

Тільки комплексний підхід зможе забезпечити гармонійний розвиток суспільства, де технології слугують благу людства, а права людини залишаються непорушними.

Список використаних джерел:

1. Кравчук С. Вплив штучного інтелекту на права людини та загальні рекомендації для сталого втілення. *Вісник Н У "Львівська політехніка". Серія: "Юридичні науки"*. 2024. № 3 (43).
2. Конвенція про захист прав людини і основоположних свобод. Верховна Рада України : офіц. портал. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text
3. Тимошенко Є. А. Правове забезпечення застосування штучного інтелекту в Україні: дис. д-ра. філос.: 081 Право. Київ, 2024.



Булавина С. Є.,
кандидат історичних наук, доцент
Волинський національний університет імені Лесі Українки
e-mail: bulavina.svitlana@vnu.edu.ua

Калиновська М. В.,
здобувачка вищої освіти
Волинський національний університет імені Лесі Українки
e-mail: kalynovska.mahdalena2023@vnu.edu.ua

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ: ЕТИЧНІ ТА ПРАВОВІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ПРАВ ЛЮДИНИ

Швидкий розвиток технологій штучного інтелекту (ШІ) зумовив їхнє широке застосування в різних сферах суспільного життя по всьому світу, зокрема в правоохоронній діяльності. В Україні розвиток ШІ є визначеним пріоритетом науково-технологічних досліджень, що закріплено на законодавчому рівні. Як член Спеціального комітету із штучного інтелекту при Раді Європи, у жовтні 2019 року Україна стала

учасником Рекомендацій Організації економічного співробітництва і розвитку з питань ШІ (*Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449) [2].

Попри значний потенціал у підвищенні ефективності правоохоронної діяльності, використання технологій ШІ породжує нові виклики у сфері захисту прав і свобод людини. Основними проблемами залишаються питання етичності та дотримання принципів верховенства права. Враховуючи ці аспекти, метою дослідження є аналіз етичних та правових аспектів, пов'язаних із застосуванням ШІ у сфері правоохоронної діяльності.

Можна виокремити кілька основних напрямків використання ШІ в правоохоронній діяльності: 1) предиктивна аналітика – використання алгоритмів машинного навчання для прогнозування злочинності у певних районах та в певний час (до прикладу, системи *Predictive Policing* у США та *National Data Analytics Solution* у Великій Британії, які аналізують дані про злочини для визначення скупчень злочинності); 2) системи розпізнавання обличч – технології, які дозволяють ідентифікувати осіб у натовпі або на записах з камер відеоспостереження, які активно впроваджуються у багатьох країнах світу для пошуку підозрюваних у скоєнні злочинів або зниклих безвісти осіб; 3) алгоритми оцінки ризиків – системи, які використовуються для оцінки ймовірності рецидиву, визначення розміру застави або винесення вироків (наприклад, система *COMPAS* у США, яка використовується для оцінки ризику повторного скоєння злочину підсудними); 4) аналітика великих даних – застосування алгоритмів для аналізу великих масивів інформації з метою виявлення

зв'язків між особами, подіями та об'єктами, які можуть мати значення для розслідування злочинів.

Інтеграція ІІІ у систему безпеки України є перспективним напрямом, проте вона вимагає значних інвестицій у цифрову інфраструктуру, законодавчих змін та адаптації технологій до місцевих реалій [1]. Очікується, що в майбутньому сфера застосування штучного інтелекту в правоохоронній діяльності розширюватиметься, охоплюючи нові розробки у сфері автоматизованого спостереження, аналізу поведінки, віртуальних помічників для слідчих та інших інструментів.

Використання ІІІ в правоохоронній сфері породжує низку етичних питань. Однією з проблем є алгоритмічна упередженість і дискримінація. Оскільки системи ІІІ навчаються на попередніх даних, які можуть містити дискримінаційні практики, це може призвести до упереджених висновків. Наприклад, якщо певні райони міст традиційно підлягали інтенсивнішому патрулюванню, алгоритми предиктивної аналітики можуть відтворювати такі тенденції, посилюючи нерівність у правозастосуванні.

Ще однією важливою проблемою є прозорість алгоритмів. Багато сучасних моделей ІІІ, особливо нейронні мережі, функціонують за принципом «чорної скриньки», що ускладнює розуміння логіки ухвалення рішень. Це може створювати проблеми у забезпеченні справедливого судочинства, адже обвинувачені та їхні захисники можуть не мати змоги ефективно оскаржити висновки системи.

