6. Рішення Конституційного Суду України у справі за конституційними скаргами Ковтун Марини Анатоліївни, Савченко Надії Вікторівни, Костоглодова Ігоря Дмитровича, Чорнобука Валерія Івановича щодо відповідності Конституції України (конституційності) положення частини п'ятої статті 176 Кримінального процесуального кодексу України № 7-р/2019 від 25.06.2019. URL: https://zakon.rada.gov.ua/laws/show/v007p710-19#n2

7. Висновок Головного науково-експертного управління Верховної Ради України на проект Закону України «Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо удосконалення відповідальності за колабораційну діяльність та особливості застосування запобіжних заходів за вчинення злочинів проти основ національної та громадської безпеки». URL: https://itd.rada.gov.ua/billInfo/Bills/pubFile/1247684

8. Зауваження Головного юридичного управління Апарату Верховної Ради України до проекту Закону України «Про внесення змін до Кримінального процесуального кодексу України щодо обрання запобіжного заходу до військовослужбовців, які вчинили військові злочини під час дії воєнного стану» (реєстраційний № 7431). URL: https://itd.rada.gov.ua/billInfo/Bills/pubFile/1437101

9. Висновок Головного науково-експертного управління на проект Закону України «Про внесення змін до Кримінального процесуального кодексу України (щодо обрання запобіжного заходу до військовослужбовців, які вчинили військові злочини під час дії воєнного стану)». URL: https://itd.rada.gov.ua/billInfo/Bills/pubFile/1350834

10. Конституція України від 28.06.1996 р. № 254к/96-ВР. *Верховна Рада України*. URL: http://zakon4.rada.gov.ua/laws/show/3477-15

11. Про введення воєнного стану: Указ Президента України від 24.02.2002 № 64/2022 : затв. Законом України від 24 лютого 2022 року № 2102-IX. URL: https://zakon.rada.gov.ua/laws/show/64/2022#n2

12. Інформація про відступ України від зобов'язань за Конвенцією про захист прав людини і основоположних свобод: заява Постійного представництва України при Раді Європи № 31011/32-017-3 від 28.02.2022 р. URL: https://rm.coe.int/1680a5b0b0

13. Гловюк І., Дроздов О., Тетерятник Г., Фоміна Т., Рогальська В., Завтур В. Особливий режим досудового розслідування, судового розгляду в умовах воєнного стану: науково-практичний коментар Розділу IX-1 Кримінального процесуального кодексу України. Вид. 4-е. Електронне видання (станом на 30 грудня 2022 р.). Дніпро-Львів-Одеса-Харків, 2023. 82 с. URL: https://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/16123/_Osoblyvyi%20rezhym%20dosudovoho%20rozsliduvannia_4_2022.pdf?sequence=3&isAllowed=y

14. Фоміна Т. Г., Рогальська В. В. Особливості застосування запобіжних заходів в умовах воєнного стану. The Russian-Ukrainian war (2014–2022): historical, political, cultural-educational, religious, economic, and legal aspects : Scientific monograph. Riga, Latvia : "Baltija Publishing", 2022. С. 1289–1297. URL: http://baltijapublishing.lv/omp/index.php/bp/catalog/view/237/6381/13417-1

15. Рішення Європейського суду з прав людини по справі «Харченко проти України» («Kharchenko v. Ukraine»), заява № 40107/02 від 10 лютого 2011 року. URL: http://zakon5.rada.gov.ua/laws/show/974_662

16. Рішення Європейського суду з прав людини у справі «Хайредінов проти України» («Khayredinov v. Ukraine»). заява № 38717/04 від 14 жовтня 2010 року. URL: https://zakon.rada.gov.ua/laws/show/974_665.

УДК 343.85
DOI: 10.31733/15-03-2024/1/632-636

Дмитро САНАКОЄВ
завідувач кафедри кримінального процесу та стратегічних розслідувань Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук, доцент

ПЕРСПЕКТИВНІ НАПРЯМИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ПРОГНОЗУВАННІ ТА ПРОТИДІЇ ЗЛОЧИННОСТІ

Останні тенденції в методах роботи злочинних угруповань з технологічним підходом, які займаються торгівлею незаконними товарами (наприклад, вогнепальною зброєю, наркотиками, культурними цінностями тощо), спричинили серйозні проблеми у секторі безпеки. Представники організованих злочинних об'єднань активно використовують криптовалютні платежі, 3D-друк, можливості соціальних медіа та DarkWeb, що призводить до нелегальних і

неконтрольованих державою транзакцій, надаючи нові бізнес-можливості для злочинців. Наведене зумовило розробку та ухвалення нормативно-правових актів щодо можливостей використання штучного інтелекту (*Далі – ШІ. Д.С.*), у т.ч. й у протидії злочинності.

Тож основними нормативними актами, що регулюють впровадження ШІ в діяльність правоохоронних органів ЄС, є Загальний регламент захисту даних (GDPR), Хартія основних прав ЄС та Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних. Окреслені у вказаних документах правила спрямовані на забезпечення етичного та законного використання технологій ШІ в правоохоронній діяльності, одночасно захищаючи права та конфіденційність осіб. Згідно з Загальним регламентом захисту даних (GDPR), використання ШІ, зокрема алгоритмів машинного навчання (ML), повинно дотримуватися принципів прозорості та відповідальності. Це означає, що організації, які використовують ШІ для обробки персональних даних, повинні забезпечити доступність і зрозумілість алгоритмів, вжити заходів для запобігання дискримінації та недопущення несправедливого впливу на особу. Головна мета полягає в тому, щоб забезпечувати права на конфіденційність та приватність громадян у цифрову епоху [1].

Відповідно до Етичної хартії щодо використання штучного інтелекту в судовій системі, коли йдеться про кримінальне провадження, найважливішими принципами визначено [2]: а) принцип поваги основних прав: забезпечення сумісності інструментів і послуг ШІ з основними правами людини; б) принцип недискримінації: недопущення порушення принципу рівності суб'єктів або груп; в) принцип якості та безпеки: це стосується обробки судових рішень та даних; з моделями в безпечному технологічному середовищі використовуються сертифіковані джерела інформації та дані; г) принцип об'єктивності та справедливості: забезпечення наявності та зрозумілості методів обробки даних, можливість проведення зовнішнього аудиту; д) принцип контролю користувача: виключення директивного підходу та забезпечення того, щоб користувачі були поінформовані та контролювали свій вибір.

Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних визначає, що при використанні ШІ необхідно дотримуватися принципів законності, справедливості та прозорості в обробці даних. Також важливо забезпечити цільове обмеження при зборі та обробці даних ШІ, щоб уникнути недискримінації та порушення прав людини. Крім того, Конвенція наголошує на важливості забезпечення безпечності та конфіденційності обробки персональних даних в контексті ШІ [3].

У Концепції розвитку штучного інтелекту в Україні зазначено, що впровадження технології ШІ є, серед іншого, невід'ємною складовою розвитку науково-технічної, оборонної, правової діяльності у сферах загальнодержавного значення [4]. Серед пріоритетів реалізації концептуальних засад державної політики в галузі штучного інтелекту – необхідність його застосування в судовій практиці; правове регулювання у сфері кібербезпеки та оборони; удосконалення законодавства про захист персональних даних; протидія спробам несанкціонованого втручання в роботу автоматизованих систем і комп'ютерних мереж; відповідність роботи систем ШІ законодавству та існуючим етичним принципам; розробка та використання систем ШІ лише за умови дотримання верховенства права, основоположних прав і свобод людини і громадянина, демократичних цінностей, а також забезпечення відповідних гарантій під час використання таких технологій; застосування технологій ШІ під час розроблення заходів ресоціалізації засуджених осіб та ризику скоєння повторного правопорушення, тощо [4].

Зазначимо, що ШІ у діяльності поліції сьогодні активно використовується для прогнозування злочинності за допомогою різних інструментів, таких як аналіз даних, машинне навчання, обробка природної мови та розпізнавання образів та ін. При використанні цих інструментів вдається аналізувати великі обсяги даних, виявляти зв'язки та шаблони, що допомагає передбачати майбутні злочинні події. У прогнозуванні злочинності використовуються різні інструменти та методи штучного інтелекту, включаючи:

1. Аналіз даних. Використання алгоритмів машинного навчання для обробки та аналізу великих обсягів даних, пов'язаних із злочинністю, дозволяє виявити тенденції, та, відповідно, вдосконалити стратегії боротьби зі злочинністю, превентивні заходи, прогнозування злочинної діяльності та виявлення злочинців. Такий підхід допомагає правоохоронним органам більш ефективно протидіяти злочинності та забезпечити безпеку громадян. Деякі з найпопулярніших інструментів цього типу такі:

1) IBM i2 Analyst's Notebook – це програмне забезпечення для візуалізації та аналізу розгортання інформації. Використовується правоохоронними органами, аналітиками

розвідки для виявлення прихованих зв'язків і шаблонів у даних. Це дозволяє користувачам імпортувати та аналізувати великі обсяги даних із різних джерел, наприклад телефонні записи, фінансові операції та активність у соціальних мережах [5]. Система має розширені можливості візуалізації даних, включаючи інтерактивні діаграми, графіки та часові шкали, щоб допомогти користувачам зрозуміти складні відносини та прийняти обґрунтовані рішення. Загалом IBM i2 Analyst's Notebook відомий своєю здатністю допомагати у складних розслідуваннях, зборі розвідувальних даних і процесах прийняття рішень, надаючи комплексну та інтуїтивно зрозумілу платформу для аналізу та візуалізації даних;

2) Palantir – це платформа для аналізу даних, яка допомагає знаходити зв'язки між різними видами даних. Використовується для інтелектуального аналізу, об'єднання і аналізу розвідувальних даних. Технологія Palantir використовується різними державними установами, фінансовими установами та іншими організаціями для таких завдань, як виявлення шахрайства, відстеження злочинців і аналіз тенденцій [6].

Palantir і IBM i2 Analyst's Notebook – це обидві потужні аналітичні системи, призначені для збору та аналізу великих обсягів даних для розвідки та безпеки. Однак, їх відрізняють підходи та функціонал. Palantir відомий своєю можливістю обробки неструктурованих даних та великим фокусом на антитерористичні і розвідувальні операції. З іншого боку, IBM i2 Analyst's Notebook зазвичай використовується для кримінального аналізу та дослідження. Різниця полягає в тому, які типи даних кожна система найкраще опрацьовує та аналізує;

3) Splunk – платформа для аналізу журналів та моніторингу в реальному часі [7]. У правоохоронних органах різних країн світу ця платформа використовується за такими напрямками: 1) розслідування та криміналістичні дослідження: правоохоронні органи можуть використовувати Splunk для збору та аналізу даних журналу з різних джерел, таких як веб-сервери, бази даних і мережеві пристрої, щоб відстежувати дії підозрюваних і збирати докази для кримінальних розслідувань; 2) моніторинг безпеки: Splunk можна використовувати для моніторингу мережевого трафіку, виявлення підозрілих дій і порушень безпеки та вжиття негайних заходів для запобігання кібератакам або витоку даних; 3) відповідність і аудит: правоохоронні органи можуть використовувати Splunk для забезпечення дотримання законів і правил захисту даних шляхом моніторингу та аналізу доступу до конфіденційних даних і створення звітів про аудит; 4) прогнозна поліція: Splunk може допомогти правоохоронним органам проаналізувати історичні дані про злочини, щоб виявити закономірності та тенденції, дозволяючи їм більш ефективно розподіляти ресурси та запобігати злочинам до того, як вони відбудуться; 5) операційна ефективність: Splunk також можна використовувати для оптимізації внутрішніх процесів, покращення часу реагування та підвищення загальної ефективності роботи правоохоронних органів.

Загалом Splunk дає правоохоронним органам потужний інструмент для аналізу та візуалізації даних, що дає їм змогу поліпшити свої розслідувальні можливості та підвищити громадську безпеку;

4) SAS – програмне забезпечення для аналізу даних та статистики. Застосування цього програмного забезпечення може мати кілька переваг для правоохоронних органів: 1) аналіз даних: SAS дозволяє ефективно та швидко аналізувати великі обсяги даних, що може бути корисним для розслідування злочинів та виявлення злочинців. 2) прогнозування: завдяки аналітичним можливостям SAS можна прогнозувати злочини та виявляти тенденції, що допомагає у запобіганні кримінальної діяльності. 3) візуалізація даних: SAS надає можливість побудови графіків та діаграм для кращого розуміння та візуалізації даних, що сприяє у виявленні зв'язків та закономірностей в злочинності. 4) безпека даних: SAS забезпечує високий рівень безпеки даних, що дозволяє зберігати конфіденційну інформацію без ризику її втрати або несанкціонованого доступу [8].

Ці інструменти допомагають поліції ефективно аналізувати та використовувати великі обсяги даних для розслідування у кримінальних провадженнях та забезпечення публічної безпеки і порядку.

2. Геоінформаційні системи (ГІС). ГІС дозволяють аналізувати злочинність на географічному рівні, визначаючи «гарячі точки» та передбачаючи потенційні зони злочинності. Наприклад, однією з таких відомих систем є CrimeStat [9]. Це програмний пакет для просторової статистики, спеціально розроблений для візуалізації та аналізу даних про злочини. Містить різні аналітичні інструменти, такі як аналіз найближчих сусідів і просторовий автокореляційний аналіз, щоб допомогти користувачам зрозуміти просторовий розподіл злочинів.

3. Прогностичне моделювання. Із використанням ШІ можна будувати математичні моделі злочинності та передбачати ймовірність вчинення злочинів у певних умовах. Прогностичне моделювання в правоохоронних органах може використовувати такі інструменти: *1) Predictive Policing Software; 2) Crime Mapping Tools; 3) Risk Assessment Models; 4) Sentiment Analysis Tools; 5) Computational Intelligence Algorithms* та ін.

4. Обробка природної мови (NLP). Аналіз текстових даних, таких як звіти про злочини та повідомлення в соціальних мережах, за допомогою NLP дозволяє отримувати інформацію про злочини та аналізувати їх. Є багато інструментів обробки природної мови (NLP), які можуть бути корисними для правоохоронних органів. Деякі з них містять: *1) системи аналізу тексту* – ці системи можуть допомогти автоматично виявляти та аналізувати свідчення, документи або повідомлення для розслідувань (наприклад, Veritone, Nuix); *2) системи мовної ідентифікації* – ці системи можуть допомогти визначити авторство текстів або анонімних повідомлень, що може бути корисним для розслідувань (голосові аналізатори, системи розпізнавання мовлення, оцінки спеціалістів); *3) машинне навчання для виявлення типовості та аномалій* – цей підхід може допомогти виявити підозрілі зв'язки або поведінку на основі аналізу текстової інформації (порушення публічного порядку, фінансові порушення, прогнозування злочинності); *4) системи пасивного моніторингу для виявлення загроз* – ці системи можуть автоматично відстежувати та аналізувати великі обсяги тексту для виявлення підозрілих або загрозливих виразів (відеоспостереження, моніторинг вебтрафіку, аналіз телефонних даних, моніторинг соціальних мереж). Загалом використання інструментів NLP може допомогти правоохоронним органам ефективніше аналізувати великі обсяги текстової інформації та виявляти потенційні загрози та злочини.

5. Відеоаналітика. Використання комп'ютерного зору для аналізу відеоматеріалів дозволяє виявляти злочини та запобігати їм. До таких інструментів в діяльності правоохоронних органах відносять: *1) оптичне розпізнавання символів (OCR):* автоматичне розпізнавання номерних знаків автомобілів або інших символів на відеозаписах для швидкого пошуку та ідентифікації; *2) виявлення об'єктів та осіб:* автоматичне виявлення підозрілих об'єктів або осіб на відеозаписах, що допомагає у попередженні злочинів або розслідуванні подій; *3) аналіз руху:* вивчення руху об'єктів на відеозаписах, допомагаючи правоохоронним органам у реконструкції подій та встановленні часової послідовності; *4) розпізнавання облич:* для розпізнавання облич на відеозаписах і порівнювання їх з базами даних для ідентифікації.

Загалом використання ШІ у роботі поліції є актуальною темою. Критика цих систем стосується окремих аспектів, таких як відсутність відповідальності, проблемні упередження у наборах даних, втручання в особисті права та поверховість. Деякі з головних проблем: 1) упередження та дискримінація; 2) обмежені дані та точність; 3) занепокоєння конфіденційністю; 4) відсутність прозорості; 5) етичні наслідки [10]. Аналогічні тенденції спостерігаємо і в системі кримінального судочинства.

Тож серед потенційних бар'єрів імплементації застосування ШІ у кримінальному процесі виокремлюють індивідуальні та системні. До першої групи відносять: 1) низьку обізнаність про ШІ; 2) низький рівень цифрової грамотності та навичок використання ШІ; 3) людський фактор (недоброчесність). До другої групи дослідники відносять: 1) технічні та технологічні бар'єри; 2) операційні бар'єри; 3) законодавчі бар'єри [11].

Проведений нами аналіз переваг та недоліків застосування систем ШІ у діяльності правоохоронних органів дозволив виокремити найбільш перспективні та пріоритетні напрями, зокрема: *1) аналіз даних:* штучний інтелект може використовуватися для аналізу великих обсягів даних про злочинність, що допомагає виявляти закономірності та тенденці; *2) прогнозування та моделювання:* за допомогою штучного інтелекту можна розробляти прогностичні моделі, які допомагають передбачати ризики злочинності у конкретних районах або в певний час; *3) виявлення відхилень та аномалій:* AI може допомогти розпізнати незвичайні моделі у злочинності, що дозволяє оперативно реагувати на потенційно небезпечні ситуації; *4) оптимізація ресурсів:* за допомогою штучного інтелекту можна ефективніше розподіляти поліцейські сили та інші ресурси для запобігання злочинності; *5) підтримка в прийнятті рішень:* AI може надавати аналітичну підтримку правоохоронним органам у процесі вирішення стратегічних питань у сфері боротьби зі злочинністю.

Ці та інші напрями повинні бути реалізовані, зокрема в межах забезпечення виконання таких загальнонаціональних завдань: 1) подальшого розвитку Єдиної судової інформаційно-телекомунікаційної системи, Електронного суду, Єдиного реєстру досудових розслідувань та доступу до них, тощо; 2) попередження кримінальних правопорушень

шляхом аналізу наявних даних за допомогою ШІ; 3) проведення аналізу даних за допомогою технологій ШІ з метою ресоціалізації засуджених; 4) винесення судових рішень у справах незначної складності (за взаємною згодою сторін) на основі результатів аналізу з використанням технологій ШІ, судової практики [4].

1. Загальний регламент про захист даних (GDPR). URL: https://gdpr-text.com/uk/ (дата звернення: 26.02.2024).
2. European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment. Adopted at the 31st plenary meeting of the CEPEJ (Strasbourg, 3-4 December 2018). URL: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c (дата звернення: 26.02.2024).
3. Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Страсбург, 28 січня 1981 року). URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення: 26.02.2024).
4. Концепція розвитку штучного інтелекту в Україні : Розпорядження Кабінету Міністрів України від 2 груд. 2020 р. № 1556-р. URL: https://www.kmu.gov.ua/npas/pro-shvalennya-koncepciyi-rozvitku-shtuchnogo-intelektu-v-ukrayini-s21220 (дата звернення: 26.02.2024).
5. i2 Analyst's Notebook : вебсайт. URL: https://i2group.com/i2-analysts-notebook
6. AI-Powered Operations, For Every Decision : вебсайт. URL: https://www.palantir.com/ (дата звернення: 26.02.2024).
7. Splunk : вебсайт. URL: https://www.splunk.com/ (дата звернення: 26.02.2024).
8. Analytics Software&Solutions : вебсайт. URL: https://www.sas.com/en_us/software/stat.html (дата звернення: 26.02.2024).
9. CrimeStat: Spatial Statistics Program for the Analysis of Crime Incident Locations : вебсайт. URL: https://nij.ojp.gov/topics/articles/crimestat-spatial-statistics-program-analysis-crime-incident-locations (дата звернення: 26.02.2024).
10. Dupont B., Stevens Y., Westermann H., Joyce M. Artificial Intelligence in the Context of Crime and Criminal Justice, Korean Institute of Criminology, Canada Research Chair in Cybersecurity, ICCC, Université de Montréal, 2018. URL: https://www.academia.edu/40999602/Artificial_Intelligence_in_the_Context_of_Crime_and_Criminal_Justice (дата звернення: 26.02.2024).
11. Перспективи та межі використання штучного інтелекту в кримінальному процесі: соціологічне дослідження. *Міжнародний фонд «Відродження». Прямуємо разом. Центр Дністрянського, Fama.Agency*. Київ, 2024. 57 с. URL: https://dc.org.ua/uploads/material/ai.pdf (дата звернення: 26.02.2024).

УДК 343.102
DOI: 10.31733/15-03-2024/1/636-638

Вікторія РОГАЛЬСЬКА
професор кафедри кримінального процесу та стратегічних розслідувань, кандидат юридичних наук, доцент

Артем РУДЕНКО
курсант ННІ права та підготовки фахівців для підрозділів Національної поліції Дніпропетровського державного університету внутрішніх справ

ШТУЧНИЙ ІНТЕЛЕКТ В ПРОЦЕСІ ЗДІЙСНЕННЯ ДОСУДОВОГО РОЗСЛІДУВАННЯ: МОЖЛИВОСТІ ТА ПРОБЛЕМАТИКА

Швидкоплинність розвитку сфери інформаційних технологій та послуг зумовлює потребу безперервної актуалізації своїх знань, вмінь та навичок сучасного правника, зокрема це стосується й тих юристів, що провадять свою діяльність у сфері кримінальної юстиції. Умови сьогодення диктують нові, раніше невідомі правила, зумовлені дуже динамічною імплементацією технологій штучного інтелекту в усі сфери суспільного життя, в тому числі й кримінального процесу, невід'ємним елементом якого є стадія досудового розслідування, що стає підґрунтям подальшого плину кримінального судочинства.