

Мішкоріз Олександр Володимирович,
начальник відділу кримінального аналізу
Головного управління Національної
поліції в Закарпатській області

АСПЕКТИ ВИКОРИСТАННЯ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ В КРИМІНАЛЬНОМУ АНАЛІЗІ

Сучасний етап розвитку правоохоронної діяльності характеризується стрімкою цифровізацією суспільства, зростанням обсягів інформації та ускладненням форм злочинної діяльності. Організовані злочинні угруповання активно використовують сучасні технології, криптовалюти, засоби анонімізації та цифрові платформи для приховування протиправної діяльності. У таких умовах традиційні методи аналізу вже не завжди дозволяють своєчасно виявляти загрози та ефективно підтримувати процес прийняття управлінських рішень [1, с. 12].

Саме тому впровадження інноваційних технологій та систем штучного інтелекту стає одним із пріоритетних напрямів розвитку кримінального аналізу як в Україні, так і в провідних правоохоронних органах світу [2, с. 45].

Як зазначають українські науковці, кримінальний аналіз є сучасною інформаційно-аналітичною технологією, спрямованою на виявлення прихованих зв'язків між подіями, особами та об'єктами з метою підтримки процесу прийняття управлінських рішень у сфері боротьби зі злочинністю [3, с. 23].

Під штучним інтелектом у сфері кримінального аналізу розуміють комплекс технологій, які забезпечують автоматизовану обробку даних, пошук закономірностей, прогнозування подій та формування аналітичних висновків на основі великих масивів інформації [4, с. 67].

Сьогодні правоохоронні органи щоденно працюють із великими обсягами інформації, що надходять із різних джерел: телефонного трафіку, банківських операцій, соціальних мереж, відкритих джерел інформації, геолокаційних сервісів та інших інформаційних ресурсів. Технології штучного інтелекту забезпечують автоматизацію процесу їх обробки та значно скорочують час підготовки аналітичних продуктів [5, с. 88].

Одним із найперспективніших напрямів є використання технологій Big Data. Завдяки сучасним алгоритмам машинного

навчання правоохоронні органи можуть аналізувати мільйони записів, виявляти приховані зв'язки між учасниками злочинних груп, прогнозувати ризики та визначати потенційні загрози громадській безпеці [6, с. 34].

Особливого значення набуває застосування штучного інтелекту під час аналізу відкритих джерел інформації (OSINT). Сучасні програмні комплекси забезпечують автоматизований моніторинг соціальних мереж, новинних ресурсів та месенджерів, дозволяють виявляти мережі взаємопов'язаних акаунтів, аналізувати інформаційні кампанії та встановлювати ознаки координації протиправної діяльності [7, с. 51].

Позитивний досвід використання штучного інтелекту накопичено в діяльності Європолу й Інтерполу. Вказані організації активно використовують алгоритми машинного навчання для боротьби з кіберзлочинністю, тероризмом, торгівлею людьми та іншими формами організованої злочинності [8].

Водночас застосування штучного інтелекту потребує дотримання принципів законності, захисту персональних даних, інформаційної безпеки та прав людини. Саме тому ключовим принципом використання штучного інтелекту в правоохоронній діяльності має залишатися обов'язковий людський контроль над процесом прийняття рішень [9, с. 97].

Незважаючи на значний потенціал штучного інтелекту для підвищення ефективності кримінального аналізу, його практичне впровадження у діяльність правоохоронних органів супроводжується низкою проблемних питань організаційного, правового, технічного та етичного характеру.

Однією з ключових проблем є забезпечення належної якості даних, що використовуються для функціонування систем штучного інтелекту. Результати роботи алгоритмів безпосередньо залежать від повноти, актуальності та достовірності інформації, яка надходить із різних джерел. Наявність помилок, дублювання записів, фрагментарність відомостей або відсутність стандартизованих підходів до обробки інформації можуть суттєво впливати на точність аналітичних висновків [1, с. 78].

Не менш важливою проблемою є ризик алгоритмічних помилок та упередженості моделей машинного навчання. Використання історичних даних для навчання систем штучного

інтелекту може призводити до відтворення вже існуючих помилок або викривлень, що містяться в інформаційних масивах. У результаті виникає загроза формування необ'єктивних висновків, які можуть негативно впливати на процес прийняття управлінських рішень у сфері правоохоронної діяльності [10, с. 94].

Важливим аспектом залишається забезпечення балансу між потребами правоохоронної діяльності та дотриманням прав і свобод людини. Використання технологій штучного інтелекту пов'язане з обробкою значних обсягів персональних даних, що вимагає суворого дотримання вимог законодавства у сфері захисту інформації та права на приватність. У зв'язку з цим особливого значення набувають питання законності отримання, зберігання та використання інформації під час проведення кримінального аналізу [11].

Суттєвим викликом для правоохоронної системи України залишається також недостатній рівень нормативно-правового регулювання використання штучного інтелекту. На сьогодні відсутні комплексні механізми правового контролю за застосуванням таких технологій, що зумовлює необхідність розроблення відповідних стандартів, процедур аудиту та оцінки ефективності функціонування інтелектуальних систем.

