УДК 343.9:004.8
DOI https://doi.org/10.32782/pdu.2025.1.49

Т. А. Латковська
доктор юридичних наук, професор,
завідувачка кафедри конституційного, адміністративного та фінансового права
Чернівецького навчально-наукового юридичного інституту Національного університету «Одеська юридична академія»
orcid.org/0000-0003-3159-5994

А. В. Марущак
кандидат юридичних наук, доцент,
доцент кафедри конституційного, адміністративного
та фінансового права
Чернівецького навчально-наукового
юридичного інституту Національного Університету
«Одеська юридична академія»
orcid.org/0000-0002-4611-4906

ІНТЕГРАЦІЯ ШТУЧНОГО ІНТЕЛЕКТУ У ДІЯЛЬНІСТЬ ПРАВООХОРОННИХ ОРГАНІВ: РИЗИКИ В КОНТЕКСТІ КІБЕРБЕЗПЕКИ

Наукова стаття присвячена дослідженню феномену інтеграції штучного інтелекту у діяльність правоохоронних органів України з урахуванням сучасних викликів у сфері цифрової трансформації та кібербезпеки. Обґрунтовано, що використання ШІ в роботі правоохоронних органів є не лише технологічною інновацією, а й правовою, етичною і безпековою проблемою, що потребує системного аналізу. Проаналізовано конкретні приклади впровадження інтелектуальних рішень у практику правоохоронних органів, зокрема в сфері відеоаналітики, обробки цифрових доказів, автоматизації документообігу, прогнозової аналітики правопорушень і розслідування злочинів проти дітей. Досліджено також перспективи адаптації таких моделей, як Retrieval Augmented Generation (RAG), у кримінальному провадженні.

У межах наукового аналізу розглянуто національні нормативно-правові акти, зокрема Закон України «Про основні засади забезпечення кібербезпеки України», Концепцію розвитку штучного інтелекту в Україні до 2030 року та документи Міністерства цифрової трансформації України. Визначено, що наявне законодавче поле є фрагментарним, не забезпечує належного регулювання правового статусу алгоритмів ШІ, не передбачає механізмів відповідальності за їх наслідки та потребує уніфікації із міжнародними стандартами, зокрема ISO 27001 та ISO/IEC 27032.

Наголошено на подвійній природі статусу правоохоронних органів у контексті ШІ: з одного боку, вони є суб'єктами забезпечення національної кібербезпеки, а з іншого – самі виступають об'єктами, на які поширюються ризики цифрових загроз.Визначено, що комплексне забезпечення безпеки вимагає не лише оновлення технічної інфраструктури, а й цифрової грамотності персоналу, процедурного контролю, а також незалежного нагляду за використанням алгоритмів у публічному секторі. Окреслено сучасний стан впровадження ШІ в діяльність українських правоохоронних органів, розглянуті шляхи гармонізації правового регулювання з європейською практикою, зміцнення кібербезпеки та посилення захисту прав людини в умовах цифрової епохи.

Ключові слова: *кібербезпека, штучний інтелект, правоохоронні органи, цифровізація, Національна Поліція України, кіберзлочинність.*

Вступ. У сучасному вирі цифрових трансформацій штучний інтелект (ШІ) поступово стає невід'ємною складовою ефективного функціонування державних органів у цілому та правоохоронних органів зокрема. Його використання в оперативно-розшуковій, аналітичній, слідчій діяльності дозволяє значно підвищити точність прогнозування, пришвидшити обробку великих обсягів даних, а також автоматизувати рутинні процеси. В умовах війни та післявоєнної відбудови України, технології ШІ можуть відіграти стратегічну роль у боротьбі з новими формами кіберзлочинності, виявленні гібридних загроз, моніторингу критичної інфраструктури.

