2. Федчак І. А. Основи кримінального аналізу: навч. посібник. Львів: ЛьвДУВС, 2021. 288 с.
3. OSINT Open Source Intelligence. Інструменти та методи: навч. посібник / О. Користін, С. Демедюк та ін. Київ: 7БЦ, 2025. 460 с.
4. Кисельов А. О., Копилов Е. В., Худенко Д. М. Основи кримінального аналізу: навч. посібник. Дніпро: ДДУВС, 2023. 152 с.
5. Компендіум OSINT-інструментів / за підтримки ЄС та МФ «Відродження», 2024. 14 с.

OSINT В УМОВАХ AI-КОНТЕНТУ: ПРОБЛЕМА ВЕРИФІКАЦІЇ СИНТЕТИЧНИХ ОСОБИСТОСТЕЙ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

Ісмайлов Карен Юрійович
кандидат юридичних наук, доцент
професор кафедри кримінального аналізу
та інформаційних технологій
Одеського державного університету внутрішніх справ
Заєць Олександр Михайлович
кандидат юридичних наук, доцент

У сучасних умовах правоохоронна діяльність дедалі більше залежить не лише від здатності отримувати інформацію з відкритих джерел, а й від можливості встановлювати її достовірність, походження та придатність для подальшого аналітичного або процесуального використання. Якщо раніше OSINT переважно розглядався як інструмент пошуку, збору, зіставлення та попереднього аналізу відкритих даних, то в умовах масового поширення AI-контенту його функціональне призначення істотно ускладнюється. На перший план виходить не просто виявлення інформації, а її верифікація, встановлення автентичності цифрової особи, джерела походження зображення, відео, голосового повідомлення, профілю в соціальній мережі або цифрової біографії. Так як не вірне первинна інтерпретація займе в подальшому багато часу для виявлення.

Особливої гостроти проблема набуває у зв'язку з поширенням синтетичних особистостей – штучно створених або частково

змодельованих цифрових ідентичностей, які можуть включати AI-згенеровані фотографії, фальшиві біографічні дані, історію активності у соціальних мережах, імітовані професійні зв'язки, голосові повідомлення, deepfake-відео та інші елементи цифрової присутності. Європол у звіті IOCTA 2025 прямо зазначає, що викрадені дані можуть використовуватися для створення діпфейків, синтетичних медіа та фальшивих ідентичностей, що ускладнює протидію злочинності, а особливо кіберзлочинності та організованій злочинності [1].

У правоохоронній діяльності такі явища створюють декілька взаємопов'язаних ризиків: помилкову ідентифікацію особи; використання фейкових профілів для шахрайства, вербування, дезінформації або соціальної інженерії; дискредитацію реальних осіб через синтетичний контент; ускладнення доказування у кримінальному провадженні; зниження довіри до відкритих джерел як допоміжного інструменту кримінального аналізу. Інтерпол у межах Project SynthWave окремо розвиває правоохоронні спроможності щодо виявлення AI-згенерованих синтетичних медіа, що підтверджує міжнародне визнання проблеми як практично значущої для органів правопорядку [2].

Для України ця проблематика має додаткове значення в умовах воєнного стану, гібридних загроз, інформаційно-психологічних операцій, документування воєнних злочинів, кіберзлочинності та активного використання відкритих цифрових джерел у правоохоронній діяльності. Закон України «Про Національну поліцію» прямо передбачає здійснення поліцією інформаційно-аналітичної діяльності для реалізації її повноважень [3], а Закон України «Про основні засади забезпечення кібербезпеки України» визначає участь Національної поліції України у взаємодії в межах національної системи реагування на кіберінциденти, кібератаки та кіберзагрози [4].

Проблематика OSINT у правоохоронній діяльності вже стала предметом наукової уваги як міжнародних, так і українських дослідників та інституцій. На міжнародному рівні питання використання відкритих джерел, цифрової ідентичності, діпфейків та AI-контенту активно розглядаються в аналітичних матеріалах Europol, INTERPOL, ENISA, UNODC [5-7]. Зокрема, Europol у SOCTA 2025 звертає увагу на те, що злочинці за допомогою синтетичних медіа можуть вводити в оману потерпілих, імітувати

реальних осіб, здійснювати дискредитацію або шантаж. UNODC у 2025 році також зазначає, що злочинні групи дедалі активніше використовують AI для створення deepfake, голосового клонування та синтетичних ідентичностей у кіберзлочинних схемах.

У міжнародному науково-практичному дискурсі особливу увагу приділено не лише технічному виявленню AI-контенту, а й формуванню комплексної моделі реагування: поєднанню цифрової криміналістики, аналітики відкритих джерел, міжнародної співпраці, підготовки спеціалістів та правового регулювання. У матеріалах EL PAcCTO 2.0, присвячених «weaponizing AI», окремо наголошується на необхідності посилення правоохоронних спроможностей через спеціалізовані підрозділи, інструменти криміналістичного аналізу AI-контенту, алгоритмічну простежуваність, підготовку фахівців і міжнародну взаємодію [8].

В українській науковій площині питання OSINT розглядаються у працях, присвячених кримінальному аналізу, інформаційно-аналітичній діяльності поліції, фіксації воєнних злочинів, забезпеченню національної безпеки та використанню відкритих джерел у сфері публічної безпеки. Так, Олексій Деревягін досліджує OSINT у правоохоронній діяльності з урахуванням міжнародного досвіду використання відкритих джерел у розслідуванні кіберзлочинів, терористичних актів і воєнних злочинів [9]. Р. Биба аналізує поняття OSINT у сфері публічного порядку та безпеки, підкреслюючи потребу в удосконаленні адміністративно-правового регулювання й понятійного апарату [10]. М. Тома та О. Василова розглядають інструменти OSINT у контексті фіксації воєнних злочинів в Україні [11].

Окремо слід зазначити праці, які стосуються інформаційно-аналітичного забезпечення діяльності поліції та кримінального аналізу. В. Маковій досліджує інформаційно-аналітичну підтримку діяльності поліції як складову забезпечення інформаційної безпеки держави [12]. Крім того, у сучасних українських дослідженнях OSINT пов'язується з реалізацією філософії Intelligence-Led Policing у системі кримінального аналізу Національної поліції України [13-17].

Водночас аналіз наукових джерел свідчить, що проблема саме верифікації синтетичних особистостей в умовах AI-контенту ще не отримала достатнього комплексного висвітлення в українській

правовій науці. Переважна частина досліджень зосереджена на загальних можливостях OSINT, використанні відкритих джерел у розслідуванні, фіксації воєнних злочинів або інформаційно-аналітичному забезпеченні поліції. Менш розробленими залишаються питання правової оцінки синтетичної цифрової ідентичності, критеріїв її виявлення, стандартів документування результатів OSINT-перевірки та меж доказового використання інформації, отриманої в умовах поширення AI-згенерованого контенту.

Метою статті є наукове обґрунтування проблеми верифікації синтетичних особистостей у правоохоронній діяльності в умовах поширення AI-контенту, а також визначення основних організаційно-правових і методологічних підходів до використання OSINT для перевірки достовірності цифрової ідентичності.

Для досягнення цієї мети необхідно вирішити такі завдання: по-перше, визначити сутність синтетичної особистості як об'єкта OSINT-аналізу; по-друге, охарактеризувати основні ризики використання AI-контенту для правоохоронної діяльності; по-третє, запропонувати логіку OSINT-верифікації синтетичних цифрових профілів; по-четверте, окреслити правові та організаційні умови допустимого використання результатів такої перевірки.

Синтетична особистість у контексті правоохоронної OSINT-аналітики може бути визначена як штучно створена або істотно модифікована цифрова ідентичність, що формується шляхом поєднання реальних, викрадених, вигаданих або AI-згенерованих даних з метою імітації існування конкретної особи у цифровому середовищі. На відміну від звичайного фейкового акаунта, синтетична особистість може мати більш складну структуру: стабільну цифрову історію, зображення, створені генеративними моделями, мережу контактів, публікації, коментарі, електронні адреси, телефонні номери, фінансові або професійні атрибути.

У правоохоронній діяльності такі профілі можуть використовуватися для вчинення шахрайства, збору інформації про потерпілих, підготовки кіберзлочинів, поширення дезінформації, дискредитації державних посадових осіб, приховування реального суб'єкта злочинної діяльності або створення фіктивного інформаційного сліду. Тому основною проблемою стає не сам факт існування відкритого джерела, а питання його достовірності, стабільності, походження та зв'язку з реальною особою.

Перше завдання OSINT у таких умовах полягає у встановленні ознак синтетичності цифрової ідентичності. До таких ознак можуть належати: відсутність природної історії цифрової активності; надмірно «ідеалізовані» або стилістично однотипні фотографії; невідповідність між датами створення профілю та заявленою біографією; штучна або шаблонна мовна поведінка; неприродна мережа контактів; відсутність незалежних підтверджень існування особи в інших джерелах; використання зображень, які мають ознаки генерації або маніпуляції; збіг елементів біографії з іншими підозрілими профілями.

Друге завдання полягає у багаторівневій верифікації цифрового профілю. Така перевірка не може обмежуватися одним джерелом або одним технічним інструментом. Доцільним є застосування поетапної моделі: первинна ідентифікація профілю; фіксація доступних даних; перевірка зображень і медіаконтенту; аналіз часової лінії активності; перевірка зв'язків; зіставлення з відкритими реєстрами та іншими незалежними джерелами; оцінка ризику синтетичності; документування результатів. Саме така логіка дає змогу перейти від інтуїтивної оцінки до структурованого аналітичного висновку.

Третє завдання пов'язане з розмежуванням технічної, аналітичної та процесуальної оцінки OSINT-результатів. Технічна оцінка дозволяє виявити ознаки AI-генерації або цифрової модифікації. Аналітична оцінка дає змогу визначити ймовірність того, що профіль є синтетичним або використовується для приховування реального суб'єкта. Процесуальна оцінка має значення тоді, коли результати OSINT можуть бути використані в кримінальному провадженні, для орієнтування слідства, формування версій, підготовки запитів, призначення експертиз або документування цифрових слідів.

Важливо підкреслити, що OSINT сам по собі не повинен підміняти процесуальне доказування. Його результати можуть бути цінними для виявлення джерел інформації, побудови слідчих версій, встановлення зв'язків, попередньої ідентифікації ризиків та орієнтування оперативної або слідчої діяльності. Проте у випадках, коли йдеться про доказове використання AI-контенту або висновків щодо синтетичної особистості, необхідними є належна фіксація, збереження цифрових слідів, документування часу доступу, джерела,

способу отримання інформації, технічних параметрів файлів, а за потреби – призначення відповідної експертизи.

Четверте завдання стосується організаційно-правового забезпечення такої діяльності. У межах Національної поліції України OSINT-верифікація синтетичних особистостей має розглядатися як частина ширшої інформаційно-аналітичної діяльності, що здійснюється виключно в межах законних повноважень. Стаття 25 Закону України «Про Національну поліцію» закріплює повноваження поліції у сфері інформаційно-аналітичного забезпечення, зокрема формування та використання інформаційних ресурсів для виконання завдань поліції [3, ст. 25]. Водночас використання OSINT має відповідати принципам законності, необхідності, пропорційності, захисту персональних даних і недопущення необґрунтованого втручання у приватне життя.

Окремого значення набуває підготовка правоохоронців до роботи з AI-контентом. Звичайні навички пошуку інформації у відкритих джерелах уже недостатні. Потрібна спеціалізована підготовка з аналізу діпфейків, синтетичних медіа, цифрової поведінки бот-мереж, виявлення AI-згенерованих зображень, оцінки достовірності цифрових біографій, а також правильного документування результатів. Національна поліція України вже використовує навчальні підходи, пов’язані з OSINT, протидією дезінформації та технологіями кримінального аналізу, що підтверджує практичну потребу у розвитку цього напряму.

З урахуванням викладеного OSINT в умовах AI-контенту має розглядатися не як допоміжний «пошуковий» інструмент, а як комплексна методологія перевірки цифрової реальності. Її сутність полягає у переході від простого накопичення відкритих даних до встановлення їх походження, автентичності, взаємозв’язку, стабільності та придатності для правоохоронного використання. Саме тому проблема синтетичних особистостей є не лише технологічною, а й правовою, організаційною та доказовою.

Проведений аналіз дає змогу сформулювати такі висновки.

Синтетична особистість є новим об’єктом правоохоронного OSINT-аналізу, оскільки поєднує ознаки фейкового акаунта, AI-згенерованого медіаконтенту, цифрової легенди та потенційного інструмента злочинної діяльності. Її небезпека полягає не лише у неправдивості окремих даних, а у створенні переконливої

цифрової ідентичності, здатної вводити в оману потерпілих, правоохоронців, установи та автоматизовані системи перевірки.

Основним завданням OSINT в умовах AI-контенту стає верифікація, а не лише пошук інформації. Правоохоронна аналітика має бути орієнтована на перевірку автентичності джерела, походження медіаконтенту, природності цифрової поведінки, реальності соціальних зв'язків і відповідності біографічних даних незалежним відкритим джерелам.

Результати OSINT-перевірки синтетичних особистостей потребують стандартизованого документування. Доцільним є запровадження внутрішніх методичних рекомендацій для підрозділів поліції щодо фіксації цифрових слідів, збереження копій сторінок, опису інструментів перевірки, зазначення часу доступу, джерел інформації та рівня достовірності встановлених даних.

Перспективним напрямом удосконалення правоохоронної діяльності є поєднання OSINT, кримінального аналізу та цифрової криміналістики. Такий підхід дозволить не лише ефективніше виявляти синтетичні особистості, а й забезпечувати належну якість інформаційно-аналітичних матеріалів, які можуть використовуватися для формування слідчих версій, оперативного реагування та подальшого процесуального закріплення доказів.

Список використаних джерел:

1. Steal, deal and repeat - How cybercriminals trade and exploit your data Internet Organised Crime Threat Assessment (IOCTA) 2025. European Union Agency for Law Enforcement Cooperation, 2025. 25 p.

2. Project SynthWave develops capabilities for law enforcement to detect AI-generated synthetic media and counter the threats posed by this technology. March 2025 – February 2026. URL: https://www.interpol.int/en/How-we-work/Innovation/Projects/Project-SynthWave

3. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text

4. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

5. European union serious and organised crime threat assessment the changing dna of serious and organised crime. European Union

Agency for Law Enforcement Cooperation. UNODC, 2025. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

6. Emerging threats: The intersection of criminal and technological innovation in the use of automation and artificial intelligence in the cybercrime landscape of Southeast Asia. Cybercrime Technical Brief Series. September 2025. 24 p. URL: https://www.unodc.org/roseap/uploads/documents/Publications/2025/UNODC_Report_Emerging_threats_-_The_intersection_of_criminal_and_technological_innovation_in_the_use_of_automation_and_AI.pdf

7. Incident reporting. ENISA. 2025. URL: https://ciras.enisa.europa.eu

8. Weaponizing artificial intelligence: how ai reshapes the world of organized crime. European Union Agency for Law Enforcement Cooperation. Luxembourg: Publications Office of the European Union, 2025. 49 p. URL: https://www.expertisefrance.fr/ sites/ expertise/files/2026-02/eng_elpaccto2-weaponizingai_compress.pdf

9. Борисова К., Жмуровська К., Кришталь, Є., Деревягін О. OSINT у правоохоронній діяльності: міжнародний досвід та українські перспективи. *UNIVERSUM. №* 25. 2025. С. 205-210.

10. Риба Р.Ю. Поняття OSINT у сфері публічного порядку та безпеки. *Науковий вісник Ужгородського національного університету*. Серія: Право. Том 3 № 92. 2025. С. 38-43/

11. Василенко В.М. Цифрова трансформація правоохоронних органів: ризики в умовах гібридних загроз та шляхи їх подолання. *Вісник Кримінологічної асоціації України*. 2024. Т. 32, № 2. С. 945-958.

12. Маковій В.П., Усата Г.О. Інформаційно-аналітична підтримка діяльності поліції як складова частина системи заходів із забезпечення інформаційної безпеки держави. *Морська безпека та оборона.* № 1. 2023. С. 62-68.

13. OSINT Open Source Intelligence. Інструменти та методи: навчальний посібник / Користін О., Демедюк С., Ісмайлов К., Ланде Д. та ін., за заг. ред. Користіна О.Є., Демедюка С.В. Київ: 7БЦ, 2025. 460 с.

14. Ісмайлов К.Ю. Особливості кримінальної розвідки з відкритих джерел як інструмент збирання оперативної інформації. *Південноукраїнський правничий часопис*. 2016. № 2. С. 110-113

15. Реалізація філософії «Intelligence-led Policing» в системі кримінального аналізу Національної поліції України: монографія / Користін О., Бутко Р., Денисенко Б., Ісмайлов К.Ю. та ін., за заг. ред. Користіна О.Є. Київ: «ВАІТЕ», 2024. 444 с.

16. Основи кримінального аналізу: підручник / Бабенко А.М., Заєць О.М., Некрасов В.А., Ісмайлов К.Ю., Пефтієв Д.О. та ін.; за заг. ред. Користіна О.Є., 2019. Одеса. 296 с.

17. Савенко Д.О., Ісмайлов К.Ю. OSINT та соціальні мережі: загрози та можливості для молодіжних комунікацій. *The 7th International scientific and practical conference «Sociological and psychological models of youth communication»* (February 18-21, 2025) Copenhagen, Denmark. International Science Group. 2025. с. 242-246.

OSINT В СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ТА ДІЯЛЬНОСТІ ОРГАНІВ ПРАВОПОРЯДКУ

Кардашевський Юрій Романович
доктор філософії у галузі права,
керівник відділу внутрішнього контролю НАЗК

В умовах глобалізації та інтенсивного розвитку цифрових технологій економічна безпека стала однією з найважливіших складових національної безпеки. Використання відкритих джерел інформації (OSINT) у системі економічної безпеки дозволяє органам правопорядку ефективно реагувати на нові виклики, що виникають у різних сферах економічної діяльності, таких як корупція, шахрайство, кіберзлочинність та інші форми економічних правопорушень. OSINT, завдяки своєму доступу до широкого кола публічних джерел, має значний потенціал у сфері розвідки та аналізу економічної ситуації, що допомагає органам правопорядку забезпечити стійкість економічної системи і протидіяти злочинним проявам в економічній сфері.