорядку.

Аналогічно до глобальних тенденцій, де провідні демократії світу вже розпочали процес нормативного регулювання використання цифрових технологій, Україна має вибудувати власну, суверенну модель імплементації інноваційних рішень. Відтак, окреслений дискурс вимагає від нас не тільки технічного аналізу можливостей нейромереж, а й глибокої наукової рефлексії щодо правових меж, за якими закінчується ефективність діяльності спецслужб і починається ризик для демократичних інститутів. У наведеному контексті розгляд ролі СБУ крізь призму ШІ є надто важливим кроком до створення інтелектуальної системи національної безпеки, здатної діяти на випередження в умовах тривалої гібридної війни.

Варто взяти до уваги і той аспект, що сьогодні СБУ є одним із основних суб'єктів забезпечення національної кібербезпеки (відповідно до ч. 2 ст. 8 Закону «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. №2163-VIII [4]). І, що не менш важливо, часом використання ШІ може бути доволі ефективним методом фільтрації ворожих ІПСО та виявлення прихованих осередків дестабілізації.

З точки зору оперативно-технічного забезпечення, впровадження ШІ дозволяє автоматизувати процес верифікації цифрових слідів під час проведення контррозвідувальних заходів у кіберпросторі, що безпосередньо мінімізує вплив людського фактору при ідентифікації об'єктів за непрямими ознаками. Втім, слід враховувати, що згідно зі ст. 8 Закону України «Про оперативно-розшукову діяльність» від 18.02.1992 №2135-XII [5], використання технічних засобів отримання інформації має бути чітко санкціоноване, а алгоритмічне профілювання станом натепер перебуває поза процесуальним регулюванням. Досить цікаво, що нейромережі можуть здійснювати кореляційний аналіз між закритими реєстрами та відкритими джерелами в режимі «real-time», що щонайменше утричі скорочує час на підготовку аналітичного висновку для прийняття рішення про заведення

справи оперативної перевірки. Проте, незважаючи на технологічну досконаліть, потрібно апелювати до того, що машинний алгоритм не здатний оцінити оперативну обстановку в сукупності її етичних та юридичних нюансів, а відтак роль людини-оператора залишається визначальною для верифікації критично важливих розвідувальних даних.

Звертаючись до практичного досвіду, слід зупинитися на позиції закордонних фахівців, зокрема експертів з контррозвідки Ізраїлю, які наголошують на пріоритетності автоматизованого аналізу для виявлення ознак підготовки терористичних актів [6]. Окреслений підхід є досить слушним у частині автоматизації ідентифікації аномальної активності, проте, враховуючи норми вітчизняного процесуального права, вважаю за необхідне наголосити: будь-який результат роботи ШІ в наших реаліях є *виключно орієнтуючою інформацією*. Так, на противагу абсолютній автоматизації прийняття рішень, більш обґрунтованою все ж видається модель, де система безпосередньо фіксує відхилення в поведінці об'єктів або в мережевому трафіку, а остаточну юридичну оцінку дає оперативний співробітник. Подібним чином, використання OSINT-технологій для моніторингу відкритих джерел дає змогу ідентифікувати координаторів вогню з ефективністю, що недоступна при ручному пошуку.

Втім, практична імплементація зазначених інструментів станом натепер обмежується юридичними протиріччями, що виникають при спробах легалізації результатів використання ШІ в кримінальному провадженні. Як відомо, Кримінальний процесуальний кодекс України від 13.04.2012 р. №4651-VI [7] не містить чітких алгоритмів визнання висновку автоматизованої системи допустимим доказом. Аналогічно до позиції Європейського суду з прав людини у справі «Узун проти Німеччини», де розглядалася правомірність використання засобів технічного спостереження [8], ми повинні забезпечити умови, за яких технологічне втручання буде *передбачуваним* та *санкціонованим*. Відтак, запозичуючи досвід правоохоронних органів США щодо використання аналітичних платформ [9], нам необхідно розробити нормативні акти, які дозволять

використовувати аналітичні звіти ШІ як підставу для ініціювання негласних слідчих (розшукових) дій.

Зрештою, роль СБУ в системі національної безпеки сьогодні полягає у виконанні функцій високотехнологічної системи контролю інформаційних потоків. Зосереджуючись на захисті об'єктів критичної інфраструктури, зокрема в межах виконання Постанови Кабінету Міністрів України «Деякі питання об'єктів критичної інфраструктури» від 09.10.2020 р. №1109 [10], варто відмітити, що впровадження ШІ, в перспективі, надасть можливість фіксувати підготовку до кібератак на етапі сканування вразливостей мереж. Безумовно, окреслений вектор розвитку вимагає не тільки модернізації матеріально-технічної бази, але й в тому числі перегляду підходів до документування.

Список використаних джерел:

1. Про Службу безпеки України: Закон України від 25.03.1992 №2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12

2. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14.09.2020 №392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text

3. Конституція України від 28.06.1996 №254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

4. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 №2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19

5. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 №2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text

6. Barnea A., Assessment Strategic. Integrating the Counterintelligence Discipline into Israel's Security Concept. 2020. URL: https://www.researchgate.net/publication/346024626_Integrating_the_Counterintelligence_Discipline_into_Israel's_Security_Concept

7. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 №4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

8. Uzun v. Germany. App 35623/05. Judgement 02.09.2010. URL: https://hudoc.echr.coe.int/eng?i=001-100293

9. DOJ Report on AI in Criminal Justice: Key Takeaways. 2025. URL: https://counciloncj.org/doj-report-on-ai-in-criminal-justice-key-takeaways/

10.Деякі питання об’єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 09.10.2020 №1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text

Торбас О.О.
завідувач кафедри кримінального процесу,
доктор юридичних наук, професор
(Національний університет
«Одеська юридична академія»)

СПОСОБИ ВИЯВЛЕННЯ DEEPFAKE ПІД ЧАС ПРОВЕДЕННЯ ЕКСПЕРТИЗ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Сучасний розвиток інформаційних технологій взагалі та штучного інтелекту зокрема здійснив вплив (а інколи навіть і революцію) на всі сфери життєдіяльності людини. Не стала виключенням і сфера кримінальної юстиції. Наразі різні моделі машинного навчання та ШІ використовуються при моделюванні та прогнозування злочинності, а методи та способи OSINT дозволяють проводити ефективне досудове розслідування з мінімальними витратами часу та ресурсів. Поряд з цим технології ШІ застосовують і злочинці. І якщо ще років п'ять назад застосування штучного інтелекту було досить обмеженим та вимагало спеціальної технічної підготовки зловмисників, то наразі доступність таких технологій значно знижує поріг компетентності для їх застосування. Окрему загрозу з точки зору забезпечення законності та ефективності кримінального провадження становлять Deepfake – технологія, яка використовує штучний інтелект для створення дуже реалістичних фальшивих зображень та відео. Вона базується на нейронних мережах, зокрема генеративно-змагальних мережах (GAN) [1]. Наразі слідчі, прокурори та судді не можуть «всліпу» довіряти фото та відео матеріалам, які використовуються як докази у кримінальному провадженні, адже можливості їх підробки є вкрай великими. Саме тому наразі у кримінальних провадженнях під час проведення експертиз таких матеріалів додатково експертам ставиться питання на кшталт «чи можливо виключити застосування штучного інтелекту при створенні звукозаписів (відеозаписів/відеозвукозаписів) наявних на оптичному диску». Самі ж експерти стикнулись з вкрай складною проблемою, адже технології ШІ та Deepfake кардинально відрізняються від

звичайної підробки фото, відео чи звукозапису, а тому потребують інших підходів для їх виявлення.

Як вже було зазначено, Deepfake створюється завдяки GAN – генеративно-змагальній мережі (Generative Adversarial Networks), яка була розроблена у 2014 році. GAN складається з двох нейронних мереж: генератора та дискримінатора. Ці мережі перебувають у стані гри з нульовою сумою одна проти одної [2]. Генератор створює синтетичні дані, максимально наближені до реальних, тоді як дискримінатор визначає автентичність згенерованих даних. З плином часу генератор удосконалюється у створенні високореалістичних результатів, здатних вводити дискримінатор в оману, внаслідок чого формується переконливо реалістичний медіаконтент [3].

Таким чином GAN не лише створює реалістичні зображення, а ще і сам себе постійно вдосконалює, через що виявляти такі підробки стає досить складно. Однак і не неможливо. Вже зараз експерти-криміналісти розробили низку автоматизованих методів, які дозволяють виявляти Deepfake, які також базуються на машинному навчанні та ШІ. До найбільш корисних відносять наступні:

1) глибокі нейронні мережі (Deep Neural Networks, DNN) та згорткові нейронні мережі (Convolutional Neural Networks, CNN) [4]. Загалом ці мережі є особливо ефективними для виявлення візуальних аномалій у змінених зображеннях або відео. Для навчання CNN застосовуються великі набори автентичних та модифікованих зображень з метою формування здатності автоматично виявляти невідповідності, зокрема неприродне освітлення, артефакти контурів або зміни на рівні пікселів [5];

2) трансферне навчання та попередньо навчені моделі. Глибоке навчання широко використовує трансферне навчання, за якого модель попередньо навчається на великому, різноманітному наборі даних і адаптується до меншого, спеціалізованого набору для виконання конкретного завдання. У контексті виявлення маніпуляцій цей підхід може застосовуватися для адаптації загальних моделей розпізнавання об’єктів до ідентифікації специфічних ознак модифікацій, що істотно підвищує ефективність та точність [6];

3) автокодери та виявлення аномалій. Автокодери здійснюють стиснення та реконструкцію даних із метою відтворення оригіналу. Виявлення будь-яких маніпуляцій за допомогою автокодера є відносно простим, оскільки втручання завжди спричиняє порушення зв'язків між пікселями, а ці відмінності легко ідентифікуються як індикатори аномалії [7];

4) мультимодальне навчання. Мультимодальне навчання є ще однією передовою технологією. У цьому підході моделі глибокого навчання в режимі реального часу обробляють одночасно різні типи даних – візуальні, звукові, текстові тощо. У випадку маніпуляцій, зокрема Deepfake [8], мультимодальна система може паралельно аналізувати як відеоряд, так і звукову доріжку. Такий підхід дає змогу виявляти невідповідності між рухом губ і мовленням.