Разом із тим, стрімке впровадження цифровізаційних процесів у роботу поліції, прокуратури, прикордонної та антикорупційної служб супроводжується низкою викликів, серед яких ключове місце посідають ризики у сфері кібербезпеки. Відсутність належного правового регулювання, слабкий контроль за алгоритмами, незахищеність каналів обміну даними, потенційні маніпуляції з боку третіх сторін – усе це створює передумови для зловживань та порушення прав людини. Особливо небезпечною є можливість використання ШІ для політично вмотивованого контролю, маніпуляції доказами або несанкціонованого доступу до конфіденційної інформації.

Аналіз останніх досліджень і публікацій. Проблематика інтеграції штучного інтелекту у діяльність правоохоронних органів стала предметом досліджень як вітчизняних, так і зарубіжних науковців. Зокрема, окремі аспекти цифровізації, використання електронних доказів та правових ризиків застосування ШІ розглядалися у працях В. Шепітька, О. Стрільцевої, Г. Авдєєвої, Е. Живуцької-Кожловської, М. Чайковського, а також у дослідженнях О. Герасименко, В. Артемова, А. Колеснікова тощо.

Актуальність теми дослідження зумовлена як глобальним трендом на цифровізацію правоохоронної сфери, так і зростанням випадків кібератак на державні установи, зокрема під час збройної агресії росії проти України. З огляду на це, **метою статті** є дослідження впровадження штучного інтелекту у діяльність правоохоронних органів та характеристика появи нових ризиків у кіберпросторі. Незважаючи на значний потенціал технологій, необхідною умовою їх ефективного і безпечного застосування є створення цілісного нормативно-правового механізму, який забезпечуватиме баланс між безпекою, ефективністю та дотриманням прав людини.

Наукова новизна публікації полягає у визначенні правового статусу правоохоронних органів як одночасно суб'єктів і об'єктів забезпечення кібербезпеки, доведення їх подвійної природи та подвійної ролі у контексті впровадження штучного інтелекту у їх діяльність.

Методи дослідження. Основою дослідження слугував діалектичний підхід, який дозволив розглянути інтеграцію штучного інтелекту у діяльність правоохоронних органів як динамічне соціально-правове явище, що перебуває на перетині технологічного прогресу та правової регламентації. Системно-структурний аналіз застосовувався для розкриття взаємозв'язків між різними рівнями правового регулювання та механізмами кіберзахисту.

Виклад основного матеріалу. Цифровізація діяльності правоохоронних органів є одним з ключових напрямів трансформації сучасної системи правосуддя в Україні, а застосування технологій штучного інтелекту поступово змінює не лише функціональну, але й нормативно-правову архітектуру правоохоронної діяльності.

У науковому середовищі все частіше звертається увага на проблемні питання впровадження цифровізації у діяльність правоохоронних органів.

Цифрові інструменти відіграють все більшу роль у сфері виявлення злочинів, забезпечення інформаційної безпеки, охорони критичної інфраструктури. Водночас, існує на недостатність нормативного регулювання та відсутність належної підготовки кадрів для ефективного використання ШІ [1].

Електронні докази, попри свою зростаючу доказову вагу, часто не мають відповідного статусу у процесуальному

законодавстві, що унеможливлює їх повноцінне використання у кримінальному провадженні. Відповідно, зростає необхідність гармонізації вітчизняних норм з європейськими стандартами [2].

Так, навіть при постійному наголошенні зі сторони наукової спільноти на потенціалі використання ШІ для попередження злочинів, аналізу кримінальних даних, ідентифікації ризиків та передбачення загроз, одночасно вказується і на відсутність правових гарантій дотримання прав людини при застосуванні таких технологій, що створює ризики порушення принципу пропорційності та правової визначеності [3].

