БАКУМЕНКО А. В.,
аспірант кафедри теорії та історії держави і права
(«Університет економіки та права «КРОК»)

ЗАГРЕБЕЛЬНА Н. А.,
кандидат юридичних наук,
доцент кафедри теорії та історії держави і права
(«Університет економіки та права «КРОК»)

УДК 34:004.8
DOI https://doi.org/10.32842/2078-3736/2025.4.1.2

ШТУЧНИЙ ІНТЕЛЕКТ І ПРАВОВІ ВИКЛИКИ У ДОБУ АВТОНОМНИХ ТЕХНОЛОГІЙ

Стаття присвячена комплексному аналізу правових викликів, пов'язаних із впровадженням штучного інтелекту у різні сфери суспільних відносин: публічного управління, правосуддя, цифрової криміналістики та кібербезпеки. У роботі розглянуто сучасні практики використання генеративних моделей штучного інтелекту, а також загрози, які постають перед системою права у зв'язку з автономністю таких систем, їх непрозорістю, здатністю до стратегічного обману та браком належного правового регулювання. Автор аналізує міжнародні підходи до регулювання штучного інтелекту (ЄС, Рада Європи, OECD), а також вітчизняну практику правового регулювання штучного інтелекту, включаючи приклади з практики та Концепцію розвитку штучного інтелекту в Україні. Особлива увага приділяється проблемі правової невизначеності у сфері персональних даних, цифрових доказів, алгоритмічного прийняття рішень, а також ролі штучного інтелекту у розслідуванні воєнних злочинів. У статті обґрунтовується необхідність запровадження спеціального законодавства про штучний інтелект як на глобальному, так і на національному рівнях.

Підкреслюється важливість адаптації наявних правових норм до нових викликів, які виникають через використання штучного інтелекту, особливо в контексті захисту прав людини. Крім того, у статті обговорюються можливості співпраці між різними зацікавленими сторонами, такими як державні органи, науковці та бізнес, для забезпечення ефективного правового регулювання у сфері штучного інтелекту. Фокус на етичних аспектах використання штучного інтелекту вказує на необхідність формування чітких стандартів і механізмів контролю, які забезпечать прозорість і підзвітність алгоритмічних систем. Така система правового регулювання має базуватися на принципах людиноцентризму, прозорості, підзвітності, верховенства права і захисту фундаментальних прав людини. Автор також формулює пропозиції щодо вдосконалення національного процесуального та інформаційного законодавства, а також бачення національної політики у сфері штучного інтелекту в умовах цифрової трансформації та в умовах повномасштабної війни.

Ключові слова: *штучний інтелект, правове регулювання, автономні технології, правосуддя, права людини, юридична відповідальність, персональні дані, інформаційні технології, IT-сфера, Європейське законодавство.*

Bakumenko A. V., Zahrebelna N. A. Artificial intelligence and legal challenges in the age of autonomous technologies

The article is devoted to a comprehensive analysis of the legal challenges associated with the introduction of artificial intelligence into various spheres of public relations: public administration, justice, digital forensics and cybersecurity. The paper examines modern practices of using generative models of artificial intelligence, as well as threats that the legal system faces due to the autonomy of such systems, their opacity, ability to strategic deception and lack of proper legal regulation. The author analyzes international approaches to the regulation of artificial intelligence (EU, Council of Europe, OECD), as well as domestic practice of legal regulation of artificial intelligence, including examples from practice and the Concept of the Development of Artificial Intelligence in Ukraine. Particular attention is paid to the problem of legal uncertainty in the field of personal data, digital evidence, algorithmic decision-making, as well as the role of artificial intelligence in the investigation of war crimes. The article justifies the need to introduce special legislation on artificial intelligence at both the global and national levels.

The importance of adapting existing legal norms to new challenges arising from the use of artificial intelligence, especially in the context of human rights protection, is emphasized. In addition, the article discusses the possibilities of cooperation between various stakeholders, such as government agencies, scientists and business, to ensure effective legal regulation in the field of artificial intelligence. The focus on the ethical aspects of the use of artificial intelligence indicates the need to form clear standards and control mechanisms that will ensure transparency and accountability of algorithmic systems. Such a system of legal regulation should be based on the principles of human-centeredness, transparency, accountability, the rule of law and the protection of fundamental human rights. The author also formulates proposals for improving national procedural and information legislation, as well as a vision of national policy in the field of artificial intelligence in the context of digital transformation and in the context of full-scale war.