В цілому необхідно підкреслити, що всі зазначені методи виявлення Deepfake 1) базуються на використанні ШІ, які налаштовані на 2) пошук аномалій у зображення, фото чи відеоряді. Користь таких моделей полягає в тому, що вона може обробляти значний обсяг інформації та досить швидко надавати результати. Крім того вони можуть помічати аномалії там, де цього не зможе зробити людина, яка буде досліджувати аналогічне фото чи відео. В той же час далеко не завжди Deepfake фото чи відео буде містити аномалії і навпаки, інколи аномалії можуть виникати в оригінальних відео через різні способи стиснення та архівації даних.

Інші методи виявлення експертами Deepfake базуються на технічному аналізі самого зображення чи фото. Дослідження показують, що шляхом поєднання спектральних, колірних та локальних дескрипторів можна виявити цифрові «сліди» оригінальних фото та відео, які були використані як навчальні дані для відповідної моделі Deepfake [9]. Доведення того, що фото або відео містить сліди інших зображень вже може свідчити про їх штучне генерування, що дозволить експертам-криміналістам робити висновки про неможливість використання таких відомостей як оригінальних у кримінальному провадженні навіть без дослідження аномалій, що особливо важливо у ситуаціях, коли таких аномалій немає.

Список використаних джерел:

1. Deepfake. Кібер Брама : офіц. вебсайт. URL: https://stopfraud.gov.ua/cybersecurity-in-communication/deepfake-i1016

2. Xue Z., Jiang X., Liu Q., Wei Z. Global & local facial fusion based GAN generated fake face detection. *Sensors*. 2023. Vol. 23, no. 2. Article 616. DOI: https://doi.org/10.3390/s23020616

3. Shah M. N., Ganatra A. A systematic literature review and existing challenges toward fake news detection models. *Social Network Analysis and Mining*. 2022. Vol. 12, no. 1. P. 1-21. DOI: https://doi.org/10.1007/s13278-022-00995-5

4. Karimi H., Roy P., Saba-Sadiya S., Tang J. Multi-source multi-class fake news detection. *Proceedings of the 27th International Conference on Computational Linguistics*. 2018. P. 1546-1557

5. Singh S., Dhumane A. Unmasking digital deceptions: An integrative review of deepfake detection, multimedia forensics, and cybersecurity challenges. *MethodsX*. 2025. Vol. 15. Article 103632. DOI: https://doi.org/10.1016/j.mex.2025.103632

6. Sultan D. A., Ibrahim L. M. A comprehensive survey on deepfake detection techniques. *International Journal of Intelligent Systems and Applications in Engineering*. 2022. Vol. 10, no. 3S. P. 189–202

7. Rana M. S., Nobi M. N., Murali B., Sung A. H. Deepfake detection: a systematic literature review. *IEEE Access*. 2022. Vol. 10. P. 25494-25513. DOI: https://doi.org/10.1109/ACCESS.2022.3154404

8. Khalid H., Tariq S., Kim M., Woo S. S. FakeAVCeleb: a novel audio-video multimodal deepfake dataset. *Proceedings of the Thirty-Fifth Conference on Neural Information Processing Systems*. Datasets and Benchmarks Track (Round 2). 2021

9. Cassia M. et al. Deepfake Forensic Analysis: Source Dataset Attribution and Legal Implications. *arXiv*. 2025. URL: https://arxiv.org

Туманянц А.Р.
доцент кафедри кримінального процесу,
кандидат юридичних наук, професор
(Національний юридичний університет імені Ярослава Мудрого)
Крицька І.О.
доцент кафедри кримінального процесу,
кандидат юридичних наук, доцент
(Національний юридичний університет імені Ярослава Мудрого)

ЗАГАЛЬНА ХАРАКТЕРИСТИКА НАЙКРАЩИХ ПРАКТИК ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ У СУЧАСНИЙ КРИМІНАЛЬНИЙ ПРОЦЕС

Поступовий перехід кримінального судочинства до електронної форми пов'язаний як з прогресом інформаційно-комунікаційних технологій, так і з сучасними вимогами щодо прискорення обміну інформацією, поліпшення стану дотримання прав і свобод людини та здійснення комплексного аналізу інформації при прийнятті рішень. Цілком природно, що виконання завдань кримінального судочинства в сучасних умовах не може бути забезпечено без ефективного врахування європейського та міжнародного досвіду у сфері кримінального правосуддя.

Тенденція впровадження інформаційно-комунікаційних технологій у світі та розвиток сучасного електронного суспільства вимагають впровадження та подальшого розвитку цифровізації кримінального судочинства в багатьох демократичних країнах, що потребує детального та систематичного аналізу чинного законодавства та уточнення алгоритму електронного кримінального судочинства.

Загалом, лідером у сфері застосування відеотехнологій у судових процесах є Франція. Вона створила Contact Video Justice (правосуддя через відеосистему) – адміністративні віртуальні стійки з доступом до Інтернету, що дозволяють громадянам подавати запити, отримувати та підписувати документи, а також

спілкуватися з адвокатом за допомогою веб-камери. У свою чергу, Польща підійшла до цього питання дещо скромніше і в 2009 році створила електронний суд для розгляду судових рішень та прискорення процесу розгляду позовів про стягнення боргів [1].

Досить креативними і водночас ефективними є індивідуальні ініціативи щодо електронного судочинства, запроваджені іншими країнами. Зокрема, естонський ЦПК передбачає проведення судового розгляду в електронному цифровому форматі та передачу клопотань, заяв, скарг безпосередньо через електронну систему розгляду справ [2]. Кримінальне судочинство Республіки Молдова пропонує до розгляду такі рекомендації, як процедура ad hoc, яка передбачає призначення судового експерта у необхідній для експертизи спеціалізації, та можливість оприлюднення під час судового розгляду відеозапису свідчень неповнолітнього свідка, щоб не залучати його знову [3].

У сучасних реаліях важливу роль відіграє вдосконалення інформаційної підтримки досудового розслідування, оскільки воно спрямоване на спрощення та прискорення процесу розкриття обставин кримінальних правопорушень [4]. З цих питань варто відзначити позитивний досвід електронної взаємодії, успішно впровадженої в Чеській Республіці між органами досудового розслідування та іншими суб'єктами процесу. Яскравим прикладом для наслідування є електронна система Чеської Республіки E-Case Management System (eCMS), яка почала функціонувати в 2006 році в поліції. Її специфіка полягає в матеріальному забезпеченні правоохоронних органів гаджетами, підключеними до eCMS, які дозволяють перевіряти осіб, транспортні засоби, реєструвати провадження, знімати відбитки пальців тощо. Головною перевагою такої системи є можливість фіксувати проведені обшукові дії та отримувати доступ до всіх електронних документів. Саме ця система була взята за основу в Україні [5].

Слід зазначити, що кожна з європейських країн впроваджувала цифрові технології за потребою та в тих сферах, де вони були необхідні. Це призвело до відмінностей у рівнях розвитку електронного правосуддя та методах його впровадження. Звичайно, деякі процеси цифрової трансформації є спільними для європейських країн, наприклад створення електронних реєстрів та

баз даних, ширше використання електронних документів та цифрових підписів, онлайн-консультації, а з початку карантинних заходів – розгляд справ у режимі відеоконференцій. Однак впровадження відповідних технологій залежить від обраної країною політики щодо електронного правосуддя.

Зокрема, в судовій системі можна виділити такі інформаційно-комунікаційні технології: бек-офіс, що підтримує процеси, пов'язані з адмініструванням справ, виготовленням документів та управлінням судом, обробкою текстів та баз даних; технології, що дають змогу сприймати те, що відбувається в самій судовій залі; зовнішні комунікаційні технології, що забезпечують зв'язок із сторонами та інформують громадськість поза межами судів. Суть цих різних технологій однакова: звести функції судді в судовому процесі до прийняття рішення з урахуванням усіх обставин. Уся підготовча та організаційна робота є функцією технології. Тому немає сумнівів, що система електронного суду вже давно є необхідністю, яка значно спрощує доступ до правосуддя.

Позитивний закордонний досвід упровадження та реалізації електронної цифрової форми кримінальних справ лише підтверджує доцільність подальшої модернізації кримінального процесу. Серед таких положень на увагу заслуговують взаємодія з електронними реєстрами, передача клопотань, заяв, скарг безпосередньо через систему електронних справ та проведення судових розглядів в електронному цифровому форматі.

Ми вважаємо, що певні технологічні рішення можуть бути використані не тільки Україною, але й іншими країнами з подібними структурами кримінального правосуддя. До них, зокрема, належать автоматичне повідомлення відповідної електронної інформаційної платформи уповноважених та інших зацікавлених осіб про початок досудового розслідування, автоматизація електронної взаємодії між слідчим і прокурором, формування шаблонів електронних процесуальних документів у реєстрі, повна інтеграція паперових кримінальних проваджень в електронні провадження на основі цієї системи; запровадження взаємодії органів досудового розслідування з іншими суб'єктами кримінального провадження за аналогією з «датобоксом» та створення спеціальної електронної системи, яка взаємодіятиме з державними реєстрами та базами даних, необхідними для кримінального провадження.