Науковці, досліджуючи юридичні аспекти використання ШІ в діяльності Національної поліції, зазначають, що чинне українське законодавство не охоплює ані процесуальні аспекти використання ШІ, ані механізми контролю за алгоритмічними рішеннями і, як наслідок, виникає потреба в оновленні законодавства та створенні нормативних актів, що регулюватимуть етичні та правові межі використання технологій у правоохоронній діяльності [4]. Зокрема, одним із напрямів використання ШІ в діяльності Національної поліції є аналіз відео з натільних камер поліцейських. Алгоритми автоматично визначають ситуації затримання, застосування сили чи неправомірної поведінки, що дозволяє не лише пришвидшити розгляд відеоматеріалів, але й запобігти зловживанням з боку самих правоохоронців. Іншим прикладом є автоматизація оформлення поліцейських рапортів, де системи штучного інтелекту підвищують якість документації, зменшуючи кількість мовних та правових помилок. Також активно застосовуються інтегровані аналітичні платформи, як-от бельгійська система «Focus», яка поєднує до півсотні баз даних і дозволяє оперативно формувати досьє на підозрюваних або учасників кримінальних справ. У практиці міжнародних розслідувань набуває поширення модель Retrieval Augmented Generation (RAG), здатна працювати з великими обсягами інформації та витягати релевантні дані з різноманітних джерел. Штучний інтелект також використовується у виявленні злочинів проти дітей: спеціальні алгоритми аналізують цифрові зображення та відео, ідентифікують повторювані візуальні елементи та формують бази даних для розслідування злочинів, пов'язаних із дитячою порнографією [5].

Особлива увага приділяється і питанням електронних доказів. Г. Авдєєва та Е. Живуцька-Кожловська провели порівняльний аналіз використання цифрових доказів у кримінальному процесі України та США. Автори дійшли висновку, що в Україні існує суттєвий брак нормативного забезпечення, що ускладнює ідентифікацію, фіксацію, зберігання та оцінку електронних джерел доказової інформації [6].

У червні 2024 року Міністерство цифрової трансформації України опублікувало Білу книгу з регулювання ШІ в Україні [7], що деталізує практичні кроки до законодавчої імплементації європейської моделі AI Act (Artificial Intelligence Act – регламент Європейського Союзу, який встановлює правила для розробки, впровадження та використання систем штучного інтелекту). Документ описує класифікацію ризиків, оцінку безпечності, етичні принципи та обов'язки розробників, постачальників і користувачів систем ШІ, і серед рекомендованих сфер використання ШІ згадується і правоохоронна сфера.

Слід зазначити, що велика кількість вітчизняних науковців висловлює позитивне відношення до використання ШІ у правоохоронній діяльності та прогнозує значний прогрес у діяльності правоохоронних органів за використання новітніх засобів ШІ.

Зокрема, представники наукової спільноти обґрунтовують, що алгоритми штучного інтелекту можуть ефективно використовуватися в межах кримінального провадження на стадіях попередження злочинів, досудового розслідування та судового розгляду. Звертається увага, що міжнародна практика підтверджує доцільність використання таких технологій задля забезпечення прав учасників процесу та зменшення навантаження на судову систему [8].

У наукових публікаціях, присвячених аналізу міжнародного та національного досвіду застосування ШІ в діяльності правоохоронних органів, автори наголошу-

ють на значному потенціалі ШІ у таких напрямах, як розпізнавання облич, аналіз відеоспостереження, прогнозування правопорушень, оперативно-розшукова діяльність [9].

Слід підкреслити і позитивні прогнози вчених на динаміку застосування ШІ у боротьбі з економічними злочинами, адже інтелектуальні системи дозволяють ефективно аналізувати великі обсяги фінансової інформації, виявляти аномалії та будувати прогностичні моделі, що сприяє попередженню фінансових махінацій. При цьому, важливим залишається питання етичного використання таких систем [10].

Розглядається і важливість ШІ у розслідуванні воєнних злочинів, скоєних росією проти України, а інтеграція ШІ значно підвищує ефективність розслідувань, особливо в умовах обмеженого людського ресурсу та великого обсягу доказової інформації. Водночас, вчені акцентують увагу на необхідності дотримання прав людини та недопущення упереджених рішень автоматизованих систем [11].

