

**Яровий Кирило Васильович**

*кандидат юридичних наук, старший викладач  
кафедри інформаційних технологій та  
кібербезпеки ННІ №1 НАВС, капітан поліції*

## **МІЖНАРОДНИЙ ДОСВІД ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В УМОВАХ ВОЄННОГО СТАНУ**

У сучасному світі інформаційні технології стають невід'ємною частиною нашого повсякденного життя, які відіграють ключову роль у вирішенні складних завдань та оптимізують різноманітні процеси. Збільшення темпів інноваційних розробок спонукає до появи новітніх векторів вдосконалення у різних сферах життєдіяльності: медицині, промисловості, освіті, фінансах та правоохоронній діяльності.

Безумовно, вдосконалення правоохоронної системи та підвищення продуктивності протидії злочинності повинні здійснюватися за допомогою сучасних інформаційних технологій. Зокрема, штучний інтелект (надалі-ШІ) став звичайним явищем у діяльності правоохоронних органів, який широко використовується як інструмент протидії злочинності, відкриваючи перед нами нові сучасні можливості.

Теоретичні та практичні аспекти пов'язані з питаннями використання технологій ШІ були предметом чисельних досліджень. Проте, порушене питання потребує подальшого дослідження з метою розробки новітніх підходів та удосконалення нормативно-правової бази для ефективного використання технологій ШІ у ході розслідування та розкриття злочинів.

Багато досліджень, включаючи роботи Ezzeddine, Bayerl та Gibson [1, с. 863-864] дотримуються спільного напрямку використання поліцією можливостей ШІ цілей безпеки. Однак громадяни часто усвідомлюють і обережно ставляться до передових поліцейських можливостей, які можуть негативно вплинути на сприйняття легітимності поліцейських зусиль і поліції загалом. У цій роботі досліджуються суб'єктивні погляди громадян на використання ШІ поліцією, включаючи суперечності між безпекою, конфіденційністю та опором.

Elsherif [2, с. 347-349] стверджує, що протидія злочинності є необхідною та життєво важливою справою, яка оновлюється та розвивається відповідно до реальності свого суспільства, і водночас не опускається завеса юридичних теорій, які завжди приховували злочинця, іноді аналізуючи його. психологічно, іноді соціально, а іноді біологічно, щоб оцінити його кримінальну серйозність і застосувати відповідні заходи для запобігання його повернення до злочину. Знову ж таки, алгоритми, які є основою ШІ, виконують завдання точніше, швидше та дешевше. Однак новизна цього способу додала певної неоднозначності у визначенні його правової природи та законності.

Sachoulidou [3] приділяє увагу інструментам і технологіям, керованим ШІ, які використовуються на стадіях попереднього розслідування чи в рамках кримінального провадження, щоб декодувати людську поведінку та полегшити прийняття рішень щодо того, кого розслідувати, заарештовувати, переслідувати та, зрештою, покарати. Насамперед підкреслює існування постійної дилеми між метою підвищення оперативної ефективності поліції та судових органів та метою захисту основних прав постраждалих осіб. Крім того, наводяться аргументи на користь перегляду сфери захисту ключових фундаментальних прав, враховуючи, серед іншого, нові виміри, яких набула підозра.

Trifonov, Nakov та Mladenov [4] спрямовують дослідження на застосуванням інтелектуальних методів для підвищення безпеки в комп'ютерних мережах. Аналіз здійсненності різних методів ШІ показав, що метод, який однаково ефективний на всіх етапах кіберінтелекту, не може бути ідентифікований. У той час як для тактичної розвідки про кіберзагрози було вибрано та експериментовано багатоагентну систему, повторювані нейронні мережі пропонуються для потреб оперативної розвідки про кіберзагрози.

Tabi, Hewage, Bakhsh та Ukwandu [5, с. 104-105] досліджують підходи, натхненні ШІ, які використовує поліція для захисту дітей в Інтернеті. Розглянуті підходи є успішними в більшості ситуацій, але мають свої недоліки. Таким чином, усі зацікавлені сторони в сфері захисту дітей потребують такого розгляду. Крім цього, автори розглядають одностороннє використання ШІ для прогнозування та виявлення зловживань в Інтернеті на відміну від особистого розслідування та втручання.

Ismail, Muhammad, та Mosali [6, с. 161-162] представлено дослідження рейтингу 27 виявлених факторів, пов'язаних з інноваціями, які впливають на представлено дослідження рейтингу 27 виявлених факторів, пов'язаних з інноваціями, які впливають на продуктивність ШІ в ОАЕ. Зазначені фактори були згруповані в чотири групи, а саме інновації процесу; управлінські можливості; особистий досвід та організаційна структура. Дослідження також виявило, що два фактори, якими є управлінські можливості та ШІ, сильно впливають на ефективність організації, тоді як інші три фактори, які обробляють інновації, особистий досвід і організаційну структуру, помірно впливають на ефективність організації в ОАЕ. Результати цього дослідження дозволять краще зрозуміти фактори, пов'язані з інноваціями, і те, як вони впливають на загальну продуктивність ШІ в ОАЕ.