Отже, немає сумнівів, що технологічні рішення в сфері правосуддя повинні бути підзвітними, стійкими та максимально прозорими. Однак не всі інновації слід впроваджувати беззаперечно, навіть якщо технологія спочатку виглядає надзвичайно перспективною. Водночас, як справедливо зазначається в науковій літературі, «як алгоритми, так і закон є інструментами впорядкування та раціональності. Ця спільність їхньої природи дає надію, що поєднання права та алгоритмів може стати успішною основою для справедливості та правосуддя» [6]. Найбільш перспективним є потенціал процедурної справедливості при використанні алгоритмів, оскільки вони можуть містити неруйнівні послідовності, що виключають довільне порушення процедури. За умови належного забезпечення відповідного змісту, безпеки та лібералізму, алгоритмічні інструменти можуть сприяти більш справедливому відправленню правосуддя.

Список використаних джерел:

1. Стах Н. (2020). Електронне судове провадження: досвід Європи. 2020. URL: https://loyer.com.ua/uk/elektronne-sudochynstvo-dosvid-yevropy/
2. Каланча І.Г. Електронний сегмент кримінального процесу Естонії. *Порівняльно-аналітичне право*. 2019. №3. С. 212-216. URL: https://pap-journal.in.ua/wp-content/uploads/2021/07/3_2019.pdf
3. Каланча І. Електронний сегмент у кримінальному процесуальному законі Молдови. *Національний юридичний журнал: теорія та практика*. 2020. С. 132-137. URL: http://www.jurnaluljuridic.in.ua/archive/2020/1/30.pdf
4. Ковальова О. В. Шляхи удосконалення інформаційного забезпечення досудового розслідування в сучасних реаліях. *Актуальні проблеми вітчизняної юриспруденції*. 2022. № 3. С. 105–110. URL: https://apnl.dnu.in.ua/3_2022/17.pdf
5. Жученко О. Д. До питання про передумови розроблення електронного кримінального провадження в Україні. *Правова держава*. 2019. № 33. С.116-122. URL: file:///D:/Downloads/Prav_2019_33_18.pdf
6. Cofone Ignacio N. Algorithmic Discrimination Is an Information Problem. *Hastings Law Journal*. 2019. Т. 70. С. 1389-1444. URL: https://repository.uclawsf.edu/hastings_law_journal/vol70/iss6/1/

Церковник С. І.
старший науковий співробітник
відділу організації наукової діяльності,
кандидат юридичних наук, старший дослідник
(Львівський державний університет внутрішніх справ)
Когут В. М.
старший науковий співробітник
відділу організації наукової діяльності,
кандидат технічних наук
(Львівський державний університет внутрішніх справ)

ЕВОЛЮЦІЯ АВТОРСЬКОГО ПРАВА В ЦИФРОВУ ЕПОХУ: ВИКЛИКИ ГЕНЕРАТИВНОГО ШТУЧНОГО ІНТЕЛЕКТУ

Стрімкий розвиток цифрових технологій у XXI столітті суттєво трансформує традиційні суспільні відносини, зокрема у сфері інтелектуальної власності. Одним із найпомітніших феноменів сучасності стало поширення систем Штучний інтелект, здатних генерувати тексти, зображення, музичні композиції та програмний код. У зв'язку з цим виникає необхідність переосмислення класичних підходів до регулювання відносин у сфері Авторське право, які історично формувалися в умовах, коли творчість розглядалася виключно як результат інтелектуальної діяльності людини [1].

Інститут авторського права має тривалу історію розвитку. Його становлення пов'язане з формуванням уявлення про автора як про фізичну особу, що створює оригінальний твір у результаті власної творчої діяльності. Протягом тривалого часу така концепція залишалася незмінною, оскільки технічні засоби лише допомагали людині фіксувати результати творчості, але не могли самостійно створювати нові об'єкти інтелектуальної власності.

Розвиток цифрових технологій та алгоритмів машинного навчання призвів до появи систем, здатних генерувати контент, який за зовнішніми ознаками може відповідати критеріям оригінальності та творчості. Особливе місце серед сучасних технологій посідає генеративний штучний інтелект, що

функціонує на основі складних алгоритмів машинного навчання та великих масивів даних [2].

Такі системи здатні аналізувати значні обсяги інформації, виявляти закономірності та створювати новий контент на основі попередньо опрацьованих даних. У результаті виникає принципово нова ситуація, коли об'єкти, що мають ознаки творчого продукту, можуть створюватися без безпосереднього творчого втручання людини.

Ця обставина породжує низку складних теоретико-правових проблем. Передусім постає питання визначення суб'єкта авторського права на твір, створений за допомогою або із застосуванням систем штучного інтелекту. Традиційна концепція авторського права виходить із того, що автором може бути лише людина, яка створила твір у результаті власної творчої діяльності [2].

Водночас у випадку використання генеративних систем штучного інтелекту виникає кілька потенційних суб'єктів, які можуть претендувати на авторство: розробник програмного забезпечення, користувач, що сформулював запит до системи, або ж власник технологічної платформи.

Виникає дискусійне питання: хто є автором твору, створеного за участю або за допомогою ГШІ? Традиційно автором вважається людина, а твори, створені виключно алгоритмом, не визнаються об'єктами авторського права.

Водночас у процесі генерації контенту можуть брати участь:

- розробник програмного забезпечення;
- користувач, що формулює завдання;
- власник технологічної платформи.

Ще однією проблемою є використання матеріалів, захищених авторським правом, для навчання систем ШІ. Великі обсяги даних, необхідні для ефективного навчання алгоритмів, часто включають твори, які охороняються законом. Використання таких даних без згоди правовласників може порушувати чинне законодовство.

Ще однією важливою проблемою є використання об'єктів авторського права для навчання алгоритмів штучного інтелекту. Більшість сучасних моделей машинного навчання функціонують на основі великих масивів текстів, зображень, музичних творів та

інших матеріалів, значна частина яких охороняється авторським правом. У зв'язку з цим виникає питання про правомірність використання таких матеріалів у процесі навчання алгоритмів.

Нормативну основу правового регулювання авторських прав в Україні становлять положення Цивільний кодекс України та Закон України «Про авторське право і суміжні права», які визначають об'єкти авторського права, суб'єктів авторських прав та порядок їх реалізації [3; 4].

Таким чином, розвиток генеративного штучного інтелекту суттєво впливає на традиційні уявлення про природу творчості та механізми правової охорони її результатів. Сучасні технологічні процеси потребують переосмислення основоположних принципів авторського права та формування нових підходів до регулювання відносин у сфері інтелектуальної власності.

Список використаних джерел:

1. Закон України «Про авторське право і суміжні права» : Закон України від 01.12.2022 № 2811-IX. URL: https://zakon.rada.gov.ua (дата звернення: 06.03.2026).

2. Цивільний кодекс України: Закон України від 16.01.2003 № 435-IV. URL: https://zakon.rada.gov.ua (дата звернення: 06.03.2026).

3. Холявка С. В. (2024) Захист інтелектуальної власності: історія розвитку та перспективи вдосконалення в сучасній Україні // Електронне наукове видання «Аналітично-порівняльне правознавство», №4. С. 177-182.

4. Захист прав інтелектуальної власності в Інтернеті. Що потрібно ззнати власнику. 2025. URL: https://www.pricecontrol.com.ua/ua/shho-potribno-znati-vlasniku-pro-zahist-prav-intelektualnoyi-vlasnosti-v-merezhi-internet/

Циганюк Ю.В.
професор кафедри кримінального права та процесу,
доктор юридичних наук, професор
(Хмельницький університет управління
та права імені Леоніда Юзькова)

ШТУЧНИЙ ІНТЕЛЕКТ У АДВОКАТСЬКІЙ ДІЯЛЬНОСТІ

На сьогодні штучний інтелект (далі - ШІ) розглядається не як заміна адвокату, а як потужний допоміжний інструмент, що відкриває новий етап в розвитку юриспруденції.

Насамперед, потрібно розглядати використання ШІ в аспекті можливостей для професійної діяльності. Так, ШІ використовується адвокатами для попереднього аналізу справ, пошуку судової практики, перевірки гіпотез, структурування матеріалів та автоматизації рутинних процесів (підготовки контрактів, позовів, правового моніторингу) [1; 2].

Серед популярних систем виділяють ChatGPT (OpenAI), Gemini (Google), Copilot (Microsoft), а також спеціалізовані юридичні інструменти, як-от Westlaw Precision та LexisNexis Brief Analyzer [3].

Але застосування ШІ ставить під загрозу фундаментальні засади адвокатської етики. І один із найголовніших ризиків - це порушення конфіденційності та адвокатської таємниці. У аналізованих дослідженнях щодо використання ШІ у адвокатській діяльності окремі автори звертають увагу, що дані, завантажені в ШІ, можуть використовуватися для тренування моделей, що створює реальну загрозу витоку інформації, захищеної адвокатською таємницею [4], а поширення даних клієнта через ChatGPT може кваліфікуватися як розголошення таємниці, якщо не було отримано інформованої згоди клієнта [4].

Також потрібно звернути увагу на компетентність і добросовісність при роботі з ШІ. Адвокат зобов'язаний здійснювати діяльність у межах власних знань. Так, підкреслюють, що ШІ може допомогти лише тоді, коли юрист уміє розпізнавати вигадки та аналізувати контекст. А недбале використання ШІ

можна розпізнати: це посилання на неіснуючі справи, «порожні» шаблонні фрази, залишені в тексті, або навіть смайли й форматування, які зовсім не властиві процесуальним документам. Отже, так само, як юридична фірма перевіряє роботу молодшого юриста, адвокат має перевіряти все, що створює штучний інтелект [1]. Таким чином, використання ШІ без подальшої перевірки результатів як на предмет фактичного існування джерел, так і щодо змісту є порушенням принципу компетентності. Але не виключено, що у майбутньому невикористання ШІ, які могли б покращити швидкість та якість послуг, також буде розглядатися як недолік професійної компетенції

Не варто забувати і про засаду незалежності адвокатури. Адже зустрічаємо інформацію, що існує ризик прихованого впливу розробників технологій на правову позицію адвоката через алгоритми або умови доступу до сервісів [4].