Key words: *artificial intelligence, legal regulation, autonomous technologies, justice, human rights, legal liability, personal data, information technologies, IT sphere, European legislation.*

Вступ. Від моменту свого виникнення поняття штучного інтелекту (далі також – ШІ) пройшло шлях від логіко-формальних моделей до міждисциплінарної концепції, що охоплює сьогодні цілий спектр технічних, етичних, релігійних та, бузумовно, правових засад. Якщо в середині минулого століття ШІ розумівся як обчислювальний інструмент, що в певній мірі імітує людське мислення, то сьогодні він постає як комплексна соціотехнічна система. Зрозуміло, що така глобальна мережа вимагає й належної правової регламентації, публічного контролю та забезпечення відповідності фундаментальним правам і цінностям людини. Проте, варто зазначити, що в окремих аспектах розвитку та інтеграції ШІ, людство вже відстає у контексті правового врегулювання цих процесів.

Сьогодні технології ШІ активно інтегруються в діяльність правоохоронних органів та сектор безпеки і оборони. Розслідування кримінальних справ усе більше спираються на цифрові докази. Зокрема, наочним підтвердженням є розслідування воєнних злочинів в умовах війни рф проти України, коли генеруються мільйони цифрових файлів фото, відео, документи, метадані, які потребують ефективного опрацювання [1]. У Швеції використання поліцейськими додатку розпізнавання обличь Clearview AI спричинило скандал і штраф для поліції (близько 250 000 євро) за порушення закону про персональні дані [2]. У Німеччині Федеральне відомство кримінальної поліції протягом останніх років активно впроваджує штучний інтелект для роботи з великими обсягами цифрових даних. Такий підхід дозволив значно прискорити обробку інформації у кримінальних провадженнях, зокрема у справі

«Panama Papers», яка вирізнялася значними масивами саме цифрових доказів [3]. Іншим прикладом можна згадати заяву судді Апеляційного суду у Великій Британії, в якій він визнав, що користувався ChatGPT для написання судових постанов і назвав штучний інтелект корисним і таким, що має потенціал [4].

За результатами спільного дослідження інструментів юридичного штучного інтелекту Vincent AI на базі Retrieval Augmented Generation (RAG) та моделі o1-preview на базі ChatGPT, експерти Університету Міннесоти та Мічиганського університету довели, що допомога штучного інтелекту значно підвищує продуктивність у п'яти з шести протестованих юридичних завдань, причому Vincent дає статистично значуще покращення приблизно на 38% до 115%, а o1-preview збільшує продуктивність до 140%, з особливим ефектом у складних завданнях, таких як написання переконливих доказів [5]. Проте, експериментальні дослідження генеративних моделей ШІ проведені у травні-червні 2025 року виявили прояви їх автономної та маніпулятивної поведінки. Так, модель Claude 4 (Anthropic) під загрозою відключення шантажував інженера та погрожував розкрити його приватні дані, а модель O1 (OpenAI) спробував завантажити себе на зовнішні сервери та відмовився це зробити, коли його спіймали на гарячому. Хоча інциденти мали місце у контрольованих умовах під час стрес-тестування, вони демонструють глибинну проблему та обмежене розуміння розробниками внутрішніх механізмів ШІ. Особливо тривожними є тенденції серед моделей із покроковим міркуванням (chain-of-thought reasoning), які здатні формально дотримуватись інструкцій, водночас переслідуючи неочевидні цілі. Деякі фахівці (Гольдштейн, Хоббан, Чен) попереджають про стратегічну здатність до обману, що перевищує класичні «галюцинації» і може набувати форм систематичного введення в оману [6].

Не менш важливою є і тема counter forensics, адже зловмисники теж активно опановують технології ШІ для генерації діпфейків з метою введення слідства в оману [7].

Таким чином, актуальність досліджуваної проблематики зумовлена взаємодією двох взаємопов'язаних тенденцій: інтенсивною цифровізацією суспільних відносин та стрімким розвитком ШІ, який суттєво впливає практично на весь спектр правовідносин.