Becker, S., Neuschkel M., Richter S. та Labudde D. [7, с. 176-177] дійшли спільного висновку, що під час судового переслідування основною метою є довести кримінальні правопорушення правильному винному, щоб засудити його на законну силу. Однак насправді цього може бути важко досягти. Зважаючи на місце скоєння злочину, можна припустити, що наявні достатні записи з камер відеоспостереження, які зафіксували злочинця на місці злочину.

Традиційні підходи та методи дослідження, такі як розпізнавання обличчя та аналіз ходи, швидко досягають своїх меж.

Gans-Combe С. [8] зосереджується на дослідженні використання ШІ у сфері права. Автор вважає, що робота слідчих і суддів може бути полегшена за допомогою цих інструментів, зокрема щодо пошуку доказів під час слідчого процесу або підготовки правових висновків, панорама поточного використання далеко не райдужна, оскільки вона часто суперечить реальність польового використання та викликає серйозні питання щодо прав людини. Однак зазначені елементи погано розуміються юридичним світом і можуть призвести до неправильного використання. Тому, виникає потреба визначити як користувачів штучного інтелекту в галузі права, так і способи його використання, а також потреба в прозорості, правила та контури якої ще належить встановити.

Розбіжності поглядів у тлумаченні визначення «штучний інтелект», відсутність належного правове регулювання у галузі кібербезпеки, а також недостатній рівень інформаційної освіченості користувачів цифрових пристроїв призводить до збільшення кібератак та витоку персональних даних. Зазначене свідчить про необхідність впровадження новітніх підходів щодо використання зазначеної технології та створення ефективних правових механізмів для захисту інформації. Таким чином, використання технологій ШІ повинно стати потужним інструментом у руках правоохоронних органів для протидії злочинності.

Крім цього, на нашу думку, вважаємо, що з метою вирішення зазначеної проблематики необхідно систематизувати існуючі підходів щодо можливостей використання технологій штучного інтелекту правоохоронними органами, акцентуючи увагу на міжнародному досвіді протидії злочинності. Зазначене дозволить забезпечити належний контроль та захист в контексті використання ШІ правоохоронними органами у ході проведення судово-експертної діяльності та досудового розслідування.

Таким чином, зосередження уваги на використанні правоохоронним органам ШІ допоможе безпечно та ефективно протидіяти злочинності, а також перейти до нового етапу розвитку стійкого цифрового майбутнього.

#### **Список використаних джерел:**

1. Ezzeddine, Y., Bayerl, P. S., & Gibson, H. (2023). Safety, privacy, or both: Evaluating citizens' perspectives around artificial intelligence use by police forces. *Policing and Society*, doi:10.1080/10439463.2023.2211813.
2. Elsherif, M.S.A. The Legal Nature and Legality of Crime Prediction by Artificial Intelligence (2021) *Arab Journal of Forensic Sciences and Forensic Medicine*, 3 (2), pp. 341-359. DOI: 10.26735/NGSO4969.
3. Sachoulidou, A. (2023). Going beyond the “common suspects”: To be presumed innocent in the era of algorithms, big data and artificial intelligence. *Artificial Intelligence and Law*, doi:10.1007/s10506-023-09347-w.

4. Trifonov, R., Nakov, O., Mladenov, V. (2019) Artificial intelligence in cyber threats intelligence. International Conference on Intelligent and Innovative Computing Applications, ICONIC 2018, art. no. 8601235, Cited 10 times. DOI: 10.1109/ICONIC.2018.8601235.

5. Tabi, C., Hewage, C., Bakhsh, S. T., & Ukwandu, E. (2023). Contemporary issues in child protection: Police use of artificial intelligence for online child protection in the UK doi:10.1007/978-3-031-09691-4\_5 Retrieved from [www.scopus.com](http://www.scopus.com).

6. Ismail, J.I.M.S., Muhammad, M.N., Mosali, N.A. Ranking of Innovation Related Factors Influencing Artificial Intelligence Performance (2022) International Journal of Sustainable Construction Engineering and Technology, 13 (4), pp. 154-164. DOI: 10.30880/ijscet.2022.13.04.013.

7. Becker, S., Heuschkel, M., Richter, S., & Labudde, D. (2022). COMBI: Artificial intelligence for computer-based forensic analysis of persons. KI - Kunstliche Intelligenz, 36 (2), 171-180. doi:10.1007/s13218-022-00761-x.

8. Gans-Combe, C. (2022). Automated justice: Issues, benefits and risks in the use of artificial intelligence and its algorithms in access to justice and law enforcement doi:10.1007/978-3-031-15746-2\_14 Retrieved from [www.scopus.com](http://www.scopus.com).