Окремо потрібно звернути увагу на «галюцинації» ШІ. Системи часто генерують вигадані цитати та неіснуючі судові рішення. Також знаходимо іншу проблему у якій зазначено, що ChatGPT у разі перекладу чи редагування тексту на власний розсуд змінював його, керуючись власним розумінням мови ненависті, моралі тощо. Із часом таке втручання може бути глибшим, зі зміною, наприклад, правової позиції і тим самим непомітним, але суттєвим впливом на професійну діяльність адвоката [4].

Звісно, що на даний момент в Україні відсутнє комплексне законодавче регулювання ШІ, хоча існують певні кроки в цьому напрямку (Кодекс суддівської етики (ст. 16), Концепція розвитку штучного інтелекту в Україні), але в сфері адвокатури використання ШІ поки що відбувається шляхом «польових досліджень» самих адвокатів.

Штучний інтелект є потужним ресурсом, але його використання вимагає від адвоката максимального аналізу результатів такої діяльності, адже основний тягар відповідальності них, точність даних та збереження таємниці завжди несе адвокат, а не алгоритм.

Список використаних джерел:

1. ШІ витісняє адвокатів – чи існує реальна загроза професії? URL: https://unba.org.ua/news/10847-shi-vitisnyae-advokativ-chi-isnue-real-na-zagroza-profesii.html

2. Підлужняк С. Штучний інтелект у правоохоронній практиці: ризики та юридичні межі. URL: https://yur-gazeta.com/dumka-eksperta/shtuchniy-intelekt-u-pravoohoronniy-praktici-riziki-ta-yuridichni-mezhi.html

3. Штучний інтелект: практичні та етичні питання у роботі юриста URL: https://www.hsa.org.ua/blog/stucnii-intelekt-prakticni-ta-eticni-pitannia-u-roboti-iurista

4. Городиський І. Штучний інтелект й адвокатська етика: виклики, які існують і ще з'являться. URL: https://justtalk.com.ua/post/shtuchnij-intelekt-j-advokatska-etika-vikliki-yaki-isnuyut-i-sche-zyavlyatsya

Черниченко І.В.
доцентка кафедри кримінального права
та правоохоронної діяльності,
кандидатка юридичних наук, доцентка
(ДВНЗ «Ужгородський національний університет»)

ШІ У СУДІ: ДОЗВОЛИТИ НЕ МОЖНА ЗАБОРОНИТИ. ДЕ ПОСТАВИТИ КОМУ?

Останні роки спостерігається активізація інтересу наукової спільноти до застосування штучного інтелекту (ШІ) у правосудді. Наприклад, Т. О. Рабко аналізувала сучасну судову практику щодо допустимості використання ChatGPT, GROK та DeepSeek у судових процесах для обґрунтування правової позиції учасника [1]. І. В. Гловюк розглянула питання, чи можна вважати покликання сторони на результати, згенеровані ChatGPT, проявом неповаги до суду [2, с. 78–81] та висловила авторську позицію щодо того, чи може використання таких посилань розцінюватися як прояв неповаги до суду та зловживання процесуальними правами залежно від наявності або відсутності так званих галюцинацій [3]. І. В. Басиста та Ж. В. Удовенко досліджували можливість застосування ШІ як допоміжного інструменту автоматизації процесу обробки інформації задля подальшого обґрунтованого ухвалення рішень людиною [4, с. 188–197]. І. А. Тітко та К. С. Крамаренко проілюстровали використання штучного інтелекту як джерела аргументації, що має місце при зверненні учасників кримінального провадження до штучного інтелекту з метою оцінки юридично-значимих фактів з подальшим використанням отриманих результатів для підкріплення власної позиції [5, с. 75–81].

Стрімкий технологічний прогрес зумовив невідкладну потребу в ґрунтовному правовому осмисленні потенційної ролі ШІ у системі правосуддя.

Водночас судова практика щодо допустимості використання згенерованих штучним інтелектом матеріалів у процесуальній діяльності лише формується, що зумовлює появу перших підходів до оцінки подібних ситуацій.

Зокрема, Верховним судом шляхом перевірки відомостей у Єдиному державному реєстрі судових рішень встановлено, що жодного з рішень, на які покликається учасник у касаційній скарзі, не існує. Виявлено, що зазначені номери справ та дати ухвалення постанов є вигаданими, а посилання на сформовані правові висновки – неправдивими. З огляду на це Верховний Суд наголосив, що подання до суду процесуальних документів, згенерованих ШІ, за відсутності фахової перевірки, свідчить про неналежне виконання професійних обов'язків і недобросовісне користування учасником процесуальними правами, що може бути кваліфіковано як прояв неповаги до суду [6]. Варто зауважити, що суддею-доповідачем у цьому провадженні був Я. О. Берназюк, який одним із перших у вітчизняній правничій науці та практиці звернув увагу на можливості застосування штучного інтелекту у професійній діяльності юристів, етичні та правові виклики, пов'язані з його використанням [7; 8; 9].

Подібний підхід простежується і в практиці судів апеляційної інстанції. Так, ухвалою Сумського апеляційного суду від 22 січня 2026 року апеляційну скаргу залишено без задоволення, оскільки на підставі аналізу її змісту суд дійшов висновку про недобросовісне використання інструментів штучного інтелекту під час її підготовки. Зокрема, посилання на нібито існуючі постанови Верховного Суду було визнано грубим викривленням судової практики. У зв'язку з цим було зазначено, що використання вигаданих правових позицій (так званих «галюцинацій» штучного інтелекту) та подання до суду неперевірених процесуальних документів свідчить про неналежне виконання професійних обов'язків, порушує принцип юридичної визначеності та є проявом неповаги до суду [10].

В іншій справі особа, яка подала апеляційну скаргу, щоб «не прикладати відповідних зусиль…, не нести додаткових витрат на таку безнадійну справу як апеляційне оскарження», звернулася до ChatGPT для обґрунтування незаконності оскаржуваної ухвали. Однак суд розцінив такі дії як зловживання процесуальними правами, прояв неповаги до суду, а також до судової системи загалом [11].

У зв’язку з цим постає інше важливе питання: чи можуть судді використовувати технології штучного інтелекту, зокрема для підготовки текстів судових рішень?

Зазначимо, що Концепцією розвитку штучного інтелекту правосуддя віднесено до одного з пріоритетних напрямів, у межах яких передбачається впровадження та розвиток технологій штучного інтелекту [12]. Водночас використання суддею технологій штучного інтелекту допускається за умови, що це не впливає на незалежність та неупередженість судді, не стосується оцінки доказів і процесу ухвалення рішень та не порушує вимог законодавства (стаття 16 Кодексу суддівської етики) [13].

Разом із тим станом на сьогодні ШІ не може повністю замінити суддю. Підтвердженням цього є скасування вироку Дніпровського районного суду м. Києва. Колегія суддів звернула увагу на зміст вироку, який обтяжений довільним трактуванням загальних понять і тверджень, наведенням теоретичних аспектів права, згенерованих штучним інтелектом ChatGPT, що ставить під сумнів суддівський розсуд та судове тлумачення окремих питань. Вирок у такому вигляді, без встановлення судом фактичних обставин кримінального провадження – в будь-якому разі не може бути законним [14].

Курйозним прикладом використання ШІ в судовій діяльності стало застосування відповідного інструменту суддею Новозаводського районного суду міста Чернігова для редагування постанови та виправлення помилок. Текст постанови був внесений до Єдиного державного реєстру судових рішень разом із фразою «Ось перевірений і відредагований варіант вашого тексту з виправленням граматичних, стилістичних і пунктуаційних помилок» [15].

Отже, очевидно, що штучний інтелект має значний потенціал для трансформації діяльності судів. Його використання дає змогу автоматизувати різні процеси, обробляти великі обсяги даних, здійснювати пошук інформації, що дозволяє суттєво заощаджувати час і ресурси. Водночас повноцінне впровадження таких технологій повинно відбуватися лише після проведення ґрунтовних наукових та практичних досліджень, чіткого та комплексного правового регулювання.

З урахуванням проаналізованої судової практики, можна дійти висновку, що штучний інтелект може бути використаний як допоміжний інструмент і виключно під контролем користувача. При цьому необхідно дотримуватися фундаментальних принципів, зокрема поваги до основних прав, недискримінації, забезпечення якості та безпеки, прозорості, неупередженості та зрозумілості. Будь-який результат, згенерований системою штучного інтелекту, повинен бути перевірений на відповідність і достовірність, а відповідальність за використання таких даних несе безпосередньо користувач.

Список використаних джерел:

1. Рабко Т. О. Штучний інтелект у ролі консультанта. Чи приймає суд його висновки? Вища школа адвокатури НААУ. 5 серпня 2025 р. URL: https://www.hsa.org.ua/blog/stucnii-intelekt-u-rolikonsultanta-ci-priimaje-sud-iogo-visnovki

2. Гловюк І. В. Покликання стороною провадження на результати, згенеровані ChatGPT: чи це неповага до суду? Штучний інтелект у правовій практиці: межі та можливості: зб. тез круглого столу (14 березня 2025 року) / упор. О. О. Барабаш. Львів : ЛьвДУВС, 2025. С. 78–81.