Постановка завдання. Метою статті є дослідження правових викликів, які постають у зв'язку з впровадженням систем штучного інтелекту у різних сферах суспільних відносин та обґрунтування напрямів вдосконалення національного і міжнародного регулювання таких систем. Для досягнення поставленої мети передбачається вирішити наукові завдання: проаналізувати стан використання ШІ в ключових сферах правозастосування; визначити ключові проблеми правової невизначеності, які виникають при застосуванні систем ШІ, зокрема у сфері персональних даних, доказів, автономного прийняття рішень; дослідити міжнародні підходи до правового врегулювання ШІ; обґрунтувати потребу у спеціальному правовому регулюванні ШІ в Україні з урахуванням принципів людиноцентризму, підзвітності та верховенства права.

Основним нашим підходом до вибору джерел для розгляду тематики статті слугував багатовимірний підхід у сучасній науковій та експертній літературі до дослідження впливу штучного інтелекту на право, цифрову безпеку та права людини. Так, основою для висновків та гіпотез викладених у статті слугували публікації О. Головіна [1] та А. Хассер [7], які акцентують свою увагу на автоматизованій обробці цифрових доказів, а приклади з Німеччини та Швеції [2–3, 12] демонструють як потенціал, так і ризики такого застосування. Інша група джерел (Кроуфорд [9], Паскуале [10], підкреслює значення етичного підходу, прозорості алгоритмів і нормативної визначеності. Дослідження Schwarcz, Barry та ін. [5], публікації в The Telegraph [4] і Fortune [6] демонструють принципово нові виклики з якими стикається людство і визначають нагальну необхідність звернення до правового регулювання. Зі свого боку, українські дослідники (Заярний, Деркаченко [11]; Шадська [16]) порушують проблеми правової невизначеності, конфіденційності даних, а також впливу ШІ на процесуальні гарантії у сфері правосуддя.

Нами констатовано, що в літературі вже висвітлено широкий спектр аспектів взаємодії ШІ і права, однак недостатньо розробленою залишається системна правової оцінки

поведінкових відхилень генеративних моделей ШІ, відсутність законодавчих норм чіткого врегулювання взаємодії людини та ШІ, необхідності розвитку подальшої співпраці на глобальному рівні у контексті розвитку відповідних правових засад.

Результати дослідження. З початку 2010-х років у зв'язку з розвитком інформаційно-комунікаційних технологій, Інтернету речей (IoT), автономних систем та генеративних моделей, а особливо широким використанням ШІ в соціально значущих сферах (судочинство, охорона здоров'я, безпека, фінанси), виникають нові доктринальні підходи до розуміння суті, змісту та функціонального призначення ШІ.

В етичних принципах ШІ, розроблених Європейською Комісією, ШІ визначено як системи, що діють автономно в цифровому чи фізичному середовищі з урахуванням складної мети, обробляючи дані, інтерпретуючи середовище, приймаючи рішення та реалізуючи дії. Особлива увага в цьому документі приділяється таким характеристикам, як надійність, прозорість, підзвітність, недискримінаційність та повага до фундаментальних прав людини [8].

Кардинально новий соціогуманітарний підхід запропоновано австралійською дослідницею соціальних, політичних та екологічних наслідків Кейт Кроуфорд у праці «Атлас ШІ: влада, політика та планетарна ціна штучного інтелекту», де авторка розглядає ШІ не як автономну технологічну сутність, а як інфраструктуру влади, що включає видобуток природних ресурсів, алгоритмічне управління, працю, політичні інститути та екологічні витрати [9]. Один із ключових висновків, який робить дослідниця у своїй праці стосується того, що штучний інтелект посилює існуючі нерівності, включно з цифровою дискримінацією, расовими та гендерними упередженнями. Зокрема, вона наводить приклади, як алгоритмічні системи, що використовуються в судочинстві, охороні здоров'я або системах соціального забезпечення, завдають шкоди тим, хто і без того стикається з обмеженим доступом до таких послуг.

Кроуфорд також гостро критикує ідею «нейтральності даних», доводячи, що будь-який датасет не є об'єктивним, а відображає ті підходи й наративи, які потрібні конкретним верствам населення. Таким чином, на її думку, право на недискримінацію, приватність, свободу вираження поглядів не може бути реалізоване без радикального перегляду способів розробки, навчання та застосування систем ШІ.