Додаткові виклики, пов'язані із застосуванням ІІІ в правоохоронній діяльності, включають **автоматизоване спостереження та приватність**. Масове впровадження систем

розпізнавання обличчя та інших технологій моніторингу може спричинити формування «суспільства під наглядом», де кожен крок громадян постійно відстежується. Окрім того, використання автоматизованих систем може ускладнювати визначення відповідальних осіб у разі помилкових рішень – розробників алгоритмів, операторів або кінцевих користувачів.

У Європі до використання ШІ в правоохоронній діяльності підходять обережно, надаючи пріоритет конфіденційності та дотриманню етичних норм. Наприклад, у Німеччині система *PRECOBS* аналізує дані про злочини для прогнозування потенційних загроз, проте її робота суворо регулюється нормами GDPR (*General Data Protection Regulation*) [3], які забезпечують контроль над обробкою персональних даних. Це демонструє можливість впровадження інноваційних технологій із дотриманням прав людини та запобіганням зловживанням.

З правової точки зору, ефективне регулювання застосування ШІ в правоохоронній діяльності має вирішити такі питання:

1. Захист права на приватність та персональні дані. Правоохоронні органи повинні дотримуватися принципів необхідності та пропорційності під час збору й обробки персональних даних, встановлюючи чіткі межі використання такої інформації.

2. Забезпечення справедливого судочинства. Використання алгоритмів оцінки ризиків та інших рішень ШІ не повинно порушувати презумпцію невинуватості та право на ефективний захист.

3. Протидія дискримінації. Правове регулювання має передбачати механізми перевірки алгоритмів на наявність

упередженості, а також інструменти виправлення можливих порушень.

4. Підзвітність та можливість оскарження. Громадяни повинні мати право оскаржувати рішення, ухвалені автоматизованими системами, та отримувати ефективний правовий захист.

Використання технологій ШІ у правоохоронній діяльності має потенціал підвищити ефективність боротьби зі злочинністю та забезпечення громадської безпеки. Однак їхнє впровадження створює нові виклики у сфері захисту прав і свобод людини. Для досягнення балансу між ефективністю правоохоронної діяльності та дотриманням прав людини необхідно розробити комплексне правове регулювання. Воно повинно встановлювати чіткі вимоги до розробки, впровадження та використання технологій ШІ, гарантувати їхню прозорість і підзвітність, а також забезпечувати механізми захисту прав громадян. Основними принципами такого регулювання мають стати людський контроль над автоматизованими системами, недискримінаційність, прозорість, підзвітність та пропорційність використання ШІ у правоохоронній діяльності.

Список використаних джерел:

1. Моргунова Т. І. Використання штучного інтелекту в правоохоронній діяльності. *Наукові інновації та передові технології*. № 2 (42). 2025. [https://doi.org/10.52058/2786-5274-2025-2\(42\)-638-652](https://doi.org/10.52058/2786-5274-2025-2(42)-638-652)

2. Про схвалення Концепції розвитку штучного інтелекту в Україні : розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. Кабінет Міністрів України: офіційний сайт. URL: <https://www.kmu.gov.ua/npas/pro-shvalennya-koncepciyi-rozvitku-shtuchnogo-intelektu-v-ukrayini-s21220>

3. General Data Protection Regulation / GDPR. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27.04.2016. URL:



Мельник Д. С.,
к.ю.н., старший дослідник,
науково-організаційний центр НА СБУ (м. Київ)

ЗНАЧЕННЯ ПРАКТИКИ ЄВРОПЕЙСЬКОГО СУДУ З ПРАВ ЛЮДИНИ ЩОДО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ДЛЯ УКРАЇНИ

Демократичні держави наразі вимушені розробляти й упроваджувати нові правові механізми, здатні адекватно регулювати відносини у сфері обігу й обробки конфіденційних даних про особу, зважаючи на стрімкий розвиток новітніх інформаційних технологій у світі.

Вказане пов'язане, насамперед з тим, що право людини на недоторканність приватного життя (включно із захистом її персональних даних) є однією з фундаментальних засад, які гарантують демократичну взаємодію між державою, суспільством і особою.

Україна вже доєдналася до низки міжнародно-правових актів у цій сфері, а Конституція нашої держави визначила найвищими соціальними цінностями людину, її життя й здоров'я, честь та гідність, а також недоторканність і безпеку. Зараз у правовому полі України використано типове європейське правове розуміння персональних даних, існує відповідна дефініція.