3. Гловюк І. В. Використання стороною ШІ у процесуальних документах: (не)зловживання? Форум з кримінального права та процесу імені Й. Л. Бронза. 29 серпня 2025 р. URL: https://surl.li/udbbbn

4. Удовенко Ж. В., Басиста І. В. Використання штучного інтелекту у кримінальному провадженні: ілюзія чи реальність. Штучний інтелект у правовій практиці: межі та можливості: збірник тез Всеукраїнського круглого столу (15 березня 2024 року) / упор. О. О. Барабаш. Львів: ЛьвДУВС, 2024. С. 188–197.

5. Крамаренко К. С., Тітко І. А. Напрями використання штучного інтелекту в кримінальних провадженнях (за матеріалами судової практики). *Електронне наукове видання «Аналітично-порівняльне правознавство».* 2026. Вип. № 1. Ч. 3. С. 75–81.

6. Ухвала Касаційного адміністративного суду у складі Верховного Суду від 15 січня 2026 р. Справа № 240/14153/24. Провадження № К/990/56043/25. URL: https://reyestr.court.gov.ua/Review/133336040

7. Берназюк Я. Практичні аспекти використання технології штучного інтелекту в юридичній сфері. URL: https://surl.lt/dmsyoh

8. Берназюк Я. Штучний інтелект у діяльності Верховного Суду: етичні та організаційні рамки. URL: https://surl.lt/klodtm

9. Берназюк Я. Штучний інтелект у правосудді: ризики алгоритмічної упередженості та дискримінації. URL: https://surl.li/pbjosk

10. Ухвала Сумського апеляційного суду від 22 січня 2026 р. Справа № 588/2256/25. Провадження: № 11-сс/816/171/26. URL: https://reyestr.court.gov.ua/Review/133587000

11. Ухвала Апеляційної палати Вищого антикорупційного суду від 28 травня 2025 р. Справа № 991/4110/25. Провадження № 11-сс/991/368/25. URL: https://reyestr.court.gov.ua/Review/127690240

12. Концепція розвитку штучного інтелекту в Україні. Розпорядження Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text

13. Кодекс суддівської етики. Рішення XX чергового з'їзду суддів України від 18 вересня 2024 р. URL: https://zakon.rada.gov.ua/rada/show/n0001415-24#Text

14. Ухвала Київського апеляційного суду від 30 липня 2025 р. Справа № 11-кп/824/1818/2025. URL: https://reyestr.court.gov.ua/Review/129699665

15. Постанова Новозаводського районного суду міста Чернігова від 17 жовтня 2025 р. Справа №751/8289/25. Провадження №3/751/2816/25 URL: https://reyestr.court.gov.ua/Review/131196945

Чорна М.В.
доцент кафедри адміністративно-правових дисциплін
інституту права та безпеки,
доктор філософії
(Одеський державний університет внутрішніх справ)

ШТУЧНИЙ ІНТЕЛЕКТ У СУДОЧИНСТВІ: ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ТА ПРАВОВІ ВИКЛИКИ

Стрімкий розвиток цифрових технологій спричинив суттєві зміни у функціонуванні державних інститутів, зокрема системи правосуддя. Одним із ключових напрямів цифрової трансформації сучасного суспільства є впровадження технологій штучного інтелекту (ШІ), які здатні здійснювати обробку великих масивів даних, аналіз інформації та підтримувати процес прийняття рішень. У юридичній сфері штучний інтелект розглядається як інструмент підвищення ефективності діяльності судів, оптимізації процесу розгляду справ та покращення доступу до правосуддя [1].

Сучасні дослідження свідчать, що використання технологій штучного інтелекту у правовій сфері може сприяти автоматизації низки процедурних процесів, таких як обробка юридичних документів, аналіз судової практики, пошук релевантних правових норм, прогнозування результатів судових спорів та систематизація доказів [2]. Застосування таких технологій дозволяє значно скоротити час на опрацювання великих обсягів інформації та підвищити ефективність діяльності судових органів.

У багатьох країнах світу технології штучного інтелекту вже активно використовуються для аналізу судової практики та підтримки прийняття управлінських рішень у сфері правосуддя. Зокрема, алгоритми машинного навчання здатні аналізувати попередні судові рішення та формувати рекомендації щодо можливих результатів справи, що сприяє підвищенню передбачуваності правозастосовної практики [3]. Водночас використання таких технологій потребує чіткого правового регулювання, оскільки їх застосування може створювати ризики

порушення принципів справедливості, рівності сторін та незалежності суддів.

В Україні питання використання штучного інтелекту в судочинстві також набуває особливої актуальності в умовах цифровізації державного управління. Науковці зазначають, що технології штучного інтелекту можуть бути ефективним інструментом для оптимізації роботи судів, зокрема шляхом автоматизованого аналізу судової практики, обробки процесуальних документів та формування статистичних даних щодо розгляду справ [4]. Разом з тим, ключовим принципом впровадження таких технологій має залишатися збереження вирішальної ролі людини у процесі здійснення правосуддя.

Окрему увагу в науковій літературі приділяють питанням допустимості використання штучного інтелекту при аналізі доказів у судовому процесі. Деякі дослідники вважають, що алгоритми штучного інтелекту можуть бути ефективними інструментами для обробки цифрових доказів, зокрема відео-, аудіоматеріалів або великих масивів електронних даних. Однак остаточна оцінка доказів та прийняття процесуальних рішень повинні залишатися виключною компетенцією судді, оскільки лише людина здатна врахувати всі обставини справи та забезпечити дотримання принципів справедливого судового розгляду [5].

Водночас застосування штучного інтелекту у правосудді пов’язане з низкою етичних та правових викликів. Серед основних ризиків дослідники виділяють можливість алгоритмічної упередженості, непрозорість функціонування алгоритмів, порушення права на справедливий суд та проблеми захисту персональних даних [6]. У випадку використання автоматизованих систем прийняття рішень виникає питання відповідальності за можливі помилки алгоритму, що потребує чіткого нормативного врегулювання.

Особливої актуальності зазначені проблеми набувають у контексті євроінтеграції України та адаптації національного законодавства до стандартів Європейського Союзу. У європейському праві значна увага приділяється забезпеченню прозорості алгоритмічних систем та запобіганню дискримінації при використанні технологій штучного інтелекту. Дослідники

підкреслюють, що автоматизовані системи можуть створювати ризики алгоритмічної дискримінації, якщо використовувані дані містять приховані упередження або нерівності [7].

Отже, впровадження штучного інтелекту у сферу правосуддя має здійснюватися з урахуванням принципів верховенства права, незалежності суддів та забезпечення прав людини. Штучний інтелект може виступати ефективним допоміжним інструментом для суддів та інших учасників судового процесу, однак він не повинен замінювати людське суддівське рішення. Подальший розвиток технологій штучного інтелекту потребує формування комплексного правового регулювання, яке забезпечить баланс між інноваційним розвитком та гарантіями справедливого судового розгляду.

Таким чином, використання штучного інтелекту у судочинстві відкриває нові можливості для підвищення ефективності функціонування судової системи, проте водночас потребує вирішення низки правових та етичних проблем. Подальші наукові дослідження у цій сфері повинні бути спрямовані на розробку правових механізмів контролю за використанням алгоритмічних систем, забезпечення прозорості їх функціонування та гарантування дотримання фундаментальних прав людини.

Список використаних джерел:

1. Борщевська О. М., Заснов І. О. Правові підстави та перспективи використання штучного інтелекту в судочинстві України. Правова держава. 2023. № 50. С. 106–117. URL: https://rp.onmu.org.ua/handle/123456789/2676;

2. Pysmenna O., Lavrentii Z. Artificial intelligence in jurisprudence: prospects and problems. Modern engineering and innovative technologies. 2024. № 31. С. 69–73. URL: https://www.moderntechno.de/index.php/meit/article/view/meit31-00-095/7187;

3. Гачкевич А. Формування рамок використання штучного інтелекту в судочинстві: іноземний досвід для України. Слово Національної школи суддів України. 2025. № 1(50). С. 45–55. URL: https://slovo.nsj.gov.ua/images/pdf/2025_1_50/Gachkevich.pdf;

4. Гачкевич А. Вплив штучного інтелекту на сферу судочинства та перспективи подальших досліджень. Слово Національної школи суддів України. 2024. № 1(46). С. 27–37. URL: https://slovo.nsj.gov.ua/images/pdf/2024_1_46/03vplyv-shtuchnogo.pdf;

5. Штучний інтелект в судочинстві та судових рішеннях: потенціал та ризики. Науковий вісник Ужгородського національного університету. Серія: Право. 2023. № 78(2). С. 315–320. URL: https://visnyk-pravo.uzhnu.edu.ua/article/view/286487/280342;

6. Bernaziuk I. Artificial intelligence in the Ukrainian judiciary: charting the course under the digital gavel. Верховний Суд України, 2025. URL: https://court.gov.ua/eng/supreme/pres-centr/news/1891488/;

7. Weerts H., Xenidis R., Tarissan F., Olsen H., Pechenizkiy M. Algorithmic unfairness through the lens of EU non-discrimination law. 2023. URL: https://ceur-ws.org/Vol-3442/paper-50.pdf.

Шевченко А.Є.
професор кафедри теорії
та історії держави і права,
доктор юридичних наук, професор
(Державний університет «Житомирська політехніка»)
Григорчук М.В.
професор кафедри права
та правоохоронної діяльності,
доктор юридичних наук, доцент
(Державний університет «Житомирська політехніка»)
Добкіна К.Р.
заступник директора
навчально-наукового інституту управління,
технологій та правових наук,
доктор юридичних наук, професор
(Національний транспортний університет)

ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ НА ПРАВА ЛЮДИНИ

Стрімкий розвиток технологій штучного інтелекту (далі — ШІ) зумовлює глибинні трансформації суспільних відносин, систем публічного управління та механізмів реалізації прав людини. Даний ресурс розроблений для автоматизації рутинних завдань, аналізу великих масивів даних, підвищення продуктивності та імітації людських когнітивних здібностей. Попри швидке поширення в усіх сферах життя суспільства створювані інтелектуальні системи здійснюють значний вплив на права та свободи людини. У зв'язку з цим виникають застереження щодо етичних та правових аспектів використання можливостей ШІ.