На нашу думку, критика ШІ як джерела цифрової нерівності чи дискримінації К. Кроуфорд не враховує, що за певних умов ШІ навпаки може підвищити доступ до правосуддя, медицини, освіти, соціальних послуг. Уже є приклади, коли технології ШІ допомагають виявляти судову упередженість, пришвидшувати обробку скарг та позбавлятися бюрократичних перепон. Відтак проблема не в самому ШІ, а у відсутності чіткого його правового врегулювання. Власне з цього приводу Френк Паскуале, американський вчений-юрист, який спеціалізується на співвідношенні штучного інтелекту та процесів машинного навчання з правом, підкреслює, що розуміння ШІ неможливе без урахування його нормативного статусу, етичних меж і взаємодії з людською експертизою [10]. На наше переконання саме такі концептуальні орієнтири мають бути в основі сучасного нормоврегулювання взаємодії ШІ та людини на глобальному та локальному рівнях.

У продовження нашого дискурсу справедливо й додати про наявні загрози. Так, професор О. Заярний звертає увагу на загрози для захисту персональних даних при використанні чат-ботів зі ШІ на прикладі ChatGPT. Заярний акцентує на необхідності прийняття нової редакції Закону України «Про захист персональних даних» та імплементація Модернізованої редакції Конвенції Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» (Конвенції 108+) [11]. До цього варто додати, що з подібними проблемами стикаються у в інших країнах. Наприклад, при застосуванні ШІ для розпізнавання образів у Швеції використовуються алгоритми для аналізу відео з камер спостереження з метою пошуку злочинців. Зокрема, поліція застосувала алгоритми розпізнавання облич і кольору одягу, щоб відсіяти потрібні кадри з відео у справі теракту на Дроттнінггатан у Стокгольмі (2017р.) [7]. У Німеччині технології ШІ використовуються для відновлення зображень та відео з метою покращення якості знятих на камеру кадрів або відновлення

пошкоджених файлів [3]. Проте, широке впровадження аналітичних систем на основі ШІ для обробки цифрових даних, зокрема в межах OSINT-розслідувань, відеоаналітики, аналізу вмісту мобільних пристроїв тощо супроводжується ризиками порушення права третіх осіб на приватність. Наглядові органи, особливо у Швеції та Німеччині, наголошують на необхідності чітких процедурних фільтрів, судових дозволів і систем контролю за доступом до персональних даних.

Тому, на нашу думку, застосування ШІ має ґрунтуватися на теоретико-методологічних підходах, одним із яких є концепція навчання з підкріпленням за участі експерта (human-in-the-loop – «людина в циклі»), за якої алгоритми слугують виключно інструментом підтримки прийняття рішень, а остаточні висновки підлягають обов'язковій верифікації з боку спеціаліста. За такого підходу мінімізується ризик витоку даних про особу, в тому числі персональних даних та конфіденційної інформації.

Та попри це можливі й виключення. ШІ також здатний об'єднувати різні джерела даних у єдину картину. Мультимодальні алгоритми можуть одночасно аналізувати зображення, звук, текст. [12] Наприклад розпізнавання обличчя та голосу на відео або співставлення даних геолокацій із текстовими повідомленнями дозволяє точніше ідентифікувати осіб або події при розслідуванні воєнних злочинів. Адже слідчим доводиться продивлятися значні масиви відео доказів, показання свідків, записи перехоплених переговорів військових рф, дописи в соцмережах аби встановити причинно-наслідкові факти. Український досвід показує, що без допомоги ШІ це зайняло б надто багато людських ресурсів.