Втім, поряд із цими перевагами дедалі чіткіше окреслюються потенційні ризики, що супроводжують інтеграцію ШІ у правоохоронну систему. Одним із найбільш вагомих викликів є загроза кібербезпеці – адже чим вищий рівень автономності мають інтелектуальні системи, тим уразливішими вони стають до зовнішніх атак, маніпуляцій або внутрішніх збоїв. Ризики посилюються й тим, що багато таких систем інтегруються у критичну інфраструктуру держави: поліцейські бази даних, аналітичні платформи розвідки, системи реагування на надзвичайні ситуації. У разі компрометації або неправомірного втручання наслідки можуть бути не лише технічними, а й правовими та соціальними, аж до порушення прав людини. Тому необхідно розглядати питання використання ШІ у правоохоронній сфері не лише крізь призму ефективності, а й у контексті комплексного забезпечення цифрової безпеки.

2 грудня 2020 року Кабінет Міністрів України затвердив Концепцію розвитку штучного інтелекту в Україні [12], яка визначила напрями державної політики, терміни імплементації та ролі ключових стейкхолдерів у сфері ШІ. Це дозволило вперше сформулювати цілі: підтримка інновацій, формування інститутів регулювання, забезпечення прав людини та етичності систем ШІ.

Згідно даної Концепції передбачено комплексний підхід до формування державної політики в галузі ШІ на період до 2030 року. Основною метою є створення умов для сталого та безпечного розвитку штучного інтелекту, включаючи його гармонізацію з національними інтересами у сфері безпеки та відповідності міжнародним стандартам.

У рамках реалізації Концепції визначено низку пріоритетних сфер, у яких держава зосереджує зусилля: освіта і професійне навчання, наука, економіка, кібербезпека, інформаційна безпека, оборона, публічне управління, правове регулювання, етика та правосуддя. Особливе значення в цьому контексті має саме кібербезпека, оскільки з розвитком інтелектуальних технологій зростають і ризики, пов’язані з уразливістю інформаційних систем, критичної інфраструктури та державних цифрових платформ.

Основним завданням державної політики у сфері кібербезпеки у зв’язку з розвитком ШІ визначено забезпечення надійного захисту комунікаційних, інформаційних та технологічних систем, з особливим акцентом на захист операторів ключових послуг і об’єктів критичної інфраструктури. Це є необхідною умовою безперервного функціонування державного управління, захисту суспільства та безпеки громадян.

Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 [13] закріплює комплексну модель національної безпеки у цифровому просторі, в якій правоохоронні органи відіграють одночасно дві ключові ролі – як суб’єкти забезпечення кібербезпеки, так і як об’єкти, що потребують її захисту. Така подвійна природа визначає специфіку їхнього функціонування у сучасному безпековому середовищі.

З одного боку, Служба безпеки України та Національна поліція наділені повноваженнями з виявлення, попередження, припинення та розслідування кіберзлочи-

нів. Вони залучені до проведення контрозвідувальних, оперативно-розшукових та кримінально-процесуальних заходів у кіберпросторі, здійснюють інформаційний обмін із суб'єктами критичної інфраструктури, беруть участь у міжнародному співробітництві, формуванні аналітичних баз даних і реагуванні на інциденти. Це надає їм важливу роль у підтриманні інформаційної стабільності в державі та запобіганні гібридним загрозам.

Водночас, самі правоохоронні органи дедалі частіше стають мішенню для кіберзагроз. Їхні інформаційні системи, оперативні бази даних, інструменти спостереження і цифрової комунікації – це елементи, уразливі до атак, втручання або шкідливого програмного впливу. В умовах воєнної агресії з боку росії, коли інформаційна безпека стала компонентом національної оборони, захищеність цифрових платформ правоохоронних структур є не лише технічним, але й стратегічним питанням.

Така ситуація вимагає особливої моделі регулювання, де правоохоронні органи не просто реалізують функцію контролю, а одночасно повинні бути інтегровані у системи захисту критичної інфраструктури, мати доступ до національних індикаторів кіберзагроз і підпорядковуватись єдиним протоколам реагування. Закон прямо передбачає обов'язок усіх суб'єктів кібербезпеки здійснювати обмін інформацією, формувати спільні плани реагування та брати участь у національних центрах кіберзахисту. Таким чином, держава формує цілісну вертикаль безпеки, у якій правоохоронні органи є як її гарантом, так і ключовою ланкою, що потребує надійної охорони.

Комплексне вирішення проблем кібербезпеки у світлі впровадження ШІ, запропоноване згаданою вище Концепцією, передбачає здійснення низки конкретних кроків:

– вдосконалення чинного законодавства та створення сучасної нормативно-правової бази, яка дозволить імплементувати кращі світові практики у сфері кіберзахисту, включаючи стандарти європейського права та рекомендації міжнародних організацій;

– розробка інноваційних систем кібербезпеки, здатних до автономного виявлення, класифікації та нейтралізації кіберзагроз за допомогою методів штучного інтелекту. Зокрема, мова йде про алгоритмічні моделі, що в реальному часі приймають рішення щодо запобігання атакам та реагування на інциденти;

– вивчення правових та організаційних аспектів ліцензування іноземних технологій штучного інтелекту, що використовуються у сфері кіберзахисту, особливо в державному секторі, з метою уникнення технологічної залежності та забезпечення суверенітету у сфері цифрової безпеки;

– створення національних цифрових платформ та продуктів, які дозволять суттєво зменшити частку використання імпортного програмного забезпечення у сфері кібербезпеки органами державної влади.

– актуалізація національних стандартів у сфері інформаційної безпеки, включаючи вимоги до захисту державних інформаційних ресурсів, мобільних пристроїв, додатків, серверів, хмарних рішень та мереж. Цей процес повинен здійснюватися з урахуванням міжнародних стандартів, зокрема ISO 27001 та ISO/IEC 27032, що забезпечують відповідність європейським підходам до інформаційної безпеки [12].

Висновки. Правоохоронні органи України наразі функціонують у подвійній якості: з одного боку, вони є суб'єктами забезпечення національної кібербезпеки, а з іншого – потенційно уразливими об'єктами для цифрових атак, зловживань та втрат чутливої інформації. Такий подвійний статус вимагає системного переосмислення підходів до безпеки, зокрема створення цілісного національного механізму цифрового захисту критичної правоохоронної інфраструктури. Сучасне українське законодавство, попри певні позитивні тенденції, зокрема прийняття Концепції розвитку ШІ, не забезпечує належного правового режиму для безпечного, етичного і відповідального використання алгоритмів у сфері правоохоронної діяльності. Відсутність чітких нормативних засад, невизначеність критеріїв допустимості цифрових доказів створюють

певні загрози. Враховуючи ці обставини, доцільним є розроблення спеціального правового режиму застосування ШІ у правоохоронній діяльності, який передбачав би прозорі механізми підзвітності та незалежний контроль за використанням алгоритмів.

Список використаної літератури:

1. Herasymenko O, Artemov V, Kravtsev O, Yunin O, Fedorchuk Y. AI Use by Ukrainian Law Enforcement in Combating Crime at Critical Infrastructure Facilities. *Salud, Ciencia y Tecnología. Serie de Conferencias*. 2025.4:1318. doi.org/10.56294/sctconf20251318
2. Moisieiev, M., Kapuliak, V., Udovenko, V., Ovcharenko, R., & Voloshanivska, T. Enhancing the Management of Electronic Evidence in Ukraine's Criminal Justice System: Future Prospects. *Journal of Lifestyle and SDGs Review*. 2025. 5(2). doi.org/10.47172/2965-730X.SDGsReview.v5.n02.pe05576
3. Kolesnikov A. Artificial intelligence in crime prevention and investigation. *Scientific notes Series Law*.2023. № 15. P. 292-295. doi: 1. 10.36550/2522-9230-2023-15-292-295.
4. Striltsiv O., Fedorenko O. Problems of legal regulation of the use of artificial intelligence technologies by the National Police of Ukraine. *Scientific Journal of the National Academy of Internal Affair*. 2022. Vol. 27, No.1. P. 30-39. https://doi.org/10.56215/0122271.30
5. Мамедова Е.А., Войтушенко І.О. Новий рубіж поліцейської діяльності: засади використання штучного інтелекту Національної поліції України. Міжнародний досвід. Центральноукраїнський вісник права та публічного управління. 2024. № 4(8). С. 51–56
6. Avdeeva, G., & Żywucka-Kozlowska, E. Problems of Using Digital Evidence in Criminal Justice of Ukraine and the USA. *Theory and Practice of Forensic Science and Criminalistics.* 2023. 30(1). P. 126-143. https://doi.org/10.32353/khrife.1.2023.07.
7. Біла книга з регулювання ШІ в Україні: бачення Мінцифри. URL: https://thedigital.gov.ua/storage/uploads/files/page/community/docs/%D0%A0%D0%B5%D0%B3%D1%83%D0%BB%D1%8E%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F%20%D0%A8%D0%86.pdf (дата звернення: 05.05.2025р.)
8. Демура М.І. Перспективи застосування штучного інтелекту у галузі кримінального судочинства. *Юридичний науковий електронний журнал*. 2022. Вип. 5. С. 554–558
9. Зачек О., Дмитрик Ю., Сеник В. Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична*. 2023. № 3. С. 148-156.
10. Чайковський Д. Штучний інтелект як новий інструмент для боротьби із злочинами у сфері економіки. *Юридичний вісник*. 2023. № 6. С.335-342.
11. Shepitko V., Shepitko M., Latysh K., Kapustina M., & Demidova. Artificial intelligence in crime counteraction: From legal regulation to implementation. *Social & Legal Studios.* 2023. 7(1). P. 135-144. doi: 10.32518/sals1.2024.135.
12. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України № 1556-р від 02.12.2020. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення: 05.05.2025).
13. 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 (дата звернення: 03.05.2025).

Latkovska T. A., Marushak A. V. Integration of artificial intelligence into the activities of law enforcement bodies: risks in the context of cybersecurity

The scientific article is devoted to the study of the phenomenon of integration of artificial intelligence into the activities of law enforcement agencies of Ukraine, taking into account modern challenges in the field of digital transformation and cybersecurity. It is substantiated that the use of AI in the work of law enforcement agencies is not only a technological innovation, but also a legal, ethical and security problem that requires systemic analysis. Specific examples of the implementation of intelligent solutions in the practice of law enforcement agencies are analyzed, in particular in the field of video analytics, digital evidence processing, document workflow automation, predictive analytics of offenses and

investigation of crimes against children. The prospects for adapting such models as Retrieval Augmented Generation (RAG) in criminal proceedings are also studied.

As part of the scientific analysis, national regulatory and legal acts are considered, in particular the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine", the Concept of the Development of Artificial Intelligence in Ukraine until 2030 and documents of the Ministry of Digital Transformation of Ukraine. It was determined that the existing legislative framework is fragmentary, does not provide for proper regulation of the legal status of AI algorithms, does not provide for mechanisms of liability for their consequences, and requires unification with international standards, in particular ISO 27001 and ISO/IEC 27032.

The dual nature of the status of law enforcement agencies in the context of AI is emphasized: on the one hand, they are subjects of ensuring national cybersecurity, and on the other hand, they themselves act as objects to which the risks of digital threats apply. It was determined that comprehensive security requires not only updating the technical infrastructure, but also digital literacy of personnel, procedural control, and independent supervision of the use of algorithms in the public sector. The current state of implementation of AI in the activities of Ukrainian law enforcement agencies is outlined, and ways of harmonizing legal regulation with European practice, strengthening cybersecurity, and strengthening the protection of human rights in the digital age are considered.

Key words: *cybersecurity, artificial intelligence, law enforcement agencies, digitalization, National Police of Ukraine, cybercrime.*