

Позитивні приклади застосування штучного інтелекту для попередження та розслідування злочинів

Роман Сушко

головний судовий експерт, Дніпропетровський науково-дослідний експертно-криміналістичний центр МВС України, м. Дніпро, Україна, e-mail: ronboss@ukr.net

Розглянуто застосування штучного інтелекту в провідних державах світу для попередження та розслідування злочинів, а також юридичні особливості такого застосування.

Ключові слова: штучний інтелект; застосування штучного інтелекту; спрощення роботи; допомога в розслідуванні; юридичні норми.

Best Practices of Artificial Intelligence Application for Prevention and Investigation of Crimes

Roman Sushko

The paper outlines the application of artificial intelligence in the world's leading countries for prevention and investigation of crimes as well as legal peculiarities of such application.

Keywords: artificial intelligence; artificial intelligence application; simplification of work; assistance in investigation; legal rules.

Можна довго обговорювати актуальність теми застосування штучного інтелекту (далі — ШІ) для допомоги в попередженні й розслідуванні злочинів, але найкраще це ілюструє успішне послуговування ШІ у правоохоронній діяльності країн — лідерів із розвитку ШІ, а саме США, Китаю, країн Євросоюзу та Великої Британії.

У США ШІ активно застосовують для розслідування злочинів і підтримання діяльності правоохоронних органів. Він допомагає не лише прискорити аналіз значних обсягів даних, а й підвищує ефективність розслідувань. Наведімо кілька прикладів послуговування ШІ у сфері кримінального правосуддя в США.

1. *Розпізнавання облич.* Поліція активно застосовує алгоритми розпізнавання облич для ідентифікації підозрюваних за фотографіями або відеозаписами з камер спостереження. Система порівнює обличчя з мільйонами зображень із соціальних мереж, новинних сайтів та інших джерел в інтернеті, що дає змогу швидко знайти підозрюваних і відстежити їх пересування (програма *Clearview AI*).

2. *Аналіз відеоматеріалів.* Правоохоронні органи послуговуються ШІ для швидкого аналізу годин відеозаписів з камер спостереження (платформа *BriefCam*). ШІ виокремлює важливі події, транспортні засо-

би або людей, що допомагає слідчим оперативно знаходити потрібні фрагменти відео. Наприклад, систему *BriefCam* застосовували для розслідування терористичної атаки на Бостонський марафон у 2013 р.

3. *Аналіз значних обсягів даних і прогнозування злочинів.* На підставі аналізування алгоритмами машинного навчання історичних даних про злочини (місце, час, тип правопорушень) *PredPol* (англ. *Predictive Policing*) допомагає поліції патрулювати райони, де ймовірність скоєння злочинів є найвищою [1—2]. Цю систему впроваджено в багатьох містах США з метою раціоналізувати розподіл поліцейських ресурсів.

4. *Цифрова криміналістика* (англ. *Digital Forensics*). Федеральне бюро розслідувань (англ. *Federal Bureau of Investigation, FBI*) активно використовує ШІ для опрацювання цифрових доказів (даних із мобільних телефонів, соціальних мереж та електронної пошти). Наприклад, під час розслідування кібератак або фінансових злочинів ШІ аналізує значні обсяги даних і знаходить зв'язки між підозрюваними та злочинними діями.

5. *ШІ для аналізу почерку й голосу.* ФБР та інші правоохоронні органи застосовують ШІ для аналізу почерку або голосових записів із метою ідентифікувати авторів листів або дзвінків, які пов'язані зі злочинами. Це стало у пригоді у справах, де злочинці надавали фальшиві документи або анонімно телефонували з погрозами.

6. *Аналіз тексту та природної мови* (англ. *Natural language*

processing, NLP). Компанії *DataRobot* і *Palantir* розробили інструменти, які допомагають аналізувати мільйони документів, допитів або електронної кореспонденції за допомогою алгоритмів опрацювання природної мови. Ці системи дають змогу швидко виявляти потенційні докази, спрощуючи роботу слідчих.

7. *Розслідування фінансових злочинів.* ШІ застосовують для виявлення аномальних фінансових транзакцій. Наприклад, ШІ відстежує рух коштів між різними банківськими рахунками для виявлення підозрілих операцій, що сприяє ідентифікації схем відмивання грошей або фінансування тероризму.

8. *Аналіз ДНК і доказів.* ШІ допомагає під час аналізу складних зразків ДНК, включно з давніми та складними зразками. Наприклад, у Нью-Йорку та інших містах США застосовують алгоритми для розподілу зразків, які містять ДНК кількох осіб, що значно покращує якість розслідувань.