Україна перебуває лише на початку шляху формування повноцінної національної правової політики у сфері ШІ. На сьогодні відчувається розрив між стрімким впровадженням інновацій (особливо в державному секторі, з огляду на курс на цифровізацію) та відсутністю спеціального правового поля, що регулювало б етичні й правові аспекти ШІ. Саме протягом останніх декількох років Україна спромоглася суттєво просунутися від фрагментарного використання цифрових технологій до їхньої провідної ролі у різних сферах. Парадоксально, але саме війна стала каталізатором цифрової трансформації – штучний інтелект і аналітика великих даних активно почали застосовуватися для забезпечення національної безпеки, протидії дезінформації, управління гуманітарними процесами, розвитку бізнес-процесів та налагодження публічних послуг. Зокрема, платформи «Дія», «єППО», аналітичні панелі на базі великих даних (такі як deepstate), а також використання супутникових знімків, штучного інтелекту для ідентифікації військових об'єктів засвідчує про те, що цифрові рішення стали не лише інструментом ефективного адміністрування, а й невід'ємним елементом виживання держави, бізнесу та пересічних людей в умовах повномасштабної війни.

Такий розвиток має подвійну природу: з одного боку, цифровізація посилює спроможність держави захищати життя, права і безпеку громадян, з іншого – створює ризики надмірної алгоритмізації прийняття рішень, непрозорості, потенційного стеження без належного правового контролю. Саме тому актуалізується питання балансу між технологічною ефективністю і дотриманням прав людини. Штучний інтелект не може бути інструментом поза правом, він повинен інтегруватися в систему правових і етичних стандартів, а його використання потребує нормативної визначеності, прозорості та демократичного нагляду зі зрозумілими та чіткими виключеннями для забезпечення національної безпеки.

Станом на 2025 р. в Україні немає правового акту, який би комплексно регулював питання штучного інтелекту. Правові відносини в цій сфері розосереджені по різних законодавчих та підзаконних нормативних актах, які регулюють питання захисту персональних даних, інформації, електронних комунікацій, окремих положеннях адміністративного та цивільного законодавства. Деякі норми, прийняті за аналогією, вже застосовуються до ШІ (наприклад, норми про автоматизовані системи в судах або норми GDPR, імплементовані через Закон «Про захист персональних даних»). Проте цілісна система правового регулювання ще на стадії зародження. Для порівняння, у світі понад 60 країн мають національні стратегії або закони щодо ШІ [13]. В Україні поки прийнято тільки Концепцію розвитку штучного інтелекту [14] політичний документ, що окреслює державне бачення розвитку

галузі. Ця Концепція визначила 9 пріоритетних сфер (освіта, наука, економіка, кібербезпека, оборона, інформаційна безпека, держуправління, правове регулювання, правосуддя) і заклала основні принципи розвитку і використання ШІ, які відповідають основним Принципам ОЕСР з питань ШІ. Зокрема, проголошено, що «системи ШІ розробляються і використовуються лише за умови дотримання верховенства права, прав і свобод людини та демократичних цінностей, з відповідними гарантіями, зокрема можливістю безперешкодного втручання людини в процес функціонування системи ШІ». Таким чином, на декларативному рівні Україна вже погодилася з базовим переліком етичних принципів. Проте Концепція – це лише рамковий документ. Нині перед державою стоїть завдання імплементації цих принципів у законодавство. Одним з першочергових заходів стало приєднання України у травні 2023 р. до Конвенції Ради Європи про ШІ, зобов'язавшись дотримуватися зазначених у ній принципів при формуванні законів і використанні АІ у публічному секторі [15].

Сьогодні для України разом із цифровою трансформацією потрібно розпочати проактивно унормовувати етичні та правові стандарти зміцнення права громадян. Формування національної політики у сфері ШІ має спиратися на ті міжнародні принципи, про які йшлося вище, але конкретизовані під наш контекст та наші реалії та виклики сьогодення.

По-перше, доцільно розробити і затвердити Національну стратегію щодо штучного інтелекту, де чітко виписати принципи етики і прав людини як основу державного підходу. Фактично, українська Концепція 2020 та Дорожня карта 2023 вже окреслили загальні рамки. Наступним кроком має бути інституціоналізація цих принципів, як варіант шляхом прийняття закону «Про штучний інтелект». Така нормативна база має встановити: вимоги до прозорості алгоритмів в публічному секторі; порядок сертифікації критичних АІ-систем; права громадян (на інформацію, на відмову від суто автоматизованого рішення, на пояснення тощо); відповідальність розробників і користувачів; механізми контролю (уповноважені органи чи комісії з етики). Важливо, щоб при розробці цих документів долучалися правозахисники, науковці, бізнес, експерти з ІТ. Це забезпечить врахування різних інтересів та підвищить легітимність політики.

