

Владислав ГАВЛОВСЬКИЙ, Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю при РНБО України, кандидат юридичних наук, старший науковий співробітник.

Михайло ГУЦАЛЮК, Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю при РНБО України, кандидат юридичних наук, старший науковий співробітник

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПРОТИДІЇ ОРГАНІЗОВАНИЙ ЗЛОЧИННОСТІ

Стрімкий розвиток технологій штучного інтелекту (ШІ) став одним із ключових факторів трансформації сучасного суспільства. Менш ніж за три роки понад 1,2 мільярда людей скористалися інструментами штучного інтелекту, що є швидшим темпом впровадження, ніж Інтернет, персональний комп'ютер чи навіть смартфон [1].

Сьогодні ШІ активно використовується у різноманітних сферах людської діяльності. Водночас поряд із позитивними можливостями технології штучного інтелекту дедалі частіше використовуються організованими злочинними угрупованнями для підвищення ефективності кібератак, фінансового шахрайства, інформаційних маніпуляцій та приховування слідів злочинів тощо. За оцінками Europol, сучасна організована злочинність фактично перетворюється на високотехнологічні кримінальні підприємства, які активно використовують цифрові технології, криптовалюти, штучний інтелект та глобальні комунікаційні платформи [2].

Одним із найбільш поширених напрямів злочинного використання ШІ є кібератаки та автоматизація злочинної діяльності [3]. Сучасні алгоритми здатні автоматично сканувати мережеву інфраструктуру та програмне забезпечення з метою пошуку вразливостей, аналізувати мільйони рядків коду та здійснювати інтелектуальний підбір способів обходу систем захисту. Крім того, організовані групи використовують AI-assisted malware – шкідливе програмне забезпечення, яке здатне адаптуватися до антивірусних систем та змінювати власний код для уникнення виявлення. Значну небезпеку становить і використання великих мовних моделей (LLM) для створення персоналізованих фішингових повідомлень різними мовами, що суттєво підвищує ефективність соціальної інженерії.

Окремим напрямом є використання технологій DeepFake та генеративного ШІ для фінансового шахрайства. Злочинці створюють підроблені відео- та аудіозаписи, імітуючи зовнішність або голос керівників компаній, представників банків чи родичів потерпілих. Такі технології активно застосовуються у схемах CEO fraud, під час яких жертви перераховують значні кошти на рахунки зловмисників. Генеративний ШІ також дозволяє створювати надзвичайно реалістичний фейковий контент, який складно відрізнити від справжнього, що суттєво ускладнює діяльність правоохоронних органів [4].

В Україні вже зафіксовано практичні випадки використання ШІ організованими групами. Зокрема, у 2025 році Національна поліція України викрила організовану групу, яка за допомогою технологій DeepFake оформлювала кредити на громадян України, завдавши збитків на суму понад 4 млн грн [5].

ШІ активно використовується й для легалізації злочинних доходів. Алгоритми машинного навчання дозволяють злочинцям автоматизувати дроблення фінансових транзакцій, аналізувати механізми банківського моніторингу та оптимізувати схеми відмивання коштів через криптовалютні сервіси та міжнародні фінансові платформи. Крім того, організовані групи використовують бот-мережі та генеративний ШІ для проведення

масштабних дезінформаційних кампаній, створення фейкових акаунтів та маніпулювання суспільною думкою.

У таких умовах особливої актуальності набуває питання використання штучного інтелекту самими правоохоронними органами для протидії організованій злочинності.

Одним із ключових напрямів застосування ШІ є аналіз великих масивів даних (Big Data). Сучасні алгоритми дозволяють правоохоронним органам здійснювати пошук прихованих зв'язків між учасниками злочинних угруповань, аналізувати структуру кримінальних мереж та встановлювати роль окремих осіб у злочинній діяльності. Так званий *criminal network analysis* дає змогу виявляти організаторів злочинних схем, координаторів фінансових операцій та осіб, причетних до міжнародних злочинних мереж. Крім того, ШІ використовується для автоматизованого аналізу фінансових транзакцій, криптовалютних переказів та електронних комунікацій, що сприяє виявленню підозрілих операцій і схем відмивання коштів.

Важливим напрямом є *predictive policing* – використання алгоритмів прогнозування злочинної активності. Аналізуючи історичні дані про правопорушення, соціально-економічні фактори та геопросторову інформацію, системи штучного інтелекту можуть визначати так звані «гарячі точки» – райони з підвищеною ймовірністю вчинення злочинів. Це дозволяє правоохоронним органам ефективніше планувати патрулювання, здійснювати превентивні заходи та застосовувати ризик-орієнтований підхід у боротьбі з організованою злочинністю. У багатьох країнах ЄС та США такі системи вже використовуються для прогнозування кримінальної активності та оптимізації розподілу ресурсів поліції.