Як зазначають автори «Human rights in the age of artificial intelligence», «…штучний інтелект продовжує проникати в наше повсякденне життя, його схильність втручатися в права людини лише посилюється» [1].

Неправомірне або помилкове використання конфіденційної інформації про фізичну особу в системах штучного інтелекту може призвести до негативних для неї наслідків. Особливо коли це

стосується даних, наприклад, про здоров’я людини, її статевої або етнічної приналежності, біометричних даних тощо. Це стосується як самої сутності технологій, так і особливостей їх застосування, що може призводити до складності оскарження автоматизованих рішень, упередженості або дискримінації. Ці аспекти часто пов’язані між собою [2].

Поряд з формуванням правової основи функціонування ШІ представники наукової спільноти активно досліджують проблеми, пов’язані з використання персональних даних штучним інтелектом, та можливих правових наслідків, пов’язаних з такою обробкою. Серед науковців, які працюють над цією проблематикою, Базалицький В. І., Жорнокуй Ю. М., Зозуляк О. І., Пунда О. О., Резворович К. Р., Ткаченко В. В., Шевченко А. Є., Щербина Б. С. та ін.

На наш погляд, осліджeння впливу ШІ на дотримання прав людини доцільно здійснювати в широкому аспекті, а саме розпочинати з основоположних міжнародних документів. Першочергово зазначаємо «Конвенцію про захист прав людини і основоположних свобод» [3], відповідно до якої статтями 6, 8, 10, 14 здійснюється регуляторний вплив, а саме прийняття спеціалізованих міжнародних актів, що конкретизують стандарти Конвенції.

Конституція України [4], хоч не містить спеціальних норм про штучний інтелект, однак її положення повністю поширюються на будь-які алгоритмічні рішення, якщо вони впливають на права, свободи та обов’язки людини, насамперед положеннями статті 3 (Людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю).

Як зазначають Ю. Коваленко і М. Войнов, автори дослідження «Штучний інтелект та права людини: орієнтири та обмеження у контексті національної безпеки та оборони», «Впровадження та застосування таких технологій у нових сферах може створювати певні ризики для основоположних прав та свобод людини, а тому потребує належного правового регулювання і розробку та впровадження безпечних систем ШІ, орієнтованих на дотримання прав людини, а також їх відповідальне використання» [5].

Цікаву думку щодо ролі ШІ в суспільному житті висловлює С. Кравчук. Дослідниця вказує на те, що «Розвиток ШІ ставить під загрозу низку ключових прав людини: право на приватність, право на інформацію, право на свободу вираження поглядів, право на справедливий суд, право на працю, право на охорону здоров'я, право на освіту, права людини в контексті кліматичних ризиків, право на недискримінацію, право на свободу пересування» [6, с. 102].

Ми погоджуємося з висновками дослідниці, проте вважаємо, що особливого контролю правовими інструментами вимагає ситуація, пов'язана з практичною реалізацією конституційного принципу верховенства права в умовах застосування можливостей штучного інтелекту.

Узагальнений висновок про вплив штучного інтелекту на права людини зроблено авторами статті «Вплив штучного інтелекту на реалізацію прав і свобод людини і громадянина в Україні» А. Є. Шевченком, С. В. Кудіним та О. І. Косіловою. Науковці зазначають, що «Проблема впливу штучного інтелекту… пов'язана, перш за все, із захистом права людини на гідність як основного та основоположного права людини, а також право на повагу до приватного та сімейного життя, свободу вираження поглядів, недискримінацію, право на свободу пересування, право на свободу і чесні вибори, право на справедливий суд. Саме тому дослідники на підставі аналізу наукової літератури зосередили свою увагу на дослідження впливу штучного інтелекту на реалізацію окремих прав та свобод людини і громадянина в Україні, а також аналізі ризиків, пов'язаних з цим впливом» [6, с. 66-67].

Висновком з вищезазначеного є те, що ШІ досить глибоко проник в усі сфери життя суспільства, проте життєво важливим залишається необхідність контролю з боку людини за результатами використання можливостей цього ресурсу на напрямках, які визначені як принципи Конституцією України.

Список використаних джерел:

1. Human rights in the age of artificial intelligence. URL : https://www.accessnow.org/wp-content/uploads/2018/11/AI-and-Human-Rights.pdf (дата звернення 27.02.2026 року).

2. Понад 57 % споживачів розглядають використання штучного інтелекту при зборі та обробці персональних даних як значну загрозу для їхньої конфіденційності, згідно з дослідженням Міжнародної асоціації професіоналів у галузі захисту даних (IAPP) 2023 року. Режим доступу: https://iapp.org/resources/article/privacy-and-consumer-trust-summary/ (дата звернення 27.02.2026 року).

3. Конвенція про захист прав людини і основоположних свобод. URL : https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення 27.02.20266 року).

4. Конституція України : Закон України. Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141.

5. Коваленко Ю., Войнов М. Штучний інтелект та права людини: орієнтири та обмеження у контексті національної безпеки та оборони. URL : https://www.helsinki.org.ua/wp-content/uploads/2024/05/Preview_AI_human_right_A4-1.pdf (дата звернення 27.02.2026 року).

6. Кравчук С. Вплив штучного інтелекту на права людини та загальні рекомендації для сталого втілення. Вісник Національного університету «Львівська політехніка». Серія Юридичні науки. № 3(43). 2024. С. 101-110.

7. Шевченко А. Є., Кудін С. В., Косілова О. І. Вплив штучного інтелекту на реалізацію прав і свобод людини і громадянина в Україні. *Legal Bulletin.* №2(8). 2023. С. 66-74.

Шерстюк В.О.
курсант навчально-наукового
інституту поліцейської діяльності
(Національна академія внутрішніх справ).
Науковий керівник – **Чукаєва А.В.**
доцент кафедри кримінології
та інформаційних технологій,
кандидат юридичних наук, доцент
(Національна академія внутрішніх справ)

ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПУБЛІЧНОМУ УПРАВЛІННІ

У сучасних умовах розвитку інформаційного суспільства технології штучного інтелекту набувають дедалі більшого значення у різних сферах діяльності людини. Не є винятком і сфера публічного управління, де застосування таких технологій поступово стає одним із напрямів модернізації державного управління. Разом із тим використання штучного інтелекту в діяльності органів державної влади залишається складним і дискусійним питанням, що пояснюється високим рівнем формалізації та чітким правовим регулюванням діяльності органів публічної адміністрації.

Розвиток цифрових технологій створює нові можливості для оптимізації управлінських процесів у державному секторі. Сучасні уряди дедалі частіше використовують інформаційні системи, що працюють на основі алгоритмів штучного інтелекту, під час аналізу даних та прийняття управлінських рішень. Такі технології можуть суттєво впливати на процес формування державної політики та надання публічних послуг, що безпосередньо позначається на житті громадян [1].

У системі публічного адміністрування управлінські рішення охоплюють як реалізацію державної політики в різних сферах суспільного життя, так і організацію надання адміністративних послуг. Саме тому використання технологій штучного інтелекту може сприяти підвищенню ефективності діяльності державних

органів, оптимізації процесів управління та покращенню якості обслуговування громадян.

Водночас впровадження технологій штучного інтелекту в державному секторі повинно супроводжуватися належним правовим регулюванням. Важливо, щоб використання таких технологій відповідало вимогам законодавства та сприймалося суспільством як допустимий інструмент реалізації державної політики. Крім того, швидкий розвиток цифрових, кібернетичних і віртуальних технологій актуалізує необхідність визначення їх правового статусу та можливостей застосування у різних сферах, зокрема у публічному управлінні.

Традиційно вважається, що основною перевагою технологій штучного інтелекту є їх здатність виконувати окремі функції, які раніше виконувалися людиною, але робити це швидше та ефективніше. Завдяки цьому такі технології можуть значно спростити процес обробки інформації та підвищити результативність управлінських рішень [2].

У наукових дослідженнях існують різні підходи до оцінки ролі штучного інтелекту в управлінні. Частина дослідників вважає, що сучасні алгоритмічні системи здатні функціонувати досить автономно та навіть частково долати інституційні обмеження [3]. Інші науковці, навпаки, наголошують, що штучний інтелект не є принципово новим явищем, а скоріше об'єднує низку технологій, які вже використовуються у сфері управління, хоча їх застосування поки що залишається обмеженим [4].

Ще однією проблемою є відсутність єдиного загальноприйнятого визначення поняття «штучний інтелект». Це створює певні труднощі для його впровадження в систему електронного урядування та використання в діяльності органів державної влади [5].

З практичної точки зору технології штучного інтелекту можуть розглядатися як ефективний інструмент для автоматизації управлінських процесів, обробки великих масивів інформації та підвищення якості прийняття управлінських рішень. Здатність таких систем швидко аналізувати значні обсяги даних може бути корисною для оцінювання ефективності державної політики та планування подальших управлінських дій.

Крім того, значний потенціал технологій штучного інтелекту спостерігається у сфері взаємодії держави з громадянами та юридичними особами. Зокрема, такі технології можуть використовуватися під час надання адміністративних послуг, що дозволить підвищити швидкість їх надання та покращити якість обслуговування.