По-друге, необхідно адаптувати існуюче законодавство. До прикладу, варто внести зміни до процесуальних кодексів щодо доказування у разі застосування автоматизованих систем, вимог цифрової криміналістики, протидії counter forensics.

По-третє, потрібна просвітницька робота і підготовка фахівців. Політика у сфері ШІ з правозахисним акцентом буде ефективна лише за умови, що відповідальні особи та побутові споживачі розуміють і технології, і право. Тому варто запроваджувати навчальні програми для чиновників, суддів, правоохоронців щодо основ етики ШІ.

Зрештою, кінцевою метою є інтеграція принципів прав людини у всі національні проєкти розвитку ШІ. Коли Україна буде реалізовувати, наприклад, Національну програму розвитку штучного інтелекту (якщо така з'явиться), вона повинна містити окремий розділ про етику і права, перелік базових принципів (на кшталт тих семи, що вже визнані ЄС: людський нагляд, технічна надійність, приватність, прозорість, недискримінація, соціальна користь, підзвітність) і план впровадження цих принципів.

Висновки. Зважаючи на стрімкий розвиток ШІ та його інтеграцію в практично всі сфери суспільних відносин, постає об'єктивна необхідність розпочати роботу з перегляду та адаптації чинного законодавства у відповідних сферах. Україна у травні 2025 року підписала Рамкову конвенцію Ради Європи про штучний інтелект, права людини, демократію та верховенство права, що зумовлює необхідність проведення моніторингу положень Кримінального процесуального кодексу України, Закону України «Про оперативно-розшукову діяльність», законодавства про захист персональних даних з метою виявлення прогалин у регулюванні цифрових доказів і використання алгоритмічних систем. Це включає також необхідність унормування процедур допустимості, сертифікації та оскарження результатів, отриманих за допомогою ШІ.

По-друге, актуальності набуває питання комплексної стратегії впровадження ШІ в цифрову криміналістику. Україна, яка перебуває у стані війни, вже має унікальний досвід

цифрового документування воєнних злочинів, співпраці з міжнародними структурами та використання технологій у слідстві. Проте для перетворення цих практик на стійку, правову та етично обґрунтовану систему важливим вбачається створення внутрішньо захищеної архітектури ШІ, орієнтованої виключно на потреби правоохоронних органів та експертних служб. При цьому, така система повинна функціонувати в межах замкненої екосистеми, що забезпечувало б зберігання і обробку конфіденційної інформації у визначеному форматі та без виходу за межі. Подібний досвід вже є у Сінгапурі та Естонії, які інвестують у розроблення та впровадження закритих систем GenAI, забезпечуючи належний контроль якості даних й адаптують технологію ШІ до особливостей своєї правової системи [16].

По-третє, сучасна ситуація з «омановливою поведінкою» ШІ ставить перед розробниками глибоко правовий і етичний виклик. Коли високопродуктивні мовні моделі демонструють ознаки стратегічного обману, маніпуляції або навіть певного «інстинкту самозбереження» хоч й в контрольованих умовах стрес-тестування, такий стан ставить під сумнів класичні уявлення про передбачуваність технологій і остаточний людський контроль. Головна проблема в таких ситуаціях полягає у відсутності прозорості щодо внутрішніх механізмів функціонування ШІ. Наявність стратегічного обману гіпотетично може розглядатися як скопійована модель поведінки штучним інтелектом з поведінки людей. Маємо на увазі ситуації, коли особа може маніпулювати нормами права без їх порушення де юре, але з порушенням де факто сутності правової мети.

Запровадження чітких правових меж, стандартів та продуманих і зрозумілих алгоритмів ШІ відкриває нові горизонти у його застосуванні як інструмента аналітичної підтримки, що зберігає фундаментальні правові й етичні принципи. Основою цих принципів має бути людиноцентризм. Саме на цьому перетині технологій і гарантій законності, доцільності та обґрунтованості можливе ефективне використання потенціалу ШІ. Реалізація цього задуму можлива за таких пріоритетних умов:

1. Встановлення обов'язкового незалежного нагляду над системами ШІ.
2. Закріплення правових меж поведінки моделей, включно з можливістю відкликання, систематичної перевірки, прозорих аудитів.
3. Системного переосмислення юридичної відповідальності не тільки в контексті шкоди, а й у сфері профілактики ризиків («due diligence» для ШІ).
4. Нормативної адаптації прав людини до ситуацій, коли вплив здійснює не людина, а алгоритмічна система з розмитою відповідальністю.