Крім того, впровадження інноваційних технологій потребує належного кадрового забезпечення. Сучасний кримінальний аналітик повинен володіти не лише методиками аналізу кримінальної інформації, а й базовими компетенціями у сфері обробки даних, машинного навчання, інформаційної безпеки та використання спеціалізованих програмних продуктів. Відповідно, актуальним завданням залишається розвиток системи професійної підготовки та підвищення кваліфікації фахівців з кримінального аналізу.

Окремим перспективним напрямом розвитку кримінального аналізу є використання генеративного штучного інтелекту та великих мовних моделей. Сучасні системи здатні автоматично аналізувати значні масиви текстової інформації, узагальнювати матеріали кримінальних проваджень, здійснювати пошук взаємозв'язків між подіями, особами та об'єктами, а також формувати аналітичні довідки та інформаційні звіти. Використання таких технологій сприяє суттєвому скороченню

часу підготовки аналітичних продуктів та підвищенню оперативності реагування на криміногенні загрози [12, с. 41].

Водночас міжнародний досвід свідчить, що правоохоронні органи дедалі активніше впроваджують інструменти штучного інтелекту для аналізу відкритих джерел інформації, виявлення ознак організованої злочинної діяльності та прогнозування кримінальних ризиків. Зокрема, у діяльності Європолу й Інтерполу технології штучного інтелекту використовуються для обробки великих масивів даних, автоматизованого встановлення зв'язків між об'єктами аналізу та підтримки прийняття управлінських рішень під час проведення міжнародних розслідувань. Зазначені тенденції свідчать про поступовий перехід від традиційного аналізу великих даних до інтелектуальних систем підтримки аналітичної діяльності, заснованих на технологіях штучного інтелекту [13].

Отже, ефективне використання штучного інтелекту в кримінальному аналізі потребує комплексного підходу, що передбачає вдосконалення нормативно-правової бази, забезпечення високої якості даних, підготовку кваліфікованих кадрів та впровадження механізмів контролю за функціонуванням інтелектуальних систем. Лише за умови дотримання зазначених вимог технології штучного інтелекту зможуть стати дієвим інструментом підвищення ефективності правоохоронної діяльності та протидії сучасним формам злочинності.

Для України перспективними напрямками розвитку є створення єдиного інформаційно-аналітичного середовища правоохоронних органів, впровадження інструментів штучного інтелекту для підтримки кримінального аналізу, розвиток міжвідомчого обміну даними та підготовка фахівців нового покоління, здатних ефективно працювати із сучасними аналітичними технологіями.

Підсумовуючи викладене, слід зазначити, що штучний інтелект уже сьогодні стає невід'ємною складовою кримінального аналізу. Його впровадження дозволяє значно підвищити швидкість обробки інформації, якість аналітичних продуктів та ефективність діяльності правоохоронних органів загалом. Майбутнє кримінального аналізу полягає у гармонійному поєднанні професійного досвіду аналітика, сучасних інформаційних технологій та можливостей штучного інтелекту.

На завершення, якщо згадати славетну фразу Натана Ротшильда “хто володіє інформацією – володіє світом”, усе чіткіше окреслюється думка про перехід концепції від володіння інформацією до її швидкого усвідомлення.

У ХХІ столітті перемагає не той, хто має більше інформації, а той, хто здатний швидше перетворити її на знання та управлінське рішення.

Список використаних джерел

1. Горбач Д. О. Кримінальний аналіз у діяльності правоохоронних органів України : монографія. Київ : НАВС, 2021. 248 с.
2. Коваленко В. В. Інформаційно-аналітичне забезпечення діяльності Національної поліції України. Київ : Юрінком Інтер, 2020. 312 с.
3. Половніков В. В. Основи кримінального аналізу : навчальний посібник. Київ : НАВС, 2019. 198 с.
4. Рассел С., Норвіг П. Штучний інтелект: сучасний підхід. Київ : Діалектика, 2021. 1408 с.
5. Марутян Р. Р., Семенченко А. І. Великі дані (Big Data) в системі державного управління та безпеки. Київ : НАДУ, 2020. 236 с.
6. Provost F., Fawcett T. Data Science for Business. Sebastopol : O'Reilly Media, 2013. 414 p.
7. Steele R. Open Source Intelligence. Virginia : OSS International Press, 2019. 372 p.
8. Europol. EU Serious and Organised Crime Threat Assessment (SOCTA) 2025. Hague, 2025.
9. United Nations Office on Drugs and Crime. Artificial Intelligence and Criminal Justice. Vienna, 2024.
10. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. 4th ed. Harlow : Pearson Education, 2021. 1136 p.
11. Council of Europe. Guidelines on Artificial Intelligence and Data Protection. Strasbourg, 2019.
12. Europol. AI and Policing – The Benefits and Challenges of Artificial Intelligence for Law Enforcement. Hague, 2024.
13. Interpol. Project INSIGHT: Criminal Intelligence Analysis and Artificial Intelligence. Lyon, 2025.