Разом із тим застосування штучного інтелекту в публічному управлінні супроводжується низкою проблем. На відміну від приватного сектору, державні інституції є менш гнучкими щодо впровадження інноваційних технологій. Крім того, важливим залишається питання відповідальності держави за використання систем штучного інтелекту, особливо у випадках прийняття управлінських рішень або надання адміністративних послуг.

Окремої уваги потребує і питання комерційного використання технологій штучного інтелекту. У державному секторі такі технології повинні застосовуватися насамперед в інтересах суспільства, тому комерційна складова їх використання має бути обмежена. Водночас держава повинна сприяти формуванню довіри громадян до нових технологій та забезпечувати їх поступову адаптацію до цифрових змін.

Одним із можливих шляхів впровадження штучного інтелекту в публічному управлінні може стати реалізація пілотних проєктів у сфері надання адміністративних послуг. Такий підхід дозволить оцінити ефективність використання відповідних технологій, виявити можливі ризики та сформувати необхідну нормативно-правову базу.

Таким чином, використання технологій штучного інтелекту в публічному управлінні має значний потенціал для підвищення ефективності діяльності державних органів. Проте для їх повноцінного впровадження необхідним є формування чіткої системи правового регулювання, забезпечення належного рівня захисту інформації та встановлення ефективного державного контролю за використанням таких технологій.

Список використаних джерел:

1. Busuioc M. Accountable Artificial Intelligence: Holding Algorithms to Account. *Public Administration Review*. 2020. Vol. 81,

Issue 5. P. 825-836. URL: https://onlinelibrary.wiley.com/doi/10.1111/puar.13293

2. Schiff D. S., Schiff K. J., Pierson P. Assessing Public Value Failure in Government Adoption of Artificial Intelligence. *Public Administration*. 2021. P. 1-21. URL: https://www.researchgate.net/publication/351111444_Assessing_Public_Value_Failure_in_Government_Adoption_of_Artificial_Intelligence

3. Ahn M. J., Chen Y. C. Digital Transformation toward AI-Augmented Public Administration: The Perception of Government Employees and the Willingness to Use AI in Government. *Government Information Quarterly*. 2022. Vol. 39, Issue 2. Article 101664. URL: https://www.sciencedirect.com/science/article/abs/pii/S0740624X21001003

4. Medaglia R., Tangi L. The Adoption of Artificial Intelligence in the Public Sector in Europe: Drivers, Features and Impacts. 2022. URL: https://doi.org/10.1145/3560107.3560110

5. Sienkiewicz-Małyjurek K. Whether AI Adoption Challenges Matter for Public Managers? The Case of Polish Cities. *Government Information Quarterly*. 2023. Vol. 40, Issue 3. Article 101828. URL: https://www.sciencedirect.com/science/article/abs/pii/S0740624X2300028X

Юрчук О.В.
начальниця відділу правового аналізу
та моніторингу інвестиційної діяльності
управління з питань економічної політики
(Львівська обласна рада),
викладачка кафедри медичного права ФПДО
(Львівський національний медичний університет імені Данила Галицького)

ВИКОРИСТАННЯ АЛГОРИТМІВ ШТУЧНОГО ІНТЕЛЕКТУ ПРИ ЗДІЙСНЕННІ АНАЛІЗУ СИСТЕМИ ОПОДАТКУВАННЯ ТА ЗАБЕЗПЕЧЕННЯ СТАЛОГО РОЗВИТКУ МЕДИЧНОГО СЕКТОРУ В СУЧАСНИХ УМОВАХ

Охорона здоров’я є пріоритетною сферою соціальної політики держави та пріоритетною галуззю економіки, оскільки безпосередньо впливає на якість життя, здоров'я та благополуччя нації.

Ефективна господарська діяльність в сфері охорони здоров’я залежить в тому числі від належного правового регулювання оподаткування операцій з надання медичних послуг.

Правовідносини, що виникають у сфері справляння податків і зборів, а також оподаткування операцій з постачання медичних послуг, регулюються Податковим кодексом України (далі – ПК України) [1].

Так, відповідно до підпункту 197.1.5 пункту 197.1 статті 197 ПК України звільняються від оподаткування операції з постачання послуг з охорони здоров’я закладами охорони здоров’я, що мають ліцензію на постачання таких послуг, а також постачання послуг реабілітаційними установами для інвалідів та дітей-інвалідів, що мають ліцензію на постачання таких послуг відповідно до законодавства.

Зі змісту наведеної норми варто виокремити умови, за наявності яких ПК України звільняє від оподаткування податком на додану вартість (далі – ПДВ) послуги з охорони здоров’я:

1) медичні послуги надають –

заклади охорони здоров'я, перелік яких затверджено наказом Міністерства охорони здоров'я України від 28.10.2002 № 385 (зареєстрований в Міністерстві юстиції України 12.11.2002 за № 892/7180) [4];

реабілітаційні установи для осіб із інвалідністю та дітей із інвалідністю;

2) ці заклади/установи мають ліцензію на постачання таких послуг.

Отже, послуги з охорони здоров'я, які надають заклади охорони здоров'я та реабілітаційні установи для інвалідів та дітей-інвалідів за наявності спеціального дозволу (ліцензії) на надання відповідних видів послуг з охорони здоров'я, звільняються від оподаткування ПДВ за умови, що такі операції не перелічені в абзацах «а»–«о» пп. 197.1.5 п. 197.1 ст. 197 ПК України.

При цьому операції, перелічені в абзацах «а»–«о» пп. 197.1.5 п. 197.1 ст. 197 ПК України, оподатковуються ПДВ за основною ставкою – 20%.

Також, за змістом листів Державної фіскальної служби № 28692/6/99-99-15-03-02-15 від 30.12.2016 та № 1116/6/99-99-15-03-02-15 від 20.01.2017, вбачається, що операції з постачання послуг з охорони здоров'я закладами охорони здоров'я, що мають ліцензію на надання таких послуг, звільняються від оподаткування ПДВ, за винятком послуг, перелічених у підпунктах «а»–«о» пп. 197.1.5 п. 197.1 ст. 197 ПК України, які підлягають оподаткуванню у загальновстановленому порядку [5; 6].

Аналіз судової практики щодо спорів, які виникають з приводу звільнення від оподаткування операцій з постачання послуг з охорони здоров'я закладами охорони здоров'я, дає змогу виявити недоліки і прогалини практичної діяльності в сфері охорони здоров'я [9].

У справі № 560/3873/20 предметом апеляційного розгляду були доводи Головного управління ДПС у Хмельницькій області про те, що, відповідно до вимог ст. 197 ПК України, від оподаткування звільняються певні операції, а не підприємство.

Спростовуючи такі доводи апеляційної скарги, апеляційний адміністративний суд дійшов висновку про те, що діяльність позивача полягає у постачанні послуг з охорони здоров'я як закладом охорони здоров'я, а тому останній звільняється від

оподаткування податком на додану вартість, відповідно до правових положень податкового законодавства.

При цьому суд наголосив, що операції, зазначені в податкових накладних, фактично не можуть бути об'єктом оподаткування, оскільки товариство (платник податків), відповідно до вимог ст. 197 ПК України, звільнене від оподаткування ПДВ. Також у поданих товариством податкових деклараціях немає записів про операції, що оподатковуються [7].

Отже, аналіз нормативно-правових актів та судової практики свідчить про важливість правильного розуміння в частині надання податкових пільг щодо сплати ПДВ закладами охорони здоров'я при здійсненні ними господарської діяльності з медичної практики. Разом з тим, усунення недоліків і прогалин зменшить навантаження судової системи та стабільність роботи як закладів охорони здоров'я так і контролюючих органів.

Одночасно, отримання податкових пільг щодо сплати ПДВ закладами охорони здоров'я закріплює за суб'єктами господарювання обов'язок, який полягає в аналізі великого масиву інформації щодо операцій з постачання послуг з охорони здоров'я, які підлягають оподаткуванню за пільговою ставкою.

Відповідно до інформації Головного управління ДПС у Львівській області, у 2025-2026 роках зареєстровано 689 платників (юридичних осіб) в галузі «Охорона здоров'я та надання соцдопомоги» (крім бюджетних установ та комунальних некомерційних підприємств), які щодня здійснюють господарську діяльність з медичної практики, надають медичні послуги пацієнтам з різними захворюваннями, ускладненнями та персоналізують плани лікування.

Варто звернути увагу, що в грудні 2020 року Кабінет Міністрів України затвердив Концепцію розвитку штучного інтелекту в Україні, у якій визначені мета, принципи та завдання розвитку таких технологій як одного з пріоритетних напрямів у сфері науково-технологічних досліджень і наведено визначення ШІ: це організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та

використовувати власні бази знань, моделі ухвалення рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань [2].

Також, розпорядженням Кабінету Міністрів України № 320-р від 13.04.2024 схвалено Концепцію Державної цільової науково-технічної програми з використання технологій штучного інтелекту в пріоритетних галузях економіки на період до 2026 р., згідно з якою використання технологій ШІ в пріоритетних галузях економіки дасть змогу підвищити ефективність ухвалення рішень шляхом автоматизованої обробки різноманітної інформації та виявлення нових інформаційних шаблонів і тенденцій [3].

Слід звернути увагу, що медичні установи дедалі частіше використовують аналітичні системи на основі складних алгоритмів машинного навчання, зокрема, щоб виявляти пацієнтів з високим ризиком тих чи інших захворювань, прогнозувати ускладнення та персоналізувати плани лікування [8].

Таким чином, вважаю за доцільне використовувати алгоритми ШІ в сфері охорони здоров'я, що в свою чергу дасть змогу підвищити ефективність роботи закладів охорони здоров'я шляхом автоматизованої обробки інформації щодо операцій з постачання послуг з охорони здоров'я, які підлягають оподаткуванню за пільговою ставкою.