Суттєву роль ШІ відіграє і в цифровій криміналістиці. Інтелектуальні системи здатні автоматизувати аналіз значних обсягів цифрових доказів, пришвидшувати пошук релевантної інформації та виявляти приховані закономірності. Особливо актуальним є використання ШІ для OSINT-розвідки, аналізу соціальних мереж, даркнет-майданчиків та зашифрованих каналів комунікації. Алгоритми машинного навчання дозволяють виявляти аномалії у мережевому трафіку, підозрілу поведінку користувачів та ознаки підготовки кібератак або фінансових злочинів. Такі технології суттєво підвищують ефективність розслідування складних кіберзлочинів і діяльності транснаціональних злочинних угруповань.

Окремим напрямом застосування ШІ є використання біометричних систем. Системи розпізнавання облич та відеоаналітики дозволяють ідентифікувати підозрюваних у режимі реального часу, здійснювати пошук осіб у натовпі та аналізувати відеозаписи з камер спостереження. В Україні з 2022 року активно використовується система Clearview AI, яка допомагає правоохоронним органам встановлювати особи військових злочинців, перевіряти осіб на блокпостах та ідентифікувати загиблих. Таким чином, використання технологій штучного інтелекту створює нові можливості для ефективної протидії організованій злочинності, однак одночасно потребує належного нормативно-правового регулювання та забезпечення балансу між безпекою і правами людини.

Водночас впровадження таких технологій породжує низку правових, етичних та організаційних проблем, пов'язаних із захистом прав людини, приватності та нормативним регулюванням використання ШІ у правоохоронній діяльності.

Насамперед актуальною залишається проблема відсутності чіткого законодавчого визначення злочинів, учинених із використанням технологій штучного інтелекту. В Україні більшість таких діянь кваліфікуються за традиційними нормами кримінального законодавства, зокрема як шахрайство, несанкціоноване втручання в роботу інформаційних систем або порушення недоторканності приватного життя. Водночас чинне законодавство не враховує специфіку використання генеративного ШІ, DeepFake-технологій чи автономних алгоритмів. Окремою проблемою є *admissibility AI-generated evidence* - допустимість доказів, отриманих або сформованих із використанням алгоритмів штучного інтелекту, а також питання достовірності та перевірки таких доказів у кримінальному провадженні.

Серйозні виклики виникають і в етичній сфері. Використання систем відеоспостереження, біометричної ідентифікації та аналізу великих масивів персональних даних може створювати ризики порушення права на приватність та сприяти формуванню механізмів масового стеження.

Крім того, алгоритми штучного інтелекту можуть містити помилки або демонструвати алгоритмічну дискримінацію через використання неповних чи упереджених наборів даних. Особливу небезпеку становлять помилки систем розпізнавання облич, які можуть призводити до неправильної ідентифікації осіб та порушення прав людини.

Не менш важливими залишаються організаційні проблеми. Правоохоронні органи часто стикаються з нестачею висококваліфікованих фахівців у сфері штучного інтелекту, цифрової криміналістики та аналізу даних. Додатковими перешкодами є недостатній рівень технічного забезпечення, обмежене фінансування та залежність від іноземного програмного забезпечення. В Україні також відсутня комплексна державна стратегія щодо впровадження технологій ШІ у діяльність правоохоронних органів, що ускладнює координацію між державними органами та створення єдиної системи протидії сучасним формам організованої злочинності.

Насамкінець важливим є і використання ШІ для прийняття рішень у судовій діяльності, адже у кінцевому рахунку тільки суд може приймати відповідний вирок по справі [6].

Список використаних джерел

1. AI Diffusion Report: Mapping global AI adoption and innovation URL: <https://news.microsoft.com/source/emea/features/ai-diffusion-report-mapping-global-ai-adoption-and-innovation-3/>
2. Europol warns of AI-driven crime threats URL: <https://www.reuters.com/world/europe/europol-warns-ai-driven-crime-threats-2025-03-18>
3. Mykhaylo Gutsalyuk AI in Cybersecurity: An Instrument for Defense and Attack // Oleksii Kostenko, & Yuriy Yekhanurov (Eds.). (2024). DIGITAL TRANSFORMATION IN UKRAINE: AI, METAVERSE, AND SOCIETY 5.0. DOI: <https://doi.org/10.69635/978-1-0690482-1-9-ch23>
4. Europol warns AI is making organized crime ‘more precise and devastating’ because it’s able to create ‘highly realistic synthetic media’ that propagates violence and normalizes corruption. URL: <https://fortune.com/2025/03/18/europol-ai-organized-crime>
5. Шахрайство з використанням ШІ: поліція викрила групу, яка оформила кредитів на українців на 4 млн. URL: <https://minfin.com.ua/ua/2025/10/14/160446190>
6. Впровадження штучного інтелекту у судову діяльність: міжнародний та український досвід // *Наукові праці Київського авіаційного інституту*. Серія: Юридичний вісник «Повітряне і космічне право». № 2(75). С. 167–175. DOI: <https://doi.org/10.18372/2307-9061.75.20230>