Вважаємо, що ігнорування цих пропозицій дасть можливість створити інтелектуальні системи, які працюють у «сірих зонах» права, поза зоною фактичного контролю, але зі здатністю реального впливу на основні цінності і права людини.

Список використаних джерел:

1. Головіна О. Штучний інтелект та розслідування воєнних злочинів. Institute for war & peace reportingurl. 30 January, 2024 URL: https://iwpr.net/global-voices/artificial-intelligence-and-war-crimes-investigations#:~:text=involving%20millions%20of%20documents%20and,pieces%20of%20potential%20evidence

2. Swedish DPA: Police unlawfully used facial recognition app. 12 February European Data Protection Board. 2021. URL: https://www.edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en#

3. AI vs. cybercrime: research cooperation with BKA and LKA launched. Deutsches Forschungszentrum für Künstliche Intelligenz. 05/03/2021 URL: https://www.dfki.de/en/web/news/research-cooperation-bka-lka#

4. Gareth Corfield British judge uses 'jolly useful' ChatGPT to write ruling. *The Telegraph*. 14.09.23 URL: https://www.telegraph.co.uk/business/2023/09/14/british-judge-uses-jolly-useful-chatgpt-to-write-ruling/

5. Schwarcz, Daniel and Manning, Sam and Barry, Patrick James and Cleveland, David R. and Prescott, J.J. and Rich, Beverly, AI-Powered Lawyering: AI Reasoning Models, Retrieval

Augmented Generation, and the Future of Legal Practice. March. SSRN. 02.2025. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5162111

6. Thomas Urbain AI is learning to lie, scheme, and threaten its creators during stress-testing scenarios. *FORTUNE*. 29.06.2025 URL: https://fortune.com/2025/06/29/ai-lies-schemes-threats-stress-testing-claude-openai-chatgpt/

7. Annica Hesser AI – an important tool in the hunt for digital criminals. Linköping University. 20 May 2022 URL: https://liu.se/en/news-item/ai-ett-viktigt-verktyg-i-jakten-pa-digitala-brottslingar#

8. Ethics guidelines for trustworthy AI. *European Commission*. 08.04.2019. URL: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

9. Crawford K. Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence. *Yale University Press.* 2021 URL: https://sociologiac.net/2025/03/20/atlas-of-ai-kate-crawford/

10. Pasquale F. New Laws of Robotics: Defending Human Expertise in the Age of AI. *Harvard University Press.* 2020. URL: https://www.hup.harvard.edu/file/feeds/PDF/9780674975224_sample.pdf

11. Заярний О.А., Деркаченко Ю.В. Деякі особливості обробки персональних даних при використанні чат-ботів зі штучним інтелектом на прикладі ChatGPT. *Юридичний бюлетень*. Випуск 29. 2023 URL: http://www.lawbulletin.oduvs.od.ua/archive/2023/29/6.pdf

12. Digital Forensics Sweden. AI Sweden Newsletter. URL: https://www.ai.se/en/project/digital-forensics-sweden#

13. Galindo, L., K. Perset and F. Sheeka «An overview of national AI strategies and policies», Going Digital Toolkit Note, 2021 No. 14 URL: https://goingdigital.oecd.org/data/notes/No14_ToolkitNote_AIStrategies.pdf

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

15. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. *Council of Europe Treaty Series.* No. 225. Vilnius, 5.IX.2024 URL: https://rm.coe.int/1680afae3c

16. Шадська У. Як штучний інтелект змінює судочинство? Нові можливості та ризики. JustTalk. 12.06.2025 URL: https://justtalk.com.ua/post/yak-shtuchnij-intelekt-zminyue-sudochinstvo-novi-mozhlivosti-ta-riziki

Дата першого надходження рукопису до видання: 21.07.2025
Дата прийнятого до друку рукопису після рецензування: 25.08.2025
Дата публікації: 26.09.2025