Отже, на моє переконання, використання алгоритмів у медичній практиці відкриє нові можливості для оптимізації господарської діяльності в сфері охорони здоров'я та забезпечення сталого розвитку медичного сектору.

Список використаних джерел:

1. Податковий кодекс України (Відомості Верховної Ради України (ВВР), 2011, № 13-14, № 15-16, № 17, ст.112). URL: https://zakon.rada.gov.ua/laws/show/2755-17#Text.

2. Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-p#Text.

3. Про схвалення Концепції Державної цільової науково-технічної програми з використання технологій штучного інтелекту в пріоритетних галузях економіки на період до 2026 року :

Розпорядження Кабінету Міністрів України від 13.04.2024 № 320-р. URL: https://zakon.rada.gov.ua/laws/show/320-2024-р#.

4. Про затвердження Переліку закладів охорони здоров’я : Наказ Міністерства охорони здоров'я України 28.10.2002 № 385 URL: https://zakon.rada.gov.ua/laws/show/z0892-02#Text

5. Лист Державної фіскальної служби № 28692/6/99-99-15-03-02-15 від 30.12.2016 (Про розгляд листа). URL: https://tax.gov.ua/baneryi/podatkovi-konsultatsii/konsultatsiidlya-yuridichnih-osib/print-71066.html.

6. Лист Державної фіскальної служби № 1116/6/99-99-15-03-02-15 від 20.01.2017 (Про розгляд звернення). URL: https://tax.gov.ua/baneryi/podatkovi-konsultatsii/konsultatsiidlya-yuridichnih-osib/print-71258.html.

7. Постанова Сьомого апеляційного адміністративного суду від 28.01.2021 у справі № 560/3873/20. URL: https://reyestr.court.gov.ua/Review/94565119.

8. Harry A. The Future of Medicine: Harnessing the Power of AI for Revolutionizing Healthcare. International Journal of Multidisciplinary Sciences and Arts. 2023. №2(1). P. 36-47.

9. Юрчук О.В. Оподаткування операцій з постачання послуг з охорони здоров’я закладами охорони здоров’я: питання теорії та практики // Медичне право. – № 1(31) 2023. с. 58-65.

Ярема О.Г.
т.в.о. завідувача кафедри
адміністративно-правових дисциплін
навчально-наукового інституту
права та правоохоронної діяльності,
кандидат юридичних наук, доцент
(*Львівський державний університет внутрішніх справ*)

РОЗВИТОК ПРАВОВОГО РЕГУЛЮВАННЯ ВІДНОСИН ІЗ РОЗРОБКИ ТА ВПРОВАДЖЕННЯ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ

У даний час у світі мало документів, які планують розвиток законодавства щодо правового регулювання відносин із розробки та впровадження систем штучного інтелекту. У більшості випадків йдеться про основні принципи, які визначають концептуальний вектор розвитку правового регулювання сфери, але конкретним планом не є. Рекомендації Організації економічного співробітництва і розвитку з питань штучного інтелекту (Organisation for Economic Co-operation and Development, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449) спрямовані на стимулювання та підтримку компаній та розробників, наукових досліджень, на фінансування першочергових напрямів діяльності [1].

В Україні прийнята Концепція розвитку штучного інтелекту, що є документом планування розвитку законодавства та правового регулювання [2].

У Концепції визначаються мета та завдання правового регулювання відносин у сфері технологій штучного інтелекту, принципи, основні проблеми регулювання та підходи до їх вирішення, окремі напрями та сфери, які вимагають уваги у зв'язку з специфікою відносин. Концепція містить механізми її реалізації.

Метою Концепції є визначення пріоритетних напрямів і основних завдань розвитку технологій штучного інтелекту для задоволення прав і законних інтересів фізичних і юридичних осіб, побудови конкурентоспроможної національної економіки, вдосконалення системи публічного управління. Це передбачає

стимулювання розробки, впровадження та використання таких технологій, створення програмного забезпечення у безпечному виконанні.

У завданнях Концепції розвитку штучного інтелекту наголошено на необхідності створення основ регулювання нових відносин, визначення правових бар'єрів, що ускладнюють розвиток галузі, формування національної системи стандартизації у сфері технологій штучного інтелекту. Напрями регулювання у Концепції поділені на загальногалузеві та галузеві. До перших віднесено: освіта і професійне навчання (сфери – загальної середньої освіти, вищої освіти; підвищення кваліфікації та професійної перепідготовки кадрів); наука; економіка; кібербезпека; інформаційна безпека; оборона; публічне управління; правове регулювання та етика; правосуддя.

Концепція розвитку штучного інтелекту передбачає створення механізмів впровадження продуктів із системами штучного інтелекту (далі – ШІ), розвиток проблем юридичної відповідальності, вдосконалення режиму обороту даних і експорту даних систем, розвиток страхових інститутів, забезпечення безпеки, впровадження актів Європейського Союзу, створення нормативних умов для застосування систем при прийнятті юридично значущих рішень, вдосконалення системи технічного регулювання та оцінки відповідності.

Реалізація освітніх напрямів спрямована на підвищення довіри населення до систем ШІ. Пріоритетними галузевими напрямами впровадження ШІ визначено: охорона здоров'я, публічне управління, транспорт, містобудування, розвиток «розумних міст», фінансова сфера, оборона, промисловість.

Правове регулювання відносин у сфері застосування технологій та систем ШІ потрібно опрацьовувати не з погляду окремих сфер застосування такого програмного забезпечення та технологій, а створювати комплексне уявлення про регулювання.

Правове регулювання відносин щодо використання систем штучного інтелекту має максимально базуватися на існуючих нормах щодо схожих відносин у сфері інформаційних технологій.

Окрему увагу при розгляді питання варто приділити технічним нормам – стандартам і технічним регламентам, а також іншим окремим регуляторам (етичним, організаційним тощо).

Їхню роль при взаємодії з правовим регулюванням відносин у сфері створення та використання систем ШІ складно переоцінити. Вони дозволяють формувати комплексне багатогранне уявлення про об'єкти регулювання. Наприклад, Artificial Intelligence Act [3].

На відміну від суто правових норм стандартизація та розробка етичних норм у цій галузі йде, активно видаються міжнародні та національні документи (UNESCO's Recommendation on the Ethics of Artificial Intelligence: key facts. Available at [4].). Усі вони мають рекомендаційний характер, проте використання їх та відсилання до них при розробці нормативно-правових актів є доречним.

Документи стандартизації розробляються експертами відповідної галузі, встановлюють межі розробки та впровадження нових технологій. Етичні норми та принципи відображають думки та побоювання людей.

З виникненням нових суспільних відносин, пов'язаних з використанням інформаційних технологій, особливої значущості набуває правове регулювання, що забезпечує стійкий і динамічний розвиток цього напряму. Це може забезпечити комплексне використання різних регуляторів – етичних, технічних, організаційних, правових і інших.

Правове регулювання відносин у галузі розроблення та використання систем штучного інтелекту повинно включати: понятійно-категоріальний апарат; спеціальні засади; роль і значення окремих видів систем ШІ, їх застосування в окремих сферах життя з урахуванням функціональних характеристик; загальні вимоги до розробки та правила використання систем ШІ кожного виду; роль і місце окремих регуляторів, а також механізми їхньої взаємодії.

Необхідно передбачити захист від загроз і ризиків з можливістю подальшого розвитку технологій: ліцензування діяльності розробників систем штучного інтелекту та сертифікація останніх; юридично оформлена згода особи, щодо якої системою ШІ приймається автоматизоване рішення; страхування відповідальності розробника; правові презумпції та фікції; презумпція відповідальності людини за рішення систем штучного інтелекту; юридична фікція визнання за системою штучного інтелекту правосуб'єктності; правові гарантії, пільги та стимули

для розвитку галузі та інші засоби та механізми правового регулювання.

Особливе місце у регулюванні розглянутих технологій займає технічне регулювання. Воно більш ефективне щодо завдань формування понятійного апарату, який надалі може використовуватися в процесі правового регулювання, у тому числі при застосуванні посилань до нього. Механізми створення та застосування технічних норм дозволяють більш оперативно порівняно з правовими нормами реагувати на нові технологічні виклики та загрози, розробляються експертами у відповідній галузі, встановлюють межі розробки та впровадження нових технологій з урахуванням інтересів розробників і держави. Зазначене відповідає забезпеченню функціонування та діяльності Технічних комітетів стандартизації відповідно до вимог 7.1.5 ДСТУ 1.14:2015 «Національна стандартизація. Процедури створення, діяльності та припинення діяльності технічних комітетів стандартизації» за напрямом штучного інтелекту та взаємодії між відповідними Технічними комітетами України та міжнародними підкомітетами стандартизації ISO/IEC JTC 1/SC 42 Artificial Intelligence щодо спільного розроблення стандартів у галузі штучного інтелекту [2].

Список використаних джерел:

1. Recommendation of the Council on Artificial Intelligence. URL: https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449

2. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України від 02.12.2020 р. № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text

3. The EU Artificial Intelligence Act. Up-to-date developments and analyses of the EU AI Act. URL: https://artificialintelligenceact.eu/

4. UNESCO’s Recommendation on the Ethics of Artificial Intelligence: key facts. Available at: https://unesdoc. unesco.org/ark:/48223/pf0000385082

НАУКОВЕ ВИДАННЯ

ШТУЧНИЙ ІНТЕЛЕКТ У ПРАВОВІЙ ПРАКТИЦІ: МЕЖІ ТА МОЖЛИВОСТІ

Збірник тез
Міжнародного круглого столу

13 березня 2026 року

Упорядник – **О. О. Барабаш**