9. *Генерація текстових описів подій на відео.* У межах одного з проєктів Університету Центральної Флориди, алгоритми ШІ розпізнають дії на відео, що допомагає відслідковувати й аналізувати події без утручання людини [3], оскільки оператори-люди фізично не в змозі контролювати кілька сотень камер. У разі стрілянини або дорожньої аварії ШІ одразу сповіщає про це оператора, а той негайно вживає заходів з надання допомоги потерпілим і затримання правопорушника.

Іще одним світовим лідером у застосуванні ШІ у правоохоронній

діяльності є Китай, який має найбільшу мережу камер спостереження у світі, інтегровану з ШІ для розпізнавання облич і повсюдного відеоспостереження для моніторингу громадян та виявлення злочинців. Окрім того, у Китаї діють масштабні державні програми з впровадження ШІ й автоматизації в судову систему, там активно застосовують блокчейн для відстеження цифрових доказів, що гарантує їх автентичність.

У Великій Британії застосування ШІ зосереджено на аналізі цифрових доказів і кіберзлочинах. Наприклад, *Metropolitan Police* послуговується ШІ для розслідування серйозних злочинів (кіберзлочинів і шахрайства). ШІ також допомагає правоохоронцям аналізувати значні обсяги даних з камер спостереження, фінансових операцій і соціальних мереж. Важливим аспектом застосування таких технологій є захист прав людини, наприклад відповідність *GDPR* (англ. *General Data Protection Regulation* — правовий акт, що регулює опрацювання персональних даних, включно із застосуванням із судово-експертною метою).

У країнах ЄС застосування ШІ врегульовано більш суворими правилами, особливо щодо захисту даних і конфіденційності громадян. Запроваджують розумні системи прогнозування злочинів та аналітичні інструменти для боротьби з фінансовими злочинами. Водночас технології розпізнавання облич (активно застосовувані в США та Китаї) у багатьох країнах ЄС заборонені через мож-

ливі порушення прав людини. Окрім того, країни Євросоюзу розробляють пілотні проекти зі створення автоматизованих систем аналізу доказів.

Можна дійти висновку про те, що США та Китай є лідерами у застосуванні ШІ у правоохоронній діяльності для масового моніторингу, але підходи в Китаї більшою мірою орієнтовані на тотальний контроль, тоді як у США робиться акцент на захист від злочинів і кібербезпеку. Ці дві країни мають потужні національні програми [4—5] для розвитку ШІ в галузі запобігання злочинам і їх розслідування. Окрім того, у США кожний штат може впроваджувати власні платформи й різноманітні алгоритми для застосування ШІ на варті правопорядку, що є потужним каталізатором для його розвитку та апробації.

ЄС і Велика Британія регулюють ШІ жорсткіше, з акцентом на захист конфіденційності, оскільки спільно прийняті членами ЄС нормативно-правові акти суворо забороняють утручатися в особисте життя громадян [6].

Хоча кожний із наведених прикладів має певні недоліки й помилки, а деякі платформи — запеклих опонентів, ШІ й алгоритми машинного навчання активно розвиваються, стають більш точними та значно спрощують роботу правоохоронних органів у розслідуванні злочинів і правопорушень та запобіганні їм. Сподіватимемося, що напрацьований передовими країнами досвід застосування ШІ в судово-експертній і правоохоронній діяльності найближчим часом стане звичним і в нашій державі.

Перелік джерел посилання

1. Perry W. L., McInnis B., Price C. C., Smith S., Hollywood J. S. Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations. RAND Corporation, 2013. 186 p. URL: <https://www.jstor.org/stable/10.7249/j.ctt4cgdcz> (дата звернення: 03.10.2024).
2. Ibidem. Predictive Policing. Forecasting Crime for Law Enforcement / RAND. Oct 14, 2013. URL: http://www.rand.org/pubs/research_briefs/RB9735.html (дата звернення: 03.10.2024).
3. Rigano Ch. Using Artificial Intelligence to Address Criminal Justice Needs / National Institute of Justice. Oct 8, 2018. URL: <https://nij.ojp.gov/topics/articles/using-artificial-intelligence-address-criminal-justice-needs> (дата звернення: 04.10.2024).
4. National Artificial Intelligence Initiative (NAII) / Ai.gov. URL: <http://Ai.gov> (дата звернення: 05.10.2024).
5. Webster G., Creemers R., Kania E., Triolo P. Full Translation: China's 'New Generation Artificial Intelligence Development Plan' / DIGICHINA. Aug 1, 2017. URL: <https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/> (дата звернення: 05.10.2024).
6. Загальний регламент про захист даних (GPDR) / GPDR Text. URL: <https://gdpr-text.com/uk/> (дата звернення: 06.10.2024).