20 РОКІВ ЛЬВІВСЬКОМУ ДЕРЖАВНОМУ УНІВЕРСИТЕТУ ВНУТРІШНІХ СПРАВ

Міністерство внутрішніх справ України
Львівський державний університет внутрішніх справ

РОЛЬ OSINT-ДОСЛІДЖЕНЬ У ПІДВИЩЕННІ РІВНЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Матеріали круглого столу

7 травня 2025 року

м. Львів

УДК 351.746.5:004.9:343.9(477)
Р68

Рекомендовано до розміщення в електронних сервісах ЛьвДУВС
Вченою радою навчально-наукового інституту управління, психології та безпеки
Львівського державного університету внутрішніх справ
(протокол від 5 травня 2025 р. № 7)

Р68 **Роль** OSINT-досліджень у підвищенні рівня національної безпеки України : матеріали круглого столу (м. Львів, 7 травня 2025 р.) / укладач І. О. Ревак. Львів : ЛьвДУВС, 2025. 249 с.

Опубліковано матеріали круглого столу з міжнародною участю «Роль OSINT-досліджень у підвищенні рівня національної безпеки України», який відбувся 7 травня 2025 року.

Вміщено тези доповідей учасників круглого столу, що відображають результати наукових досліджень авторів із висвітлення актуальних проблем, присвячених обговоренню потенціалу і практичного значення розвідки на основі відкритих джерел (OSINT) у зміцненні національної безпеки України в умовах гібридної війни, широкомасштабної збройної агресії та інформаційного протистояння.

Для аналітиків, фахівців сектору безпеки, правоохоронців, науковців і розробників OSINT-рішень.

Подано мовою оригіналу та в авторській редакції. Відповідальність за зміст наукових праць покладено на авторів.

The collection contains abstracts of reports and reports of the materials of the round table with international participation «The role of OSINT research in increasing the level of national security of Ukraine», which was held on May 7, 2025 at the Lviv State University of Internal Affairs. In publications of Ukrainian scientists, practitioners and young scientists reveals the current problems of the potential and practical significance of open source intelligence (OSINT) in strengthening the national security of Ukraine in the context of hybrid warfare, large-scale armed aggression and information confrontation.

УДК 351.746.5:004.9:343.9(477)

ЗМІСТ

ПЕРЕДМОВА

У сучасних умовах системних загроз національній безпеці України, спричинених повномасштабною збройною агресією російської федерації, гібридними викликами, інформаційним терором і високим рівнем транснаціональної злочинності, особливої актуальності набуває впровадження інноваційних підходів до збору, аналізу та верифікації даних. Відкриті джерела інформації (Open Source Intelligence, OSINT) перетворюються на один із ключових інструментів сучасної безпекової аналітики, забезпечуючи нову якість у прийнятті стратегічних рішень, правоохоронній діяльності, розслідуванні воєнних злочинів та протидії деструктивному впливу в інформаційному середовищі.

Круглий стіл на тему *«Роль OSINT-досліджень у підвищенні рівня національної безпеки України»* був організований з метою міждисциплінарного обговорення теоретичних засад і практичних аспектів використання OSINT-інструментів у системі безпекового управління держави. У рамках заходу було розглянуто низку важливих напрямів, серед яких – застосування OSINT-досліджень для виявлення, документування та розслідування воєнних злочинів, що є важливим елементом формування доказової бази для міжнародних судових інстанцій та історичної пам'яті.

Особливу увагу приділено методам виявлення та нейтралізації інформаційних загроз і дезінформаційних кампаній, що становлять серйозну загрозу інформаційному суверенітету України. Учасники круглого столу наголосили на потенціалі OSINT як ефективного інструменту в сфері кібербезпеки, зокрема щодо виявлення атак на критичну інфраструктуру, моніторингу кіберзагроз та виявлення аномальних фінансових потоків, що можуть свідчити про підготовку або фінансування злочинної діяльності.

Окремим вектором дискусії стала роль OSINT у протидії незаконній торгівлі, зокрема наркотиками, об'єктами культурної спадщини, а також спробам обходу міжнародних санкцій. Відзначено важливість міжвідомчої взаємодії та використання інструментів відкритої аналітики правоохоронними органами для підвищення ефективності оперативно-розшукової діяльності та досудового розслідування.

Учасники круглого столу дійшли згоди, що в умовах динамічних загроз та технологічного розвитку OSINT-підходи потребують подальшої інституалізації, вдосконалення нормативно-правового регулювання, розвитку спеціалізованої освіти та професійної підготовки фахівців. Розвиток національної школи OSINT-досліджень має стати пріоритетом у зміцненні безпекового потенціалу держави, формуванні аналітичного мислення та забезпеченні національної стійкості.

Матеріали, представлені в цьому збірнику тез, відображають результати плідного фахового обміну думками, практичного досвіду та наукових напрацювань учасників круглого столу. Переконані, що оприлюднені напрацювання сприятимуть подальшому розвитку OSINT-інструментарію в Україні, поглибленню міжвідомчої координації, а також посиленню спроможності держави до ефективної протидії загрозам у сфері національної безпеки.

Абзалов Денис,
курсант
(Донецький державний університет
внутрішніх справ)
Науковий керівник:
Габорець Ольга,
доктор філософії, доцент,
доцент кафедри оперативно-розшукової
діяльності та інформаційної безпеки
(Донецький державний університет
внутрішніх справ)

ШТУЧНИЙ ІНТЕЛЕКТ ЯК ЧИННИК ТРАНСФОРМАЦІЇ КІБЕРЗАГРОЗ У КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

У контексті сучасних глобальних трансформацій стрімкий розвиток цифрових технологій, зокрема штучного інтелекту (ШІ), суттєво змінює спектр загроз у сфері національної безпеки. Використання технологій ШІ сприяє вдосконаленню механізмів виявлення кіберзагроз, оптимізації оборонних стратегій та підвищенню стійкості критичної інформаційної інфраструктури держави. Водночас ці технології дедалі активніше застосовуються як інструменти нової генерації кіберзлочинності, гібридних війн та інформаційного впливу на державні та суспільні інститути. Така дуальна природа ШІ вимагає переосмислення підходів до формування державної політики у сфері кібербезпеки та поглибленого теоретичного аналізу відповідних викликів і загроз.

Кардинальні зміни у державній політиці з питань кібербезпеки в Україні розпочалися у 2014 році з початком збройної агресії Російської Федерації. Вказані обставини актуалізували визнання кібербезпеки як одного з ключових елементів системи національної безпеки. Зокрема, Р.О. Додонов наголошує, що Україна увійшла у найскладніший період свого розвитку, коли інформаційно-психологічний вплив перетворився на основний чинник ведення сучасної гібридної війни [1].

У цих умовах формування та реалізація державної політики у сфері кібербезпеки набула стратегічного значення, що знайшло

відображення у прийнятті низки нормативно-правових актів, створенні спеціалізованих органів кіберзахисту та розробці Національної стратегії кібербезпеки. Особливу актуальність у цьому процесі має інтеграція новітніх цифрових технологій, насамперед штучного інтелекту, у системи виявлення, моніторингу та нейтралізації кіберзагроз.

Відповідно до частини четвертої статті 3 Закону України «Про національну безпеку» [2], кібербезпека виокремлена як самостійний напрямок національної безпеки. Водночас її забезпечення є необхідною умовою для реалізації воєнної, зовнішньополітичної, економічної, інформаційної та екологічної безпеки. Це свідчить про універсальний характер функції кібербезпеки, яка пронизує усі сфери суспільних відносин, що мають критичне значення для стабільності держави.

Таким чином, забезпечення кібербезпеки набуває міжгалузевого характеру, стаючи невід'ємною складовою державного управління та стратегічного планування. Особливого значення це питання набуває в умовах зростаючої залежності критичної інфраструктури, державного управління, оборонного комплексу та фінансового сектору від цифрових технологій. Вразливість цих сфер обумовлює необхідність розробки комплексної, інтегрованої державної політики, орієнтованої як на превенцію загроз, так і на забезпечення здатності кіберпростору до оперативного реагування, відновлення та адаптації.

Штучний інтелект у цьому процесі виступає каталізатором трансформації традиційних підходів до безпеки. Використання алгоритмів машинного навчання, аналізу великих даних та систем автоматичного розпізнавання загроз дозволяє здійснювати моніторинг кіберпростору в режимі реального часу, виявляти аномальні патерни та прогнозувати потенційні атаки. Водночас недосконалість нормативно-правового регулювання і брак уніфікованих стандартів застосування ШІ у сфері безпеки створюють ризики зловживань, що вимагає розширення міжнародного співробітництва у розробці єдиних підходів до регулювання цієї галузі.

Серед основних кіберзагроз для національної безпеки більшості країн можна виокремити:

1) кібершпигунство та військові дії за підтримки або з відома держави, спрямовані на заволодіння державними, промисло-

вими таємницями, персональними даними чи іншою цінною інформацією;

2) використання Інтернету у терористичних цілях, зокрема для пропаганди, збору коштів та вербування прихильників;

3) кіберзлочинність, що включає викрадення персональних даних, відмивання коштів, продаж викраденої інформації про банківські картки, паролі серверів та шкідливе програмне забезпечення [3].

Отже, сучасний спектр кіберзагроз є багатокомпонентним і динамічним, вимагаючи системного, проактивного підходу до формування державної політики кібербезпеки. Така політика має бути спрямована на превентивне виявлення загроз, підвищення рівня кіберграмотності населення, розвиток науково-технічного потенціалу, а також на розширення міждержавного співробітництва в умовах цифрової глобалізації.

---

1. Гібридна війна: in verbo et in praxi : монографія / Донецький національний університет імені Василя Стуса / під заг. ред. проф. Р.О. Додонова. Вінниця : ТОВ «Нілан-ЛТД», 2017. 412 с.

2. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2469-19 (дата звернення: 23.04.2025).

3. Законодавство та стратегії у сфері кібербезпеки країн Європейського союзу. США, Канади та інших. URL: http://euinfocenter.rada.gov.ua/uploads/documents/28982.pdf

Блавацька Наталія,
кандидат технічних наук, доцент
співробітник
(Національна академія Служби безпеки України)

ВИКОРИСТАННЯ ПРОГРАМ ДЛЯ ПОКРАЩЕННЯ ЗОБРАЖЕНЬ В OSINT-ДОСЛІДЖЕННЯХ ПРИ ДОКУМЕНТУВАННІ ВОЄННИХ ЗЛОЧИНІВ

У сучасних воєнних конфліктах, зокрема під час неспровокованої агресії рф в Україні, зростає значення розвідки з відкритих джерел інформації (OSINT) для збору доказів воєнних злочинів та злочинів проти людяності. Фотографії, відеозаписи та супутникові знімки стають ключовими елементами в таких розслідуваннях. Проте часто OSINT-дослідники стикаються з проблемою, яка полягає в тому, що ці матеріали мають низьку якість і це ускладнює ідентифікацію об'єктів та подій. Тому використання програм для покращення зображень, в тому числі і на основі штучного інтелекту, стає необхідним для підвищення якості візуальних доказів та їх подальшого використання в судових процесах.

В таких програмних засобах реалізуються наступні сучасні технології покращення зображень, а саме:

- супер-роздільна здатність (Super-Resolution) – методи, що дозволяють збільшити роздільну здатність зображень для відновлення деталей, яких не були чітко видно на оригіналі;
- фільтрація шумів – алгоритми, які зменшують рівень шуму на зображеннях, задля покращення їх якості та роблять деталі більш розбірливими;
- корекція освітлення та контрасту – інструментарій, що дозволяє покращувати контрастність зображень та вирівнювати освітлення для ліпшого виокремлення деталей.

Покращення зображень у контексті OSINT-досліджень можуть використовувати для наступних завдань, таких як ідентифікація осіб, геолокація подій, аналіз озброєння та техніки.

При ідентифікації осіб покращені зображення обличчя дають змогу показувати більш ефективні результати при встановленні особи підозрюваних або жертв за допомогою технології розпізнавання по обличчю.

Під час здійснення геолокації подій, деталізація зображень досягається за рахунок покращення зображення та допомагає визначити місце зйомки за характерними об'єктами на фоні.

Аналіз та ідентифікація типів озброєння та військової техніки, які використовуються, стає можливою саме через покращені зображення, що є дуже важливим для розслідувань.

Проте, разом зі значними можливостями, які з'являються з застосуванням програмних засобів для покращення зображень при проведенні OSINT-досліджень, існують і певні виклики. Треба зважати на автентичність доказів, а саме надмірне покращення може поставити під сумнів достовірність зображень у суді. Крім того постають етичні питання, які пов'язані з тим, що обробка зображень жертв або чутливих матеріалів вимагає обережності та дотримання етичних норм. Також є певні завади у вигляді технічних обмежень щодо покращення зображень, а точніше сказати, не всі зображення піддаються ефективному покращенню, особливо якщо вихідна якість дуже низька.

Варто зазначити, що під час розслідування подій у Бучі українські слідчі використовували відеоаналітику та технології розпізнавання по обличчю для ідентифікації російських солдатів, підозрюваних у скоєнні воєнних злочинів. Застосування інструментів, які покращують зображення дозволило встановити підозрюваних осіб та зібрати докази для подальших судових процесів.

Аналізуючи закордонний досвід, слід сказати, що наші партнери активно використовують програмні продукти для покращення зображення під час проведення OSINT-досліджень. Наприклад, Європол створив спеціальну робочу групу OSINT для підтримки розслідувань воєнних злочинів в Україні, використовуючи технології покращення зображень та інші інструменти аналізу відкритих даних.

Підсумовуючи викладене, робимо висновок, що використання програм для покращення зображень відіграє важливу роль у документуванні воєнних злочинів та проведенні OSINT-досліджень. Технології, які реалізовано в цих програмах сприяють підвищенню якості візуальних доказів, що є критично важливим для встановлення істини та притягнення винних до відповідальності. Однак при використанні цих інструментів необхідно звертати

увагу на етичні аспекти та слідкувати за забезпеченням автентичності отриманих матеріалів.

---

1. GigaPixel AI – Topaz Labs. Інструмент штучного інтелекту для покращення зображень. URL: https://www.topazlabs.com/gigapixel-ai (дата звернення: 10.04.2025).
2. ESRGAN: Enhanced Super-Resolution Generative Adversarial Networks. URL: https://github.com/xinntao/ESRGAN (дата звернення: 10.04.2025).
3. Higgins E. We Are Bellingcat: An Intelligence Agency for the People. London: Bloomsbury Publishing, 2021. 272 p.
4. Europol. Europol sets up OSINT Taskforce to support investigations into war crimes committed in Ukraine. URL: https://www.europol.europa.eu/media-press/newsroom/news/europol-sets-osint-taskforce-to-support-investigations-war-crimes-committed-in-ukraine (дата звернення: 10.04.2025).

Благовенко Максим,
курсант
(Дніпровський державний університет
внутрішніх справ
Науковий керівник:
Рижков Едуард,
кандидат юридичних наук, професор,
професор кафедри інформаційних технологій
(Дніпровський державний університет
внутрішніх справ)

ВИКОРИСТАННЯ МЕТОДІВ OSINT В ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ КРИМІНАЛЬНОЇ ПОЛІЦІЇ

У сучасному інформаційному суспільстві обсяги відкритих даних зростають експоненційно. Соціальні мережі, публічні реєстри, новинні ресурси, вебсайти, форуми, геолокаційні сервіси та багато інших джерел містять величезну кількість інформації, яка може бути критично важливою для правоохоронної діяльності. Ігнорування цього масиву даних означає втрату цінних можливостей для розкриття злочинів, встановлення осіб, збору доказів та запобігання правопорушенням.

Методи OSINT дозволяють оперативнику ефективно збирати, обробляти, аналізувати та інтерпретувати цю відкриту інформацію, перетворюючи її на корисні розвідувальні дані. Це стає особливо актуальним у контексті зростання кіберзлочинності, транснаціональної організованої злочинності та використання цифрових технологій у вчиненні традиційних злочинів.

Використання методів OSINT є надзвичайно важливим для оперативно-розшукової діяльності, оскільки дозволяє збирати первинну інформацію про потенційних фігурантів, їхні зв’язки, спосіб життя та активи через аналіз соціальних мереж, публічних профілів та відкритих баз даних, що стає відправною точкою для подальшої розробки та виявлення нових об’єктів. Моніторинг відкритих джерел сприяє прогнозуванню злочинної діяльності, перевірці алібі та свідчень шляхом аналізу активності в соціальних мережах і геолокаційних даних, а також встановленню зв’язків між злочинцями. У сфері розшуку OSINT допомагає встановити місцезнаходження розшукуваних осіб, збирати інформацію про їхній спосіб життя в

умовах переховування та виявляти їхнє майно й активи. В оперативному супроводі кримінального судочинства інформація з відкритих джерел слугує допоміжним матеріалом для підтвердження або спростування доказів, виявлення спроб впливу на судовий процес, аналізу інформації про потерпілих та свідків, а в деяких випадках – для пошуку інформації про потенційних присяжних.

Стрімке поширення цифрових пристроїв для фото- та відеозйомки і їхня доступність для широкого загалу призвели до значного збільшення обсягу медійних файлів, які фіксують реальну ситуацію в різний час та у різних місцях. Усе частіше такі матеріали містять фотографії або відеозаписи, у тому числі з місць злочинів, на яких відображено осіб, що їх скоїли, спосіб вчинення правопорушення, використані транспортні засоби та інші обставини, важливі для розкриття та розслідування кримінальних правопорушень.

Велика кількість різноманітної інформації циркулює в мережі Інтернет, зокрема, популярні соціальні мережі, такі як «Instagram», «Facebook», «ВКонтакте» та «Одноклассники», майже завжди містять відомості про фізичних осіб. Це зумовлено тим, що самі користувачі добровільно публікують свої персональні дані, включаючи прізвище, ім’я, по батькові, дату народження, адресу проживання, контакти, інтереси, особисті фото та відео. Таким чином формується значний обсяг цифрових даних, що містять антропометричні характеристики зовнішності, анкетні відомості, зображення місць проживання та іншу інформацію.

Доступність цієї інформації в публічному просторі надає правоохоронним органам можливість вільно використовувати її в оперативних цілях. Аналіз таких даних може надавати важливу орієнтовну інформацію, злочинні зв’язкі особи, можливе місце перебування або переховування від слідства, а в окремих випадках навіть сприяти швидкій ідентифікації особи.

OSINT, або розвідка на основі відкритих джерел (від англ. Open Source Intelligence), являє собою комплексну концепцію, методологію та сукупність технологічних підходів, спрямованих на отримання та ефективне використання різноманітної інформації з публічно доступних джерел. Ключовою особливістю OSINT є неухильне дотримання законодавства при зборі та обробці даних, що робить її легітимним інструментом для підтримки прийняття стратегічно важливих рішень у сфері національної оборони та безпеки.

Процес OSINT включає в себе декілька ключових етапів: ретельний пошук інформації в різноманітних відкритих джерелах, систематичну реєстрацію та облік знайдених даних, глибокий аналіз зібраної інформації для виявлення закономірностей, зв'язків та прихованих значень, синтез отриманих аналітичних висновків у чіткі та структуровані повідомлення, а також ефективне адміністрування та своєчасне розповсюдження підготовленої інформації серед зацікавлених осіб.

OSINT – це збір та аналіз інформації з відкритих джерел. Ось деякі з методів:

Перший – розширений пошук в Інтернеті. Це використання пошукових систем, таких як Google, Bing чи DuckDuckGo, для знаходження інформації на вебсайтах, форумах, у блогах тощо.

Другий – аналіз соціальних мереж. Це вивчення профілів, публікацій та зв'язків у соцмережах, таких як Facebook, Twitter, Instagram та LinkedIn.

Третій – аналіз зображень та відео. Це використання інструментів для пошуку схожих зображень або відео, а також для аналізу метаданих, які можуть містити корисну інформацію.

Четвертий – аналіз даних. Це використання публічних баз даних, таких як реєстри компаній, судові справи чи дані про нерухомість.

П'ятий – аналіз геоданих. Це використання карт та супутникових знімків для отримання інформації про місцевість, будівлі тощо.

Шостий – аналіз Даркнету. Це дослідження прихованих частин інтернету, де можна знайти інформацію, недоступну у звичайних пошукових системах.

Сьомий – аналіз документів. Це вивчення публічних документів, таких як звіти, статті, презентації тощо.

Восьмий – аналіз коду. Це вивчення відкритого коду програм або вебсайтів для пошуку вразливостей або іншої корисної інформації.

Дев'ятий – аналіз фінансових даних. Це вивчення публічних фінансових звітів компаній або організацій.

Десятий – аналіз даних про домени та IP-адреси. Це використання інструментів для отримання інформації про власників доменів, IP-адреси тощо.

Ці методи часто використовуються разом для отримання повної картини про об'єкт дослідження.

OSINT надає можливість отримувати критично важливу інформацію щодо осіб та подій, що становлять оперативний інтерес, без обмежень, властивих роботі із закритими джерелами або традиційними методами розвідки. Завдяки впровадженню ШІ досягається автоматизований моніторинг соціальних мереж, інформаційних порталів, форумів та інших онлайн-платформ, що дозволяє оперативно збирати актуальні дані, мінімізуючи при цьому часові та інші ресурсні витрати [1, с. 86].

Специфіка інформації, отриманої за допомогою OSINT, полягає в тому, що вона є результатом глибокої аналітичної обробки значних обсягів відкритого та загальнодоступного інформаційного потоку. До цього потоку належить широкий спектр джерел, серед яких особливе місце займають засоби масової інформації, включаючи друковані видання (газети, журнали), радіомовлення та телебачення. Всесвітня мережа Інтернет є ще одним надзвичайно важливим джерелом OSINT, що охоплює онлайн-публікації різного формату, персональні та тематичні блоги, дискусійні групи та форуми, контент, створений самими користувачами (наприклад, аматорські відеозаписи з мобільних телефонів), популярні відеохостинги, такі як YouTube та RuTube, вікі-довідники з їхнім колективним наповненням, а також різноманітні вебсайти соціальних мереж, включаючи «Facebook, Twitter, Instagram» та «Telegram». Ці онлайн-платформи часто випереджають традиційні джерела інформації завдяки своїй оперативності та відносній легкості доступу до актуальних даних. Комерційні дані, такі як комерційні супутникові знімки, фінансові та промислові аналітичні звіти, а також різноманітні бази даних, також можуть бути використані в рамках OSINT. Нарешті, до інших літературних джерел, що становлять інтерес для OSINT, належать технічні звіти, патентна документація, робочі документи, ділова кореспонденція, неопубліковані наукові праці та інформаційні бюлетені. Таким чином, OSINT охоплює широкий спектр відкритих джерел інформації, що при правильному аналізі дозволяє отримувати цінну розвідувальну інформацію для підтримки прийняття обґрунтованих рішень у сфері національної безпеки [2, с. 146].

Використання методів OSINT на етапі профілактики злочинів є надзвичайно перспективним напрямком, оскільки дозволяє виявляти потенційні загрози та фактори ризику до моменту скоєння правопорушення. Аналіз відкритих джерел, таких як соціальні мережі, публічні форуми, новинні повідомлення та кримінальна статистика, може допомогти виявити зростання напруженості в певних соціальних групах, поширення екстремістських ідей, незаконний обіг зброї чи наркотиків, а також інші передумови злочинної діяльності. Отримана інформація дозволяє правоохоронним органам своєчасно вживати профілактичних заходів, проводити роз'яснювальну роботу, посилювати патрулювання в проблемних зонах та вживати інших заходів для запобігання злочинам.

Використання відкритих джерел інформації надає оперативникам значні переваги, зокрема, дозволяє сформувати об'єктивнішу картину подій, досліджуючи їх з різних перспектив, на відміну від обмеженості свідчень очевидців. Крім того, OSINT відкриває доступ до інформації з територій, куди фізичне проникнення оперуповноважених ускладнене або неможливе, а також сприяє отриманню ширшого спектру думок та свідчень, виходячи за межі офіційних осіб, оперуповноважених та безпосередніх свідків події [3, с. 47].

Інтеграція OSINT з традиційними методами оперативно-розшукової діяльності та досудового розслідування є ключовим фактором підвищення їхньої ефективності. Оперативні підрозділи мають можливість отримувати певну інформацію про користувачів через встановлені на їхніх смартфонах або інших пристроях програми. Наприклад, наявність специфічних додатків, таких як сервіси замовлення приватних літаків чи яхт, або історія пошуку в браузері відповідних запитів, може свідчити про високий рівень фінансового добробуту особи .

Впровадження OSINT у роботу оперативників стикається з проблемами величезних обсягів неструктурованих даних, необхідністю верифікації інформації, етичними та юридичними обмеженнями щодо приватності, нестачею кваліфікованих кадрів та потребою в технологічному забезпеченні й інтеграції з існуючими системами, а також ризиком протидії з боку зловмисників; водночас, це відкриває перспективи підвищення ефективності розслідувань, поліпшення профілактики злочинів, отримання унікальної інфор-

мації, зменшення ризиків для співробітників, економії ресурсів, розширення міжнародної співпраці та розвитку аналітичних можливостей, що вимагає комплексного підходу до навчання, законодавчого регулювання та технологічного обладнання [4, с. 20].

Таким чином, стрімке поширення цифрових технологій фіксації та всеосяжність інтернет-простору, зокрема соціальних мереж, генерують колосальні обсяги відкритої інформації, яка при вмілому застосуванні методології OSINT стає потужним інструментом у руках правоохоронних органів. Використання OSINT не лише розширює можливості для оперативного розшуку та розслідування злочинів, надаючи цінні відомості про осіб, обставини та навіть можливі злочинні зв'язки, але й відкриває нові перспективи для профілактики правопорушень шляхом виявлення потенційних загроз на ранніх стадіях. Інтеграція OSINT з традиційними методами збору доказів забезпечує синергетичний ефект, підвищуючи ефективність роботи кримінальної поліції, хоча й вимагає вирішення низки проблем, пов'язаних з обробкою великих даних, їх верифікацією, етичними аспектами та необхідністю технологічного й кадрового забезпечення. Впровадження OSINT є важливим кроком у модернізації системи правоохоронних органів, сприяючи підвищенню рівня національної безпеки та боротьби зі злочинністю в умовах цифрової епохи.

У контексті стрімкого зростання обсягів відкритої інформації в сучасному цифровому світі, методологія OSINT стає незамінним інструментом для правоохоронних органів. Її ефективне застосування відкриває значні можливості для оперативно-розшукової діяльності, починаючи від збору первинної інформації та встановлення злочинних зв'язків до прогнозування злочинної діяльності та розшуку осіб. Аналіз медійних файлів та даних із соціальних мереж надає цінну орієнтовну інформацію, сприяючи швидкій ідентифікації та розкриттю злочинів.

Таким чином, OSINT є ключовим елементом модернізації системи правоохоронних органів в умовах цифрової епохи, що дозволяє більш ефективно протидіяти злочинності та забезпечувати національну безпеку. Подальший розвиток та впровадження методології OSINT вимагає комплексного підходу, включаючи навчання кадрів, законодавче регулювання та технологічне оснащення.

1. Ryzhkov E. V. Features of utilizing artificial intelligence in OSINT by criminal police officers / E. V. Ryzhkov // Інструменти OSINT для юристів: як підвищити правову компетенцію у цифровому світі : матеріали всеукраїнського науково-педагогічного підвищення кваліфікації, 20 січня – 2 березня 2025 року. Львів – Торунь : Liha-Pres, 2025. – С. 85-89

2. Одерій О. В., Кожевніков О.А. Отримання криміналістично значущої інформації шляхом аналізу відкритих інтернет-джерел. / Одерій О. В., Кожевніков О. А. // Правовий часопис Донбасу №4 (73) 2020. - С. 144-155 URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/474ecadd-4472-45e7-bb0c-55541851b4fa/content

3. Кисельов А. О., Синеколодезький Р.М. Соціальні мережі та осінт-аналіз в розшуковій діяльності та діагностиці особистості. / Кисельов А.О., Синеколодезький Р.М // Студентський науковий журнал «UNIVERSUM». № 12 / 2024р. С. 40-48 URL: https://archive.liga.science/index.php/universum/article/download/1204/1216/1229

4. Мовчан А.В. Актуальні проблеми впровадження в органах Національної поліції України моделі поліцейської діяльності, керованої аналітикою / Мовчан А.В. // Соціально-правові студії. 2018. Випуск 1. С. 17-22 URL: https://sls-journal.com.ua/web/uploads/pdf/S&LS_2018_Vol.%201,%20No.%201_17-22.pdf

Бліхар В'ячеслав,
доктор філософських наук, професор,
директор навчально-наукового інституту
управління, психології та безпеки
(Львівський державний університет внутрішніх справ)

ВИКОРИСТАННЯ МЕТОДІВ OSINT ДЛЯ ВИВЧЕННЯ ВПЛИВУ ХРИСТИЯНСЬКИХ ІДЕЙ У ЦИФРОВОМУ ПРОСТОРІ: МОНІТОРИНГ, АНАЛІЗ І КІБЕРБЕЗПЕКА РЕЛІГІЙНИХ СПІЛЬНОТ

У сучасному цифровому світі, що перебуває в постійному інформаційному русі, релігійні ідеї, зокрема християнські, активно інтегруються в онлайн-простір, формуючи унікальне середовище цифрової духовності. Це не лише розширює межі релігійного впливу, а й вимагає нових підходів до його вивчення. Зростає потреба не тільки у змістовому аналізі релігійних повідомлень, але й у виявленні механізмів їх впливу на суспільну думку, поведінкові моделі та політичні уподобання.

У цьому контексті методи розвідки на основі відкритих джерел (OSINT) набувають особливої цінності. Вони дозволяють не лише збирати та перевіряти інформацію з публічних ресурсів, але й формувати цілісне уявлення про структуру та динаміку релігійного інформаційного поля. OSINT підходить для виявлення вразливих точок у цифровій комунікації християнських спільнот, аналізу безпекових ризиків і моніторингу деструктивних інформаційних впливів [1, с. 21–33]. Попри свої військові витоки, ця методологія набула міждисциплінарного характеру та активно застосовується у сфері соціогуманітарних досліджень – від політології до релігієзнавства [2].

У межах релігієзнавчого аналізу OSINT стає ефективним інструментом для вивчення змін у релігійній ідентичності, цифрової трансформації вірувань і появи віртуальних релігійних спільнот [3]. Особливого значення набуває типологізація релігійних наративів у цифровому просторі, що варіюються від дидактичних і обрядових до політизованих і контемплятивних. Їх системна ідентифікація є відправною точкою для подальшого контент-аналізу та соціологічної інтерпретації [4].

Крім того, глибинний моніторинг онлайн-дискурсу значною мірою залежить від сучасних технологій – нейромереж і алгоритмів машинного навчання. Вони дозволяють виявляти приховані тренди, неочевидні теми та маргінальні обговорення, які можуть у майбутньому набути масового розголосу. Зокрема, це стосується апокаліптичних наративів, езотеричних інтерпретацій глобальних криз або ж конспірологічних концепцій, що циркулюють у середовищі радикальних релігійних груп. Вивчення таких проявів є важливим для прогнозування можливих процесів радикалізації.

Варто також дослідити, як цифрова релігійна активність впливає на реальну соціальну поведінку: від участі в благодійності до протестної активності, зокрема у форматі онлайн-петицій, флешмобів або кампаній у соцмережах. Не менш актуальними є питання кібербезпеки християнських спільнот – фішингові атаки, хакерські втручання, підробка церковних ресурсів задля шахрайства. У таких випадках OSINT-інструменти сприяють виявленню загроз, оцінці ризиків та впровадженню превентивних заходів.

Значного ризику зазнають платформи, які забезпечують онлайн-трансляції богослужінь або здійснюють збір пожертв. Захист таких ресурсів передбачає впровадження криптографічних рішень, систем багатофакторної аутентифікації та постійний аудит цифрової інфраструктури [5]. Актуальним лишається й питання захисту персональних даних користувачів, перевірки достовірності джерел, виявлення ботоактивності та протидії маніпуляціям у публічних дискусіях. Освіченість адміністраторів у сфері цифрової безпеки прямо впливає на рівень захисту релігійних спільнот у мережі.

Аналіз практичних кейсів використання OSINT у дослідженнях діяльності українських церков у період воєнного стану показує зростання значення християнських меседжів морально-патріотичного спрямування, активізацію віртуального молитовного життя та підтримку вірян через відеозвернення. Церковна активність онлайн часто корелює з державною стратегією національного спротиву, особливо у напрямах психологічної підтримки населення, допомоги ЗСУ, організації волонтерських ініціатив тощо.

Важливо зазначити, що в умовах збройного конфлікту українське законодавство приділяє особливу увагу інформаційній безпеці. Закон «Про правовий режим воєнного стану» передбачає право держави на посилення контролю за інформаційним просто-

ром, а також на реалізацію заходів із протидії деструктивним впливам. У такому правовому полі OSINT має використовуватися в межах законності, з дотриманням принципів пропорційності, захисту прав людини та поваги до свободи віросповідання. Важливо також враховувати вимоги Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» і суміжних нормативно-правових актів щодо кібербезпеки.

Таким чином, OSINT може бути не лише засобом академічного дослідження, а й інструментом інформаційного захисту від маніпуляцій, дезінформації та атак на релігійні інституції. В умовах розвитку цифрового релігієзнавства доцільно впроваджувати практики псевдоанонімізації, обмеження збору персональних даних та дотримання етичних стандартів щодо зберігання інформації. OSINT відкриває нові перспективи у вивченні релігії в цифрову епоху – від аналізу змісту до прогнозування суспільних трендів. Водночас важливо поєднувати технічну грамотність з гуманітарною чутливістю, аби уникнути спрощень і забезпечити глибоке міждисциплінарне осмислення.

---

1. Jansen F., Martin C. OSINT and Religion: Mapping Public Faith. *Journal of Intelligence Ethics*. 2020. Vol. 5. Iss. 1. P. 21–33.
2. Lowenthal M. M. Intelligence: From Secrets to Policy. CQ Press, 2019. 616 p.
3. Campbell H. Digital Religion: Understanding Religious Practice in New Media Worlds. New York, 2013. 326 p.
4. Cheong P. H., Fischer-Nielsen P., Gelfgren S., Ess C. Digital Religion, Social Media and Culture. Peter Lang, 2012.
5. Solove D. J., Schwartz P. M. Information Privacy Law. Burlington: Aspen Publishing, 2024 1148 p.

Бутко Роман,
начальник
Департаменту кримінального аналізу,
полковник поліції
(Національна поліція України)

ВІД ЦИФРОВОГО СЛІДУ ДО ДОКАЗІВ: РОЛЬ OSINT У СУЧАСНОМУ КРИМІНАЛЬНОМУ АНАЛІЗІ

У світлі постійно зростаючих загроз, кримінальний аналіз стає необхідним інструментом, який дозволяє забезпечувати якісні рішення в сфері правопорядку та безпеки суспільства.

На Департамент кримінального аналізу покладено завдання з проведення, організації та координації інформаційно-пошукової й аналітичної роботи, спрямованої на збір, оцінку та реалізацію інформації, у тому числі з обмеженим доступом, шляхом надання її уповноваженим органам (підрозділам) для вжиття заходів відповідно до їх компетенції, оцінювання ризиків, а також використання її для забезпечення функцій покладених на поліцію (Положення про Департамент кримінального аналізу затверджене наказом (зі змінами) Національної поліції України від 29 грудня 2019 року № 1354).

Від дня створення, Департаментом, на постійній основі вживаються заходи, спрямовані на розбудову та розширення аналітичних спроможностей служби, підвищення рівня ефективності інформаційно-пошукової та інформаційно-аналітичної діяльності з урахуванням дії правового режиму воєнного стану, активізацію взаємодії з територіальними органами та підрозділами Національної поліції.

Розбудова потужностей кримінального аналізу протягом усього періоду супроводжувалася активною співпрацею з міжнародними партнерськими організаціями та адаптацією набутого досвіду. Ці складові лягли в основу реформування та реорганізації служби, розвитку її структури.

На основі зарубіжної практики керівництвом Національної поліції ухвалено рішення про необхідність розроблення універсальної аналітичної моделі правоохоронної діяльності, яка б включала найбільш оптимальні механізми, що містяться в концепціях аналітичної діяльності, керованої аналітикою (Intelligence-led policing – ILP), і Національної оперативно-аналітичної моделі

(National Intelligence Model) та успішно використовуються правоохоронними органами Європейського Союзу та Сполучених Штатів Америки, а також визначення ролі й основних потреб Національної поліції України в цьому процесі.

Тож, одним із пріоритетів розбудови служби у 2025 році є інтеграція моделі поліцейської діяльності, керованою аналітикою (ILP), яку використовує Євросоюз та національної розвідувальної моделі, насамперед, це чотири вектори на яких базується будь-яка аналітична діяльність: люди, знання, системи, джерела.

У світі, де цифрові технології невпинно змінюють наше життя, поняття «злочин» все частіше має не лише фізичний, а й цифровий вимір. І саме тому роль OSINT (Open Source Intelligence) – розвідки з відкритих джерел – у кримінальному аналізі стала неоціненною. OSINT дозволяє перетворити цифровий слід у доказ, а відкриту інформацію – у правду, яку можна підтвердити юридично.

В сучасних умовах OSINT є не просто аналітичною діяльністю, а ефективним інструментом кримінального аналізу, що дозволяє здійснювати моніторинг медіа, виявляти ІПСО, підтверджувати або спростовувати інформацію. Водночас цей процес потребує значних ресурсів і часу для обробки даних та оцінки їхнього впливу на безпеку держави. Для підвищення ефективності кримінального аналізу залучаються вітчизняні та міжнародні партнери, які надають передові програмні рішення та інформаційну підтримку.

З метою безперебійного забезпечення аналітичної діяльності працівники служби мають автоматизований доступ до 24 інформаційних і довідкових систем, реєстрів та банків даних органів державної влади та місцевого самоврядування. Крім того, Департаментом вживаються заходи спрямовані на розширення переліку ресурсів.

В роботі з аналітикою, зокрема у сфері правопорядку та розслідувань, акцент робиться на точності, актуальності, обґрунтованості та структурованості аналітичних продуктів. Однак, варто зазначити, що для OSINT не існує єдиних загальноприйнятих міжнародних стандартів, які б регламентували підходи до збору, обробки, верифікації та використання відкритої інформації. Це створює виклики в уніфікації практик, забезпеченні якості аналітичних продуктів.

У цьому контексті важливим дороговказом виступає так званий Протокол Берклі. Протокол Берклі – рекомендаційний документ, який у 2020 році представили Центр прав людини Універси-

тету Берклі в Каліфорнії та Офіс Верховного комісара ООН з прав людини. Він окреслює мінімальні стандарти для пошуку, збирання, зберігання, перевірки та аналізу відкритих джерел, і може слугувати практичним посібником для адвокатів, журналістів та дослідників. Закріплені стандарти є основою будь-якого OSINT-проєкту, тобто розвідки на основі відкритих джерел. Цей протокол вперше в історії систематизував етичні, правові та технічні стандарти збору, перевірки та використання відкритих цифрових джерел для документування порушень прав людини, воєнних злочинів і злочинів проти людяності. Він закладає підґрунтя для уніфікації OSINT-практик, дотримання принципів надійності та допустимості цифрових доказів у судових процесах.

Для правоохоронних органів України в умовах воєнного стану цей протокол є критично важливим, адже він сприяє професіоналізації підходів до збору інформації про воєнні злочини та дозволяє створювати аналітичні продукти, придатні до використання в міжнародних трибуналах.

Відсутність загальновизнаних стандартів для OSINT особливо помітна в контексті медійного моніторингу, який є ключовим напрямом роботи з відкритими джерелами. Моніторинг медіа передбачає системний процес збору, аналізу та оцінки інформації з відкритих джерел для виявлення ключових подій, тенденцій, маніпуляцій та інформаційних атак. У таких процесах використовуються OSINT-інструменти для встановлення джерел поширення інформації, хронології її появи, авторства, а також для виявлення потенційних загроз громадській безпеці.

Окремим напрямом в OSINT є геопросторовий аналіз, який базується на вивченні візуальних даних з відкритих джерел – фото, відео, супутникових знімків – з метою визначення географічного розташування події або об’єкта. Такий аналіз ґрунтується на деталях, що можуть здаватися другорядними, але містять ключову інформацію для ідентифікації місцевості. Архітектурні особливості, дорожня розмітка, тіні (що вказують на пору доби та напрямок сонця), види рослинності, мова написів на вивісках, дорожні знаки – усе це є важливими індикаторами, що дозволяють точно визначити місце зйомки. Геопросторовий аналіз часто використовується для верифікації фактів, збору доказів, оцінки оперативної обстановки, а також під час моніторингу конфліктних зон або дезінформаційних кампаній.

Повномасштабна війна внесла корективи в діяльність підрозділів