ефективність діяльності правоохоронних органів, служб інформаційної та економічної безпеки, фінансових установ і державних організацій. В умовах постійного зростання обсягів даних використання подібних систем стає необхідною складовою сучасної аналітичної діяльності. Подальший розвиток IBM i2 пов'язується з інтеграцією алгоритмів штучного інтелекту, машинного навчання та автоматизованого виявлення аномалій, що дозволить ще більше підвищити якість аналізу та швидкість прийняття обґрунтованих управлінських рішень.

Список використаних джерел

1. Chen H., Chiang R. H. L., Storey V. C. Business Intelligence and Analytics: From Big Data to Big Impact // MIS Quarterly. 2012. Vol. 36, № 4. P. 1165–1188.

2. IBM. IBM i2 Analyst's Notebook Documentation. URL: https://www.ibm.com/docs/en/i2-analysts-notebook

3. Few S. Information Dashboard Design: Displaying Data for At-a-Glance Monitoring. 2nd ed. Burlingame : Analytics Press, 2013. 272 p.

4. Marr B. Big Data: Using SMART Big Data, Analytics and Metrics to Make Better Decisions and Improve Performance. Chichester : John Wiley & Sons, 2015. 256 p.

Гаврилюк Михайло Дмитрович,
начальник відділу кримінального аналізу
Головного управління Національної
поліції у Волинській області

ВИКОРИСТАННЯ В КРИМІНАЛЬНОМУ АНАЛІЗІ ІННОВАЦІЙНИХ ТЕХНОЛОГІЙ, ЗОКРЕМА ШТУЧНОГО ІНТЕЛЕКТУ

Стрімкий розвиток цифрових технологій і штучного інтелекту (ШІ) кардинально змінює підходи до забезпечення публічної безпеки та розкриття злочинів в усьому світі. В умовах зростання рівня організованої злочинності, кіберзлочинів і транснаціональних злочинних угруповань традиційні методи кримінального аналізу поступово втрачають ефективність. Саме тому впровадження інноваційних технологій у діяльність правоохоронних органів України є не лише актуальним завданням, а й стратегічним пріоритетом реформування існуючої правоохоронної системи.

Штучний інтелект – це галузь комп'ютерних наук, яка займається створенням інтелектуальних машин, здатних виконувати завдання, що зазвичай потребують людського розуму, а інколи й перевершують людські здібності, тобто є підрозділом інформатики, який стосується автоматизації осмисленої поведінки та машинного самонавчання [1]. Разом з цим відповідно до Концепції розвитку штучного інтелекту в Україні, схваленої розпорядженням Кабінету Міністрів України від 02.12.2020 № 1556-р, штучний інтелект визначається як організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів опрацювання інформації, отриманої або самостійно створеної під час роботи, а також формувати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань [2]. Саме це визначення є основою для подальшого розгляду напрямів застосування ШІ в кримінальному аналізі.

Кримінальний аналіз як самостійний напрям діяльності поліції передбачає збирання, систематизацію та інтерпретацію інформації про злочинність з метою підтримки оперативно-службової діяльності та прийняття управлінських рішень. Застосування ШІ та суміжних інноваційних технологій дозволяє суттєво підвищити якість і швидкість такого аналізу.

Міжнародний досвід засвідчує, що провідні правоохоронні агенції світу – ФБР (США), Europol (ЄС), Metropolitan Police (Велика Британія) – активно використовують системи на основі ШІ для: аналізу великих масивів даних; прогностичної діяльності; розпізнавання осіб та транспортних засобів; моделювання дій правопорушника для розкриття злочинів, прогнозування його наступних кроків і розробки заходів безпеки.

В Україні процес упровадження подібних технологій перебуває на етапі становлення. Важливим кроком у напрямі цифровізації стало отримання доступу до хмарних аналітичних платформ та сервісів відкритих даних, зокрема рішень компаній Artellence [3, с. 161], YouControl [3, с. 160] та системи розпізнавання облич Clearview AI [4].

Зокрема, платформа Artellence (BigData) надає користувачам доступ до великих масивів структурованих і

неструктурованих даних з різних реєстрів, дозволяючи в режимі реального часу відстежувати зв'язки між особами, суб'єктами господарювання та майном. Сервіс YouControl забезпечує інтеграцію відомостей з державних реєстрів (ЄДРПОУ, реєстру нерухомості, судових рішень тощо) і широко використовується для верифікації суб'єктів у межах досудових розслідувань. Система Clearview AI, яка містить мільярди фотозображень із відкритих джерел, застосовується для розпізнавання осіб, причетних до злочинів, що суттєво скорочує час встановлення особи підозрюваного [3, с. 217].

Напрями застосування штучного інтелекту в кримінальному аналізі:

1. Прогностичний аналіз злочинності.

Алгоритми машинного навчання здатні аналізувати часові ряди злочинних проявів, геопросторові дані, соціально-економічні показники та прогнозувати «гарячі точки» злочинності. Сучасні аналітичні системи попередження злочинів (predictive policing) спрямовані на перехід від реактивного моделювання (реагування на злочин, що вже стався) до проактивного (запобігання правопорушенням шляхом оптимізації патрулювання) та демонструють точність передбачення місць скоєння злочинів до 70–80 % у порівнянні з традиційними методами [5].

2. Аналіз зв'язків та мереж.

Інструменти аналізу соціальних мереж у поєднанні з ШІ дозволяють виявляти приховані зв'язки між учасниками злочинних угруповань, ієрархічні структури організованої злочинності та канали фінансування. Програмне забезпечення i2 Analyst's Notebook, Maltego, SpiderFoot, Cobwebs та Palantir Gotham широко застосовується правоохоронними органами ЄС, США та України [3, с. 180].

3. Біометрична ідентифікація.

Системи розпізнавання облич на основі глибоких нейронних мереж досягають точності понад 99 % у контрольованих умовах. В Україні елементи такої технології вже апробовані, як під час перевірки осіб на блокпостах, масових заходів, так і встановлення осіб причетних до різного роду злочинів, зокрема із залученням можливостей Clearview AI та BigDataPeople 2.

4. Аналіз відкритих даних та реєстрів.

Платформи Artellence та YouControl дозволяють інтегрувати в єдиному інтерфейсі дані з десятків державних і комерційних реєстрів. Аналітик отримує можливість швидко встановлювати майновий стан підозрюваних, їхні корпоративні зв'язки, адреси, транспортні засоби та судову історію. Це принципово змінює швидкість і глибину досудових розслідувань, скорочуючи час збирання первинної аналітики з кількох годин до лічених хвилин.

5. Обробка неструктурованих даних.

Технології обробки природної мови дозволяють автоматично аналізувати тексти кримінальних проваджень, оперативних зведень, публікацій у соціальних мережах та месенджерах. Це скорочує час ручної обробки документів на 60–70 % і мінімізує ризик людської помилки.

6. Виявлення дипфейків і маніпульованого медіаконтенту.

Розвиток генеративного ШІ паралельно породжує нову категорію загроз: синтезовані відео- та аудіозаписи (deepfake) дедалі частіше використовуються для шахрайства, фальшивих звернень нібито від імені посадовців чи родичів, а також для виготовлення фіктивних доказів. У відповідь правоохоронні органи провідних країн впроваджують спеціалізовані детектори дипфейків на основі нейромереж, здатні аналізувати артефакти стиснення, неприродну міміку та біометричні невідповідності для встановлення автентичності медіафайлів, що стає окремим напрямом криміналістичного й кримінального аналізу.

7. OSINT-моніторинг.

Особливої актуальності для України набуває застосування ШІ-інструментів розвідки з відкритих джерел (OSINT) для виявлення інформаторів, координаторів та осіб, причетних до ймовірного скоєння різноманітних злочинів. Автоматизований моніторинг публічних каналів у Telegram та інших месенджерах дозволяє оперативно виявляти підозрілу активність, встановлювати мережі поширення дезінформації та в подальшому своєчасно інформувати зацікавлені підрозділи, що є важливою складовою кримінального аналізу в умовах повномасштабної війни.

Використання ШІ в правоохоронній діяльності також порушує низку принципових питань. По-перше, проблема «алгоритмічної упередженості»: якщо навчальні дані містять систематичні та повторювані помилки в системах ШІ, алгоритм

відтворюватиме та посилюватиме дискримінаційні патерни, що базуються на соціальних стереотипах щодо статі, етносу, віку чи інших ознаках. По-друге, питання захисту персональних даних і конфіденційності: масове збирання біометричних даних суперечить принципам Загального регламенту ЄС про захист даних, до вимог якого Україна прагне адаптуватися.

Принципово важливим є забезпечення принципу «людина в петлі»: алгоритм ШІ має бути інструментом підтримки рішення, але не заміщати повноваження слідчого або оперативного працівника обирати один із кількох законних варіантів процесуальних рішень або дій. Будь-яке рішення, що безпосередньо зачіпає права людини, повинне прийматися людиною з урахуванням висновків наявних систем.

З урахуванням наведеного, для ефективного впровадження ШІ у сферу діяльності кримінального аналізу доцільно здійснити наступні заходи:

– розробити та прийняти спеціальний нормативно-правовий акт щодо використання ШІ в правоохоронній діяльності з визначенням меж допустимого застосування;

– провести модернізацію інформаційної інфраструктури та забезпечити створення єдиної архітектури, яка дозволяє різнорідним інформаційним системам обмінюватися даними та функціонувати як єдине ціле;

– запровадити системну підготовку аналітиків у сфері роботи з ШІ-інструментами;

– для обміну технологіями та досвідом налагодити міжнародне партнерство з правоохоронними органами країн – членів ЄС, та активно застосовувати програми технічної допомоги КМЄС в Україні.

Упровадження штучного інтелекту в повсякденній діяльності працівників кримінального аналізу є об’єктивною необхідністю в умовах сучасних викликів для Національної поліції України. Наявні світові практики свідчать про значний потенціал таких технологій для підвищення ефективності протидії злочинності. Водночас їх застосування потребує чіткої правової регламентації, дотримання прав людини та постійного вдосконалення кадрового потенціалу. Баланс між технологічними можливостями та гуманістичними цінностями який передбачає, що технології мають служити людині та її розвитку, а не навпаки – повинен стати основою поліцейської діяльності в цифрову епоху.

Список використаних джерел

1. Основи штучного інтелекту: що це таке URL: https://lemon.school/blog/yak-stvoryuyetsya-shtuchnyj-intelekt

2. Про схвалення Концепції розвитку штучного інтелекту в Україні : розпорядження Кабінету Міністрів України від 02.12.2020 р. № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р

3. Реалізація філософії «Intelligence-led Policing» в системі кримінального аналізу Національної поліції України : монографія / О. Користін та ін. ; за заг. ред. О. Є. Користіна. Київ : BAITE, 2024. 444 с.

4. 10 мільярдів фото і система розпізнавання: Україна отримала доступ до бази Clearview AI. Укрінформ. URL: https://www.ukrinform.ua/rubric-technology/3429032-10-milardiv-foto-i-sistema-rozpiznavanna-ukraina-otrimala-dostup-dobazi-clearview-ai.html

5. Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations / W. L. Perry et al. RAND Corporation, 2013. 238 p.

Гвоздюк Віталій Валерійович,
старший науковий співробітник науково-дослідної лабораторії з проблем протидії злочинності навчально-наукового інституту поліцейської діяльності Національної академії внутрішніх справ, доктор філософії в галузі права

OSINT-ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-АНАЛІТИЧНІЙ ДІЯЛЬНОСТІ ОПЕРАТИВНИХ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Сучасна злочинність дедалі активніше використовує цифровий простір для підготовки, вчинення та приховування кримінальних правопорушень. Значна частина інформації, що становить оперативний інтерес, сьогодні поширюється у відкритому доступі через соціальні мережі, вебсайти, месенджери, електронні реєстри, геоінформаційні сервіси та інші цифрові платформи. За таких умов своєчасне виявлення, перевірка та аналіз відкритої інформації стають необхідною складовою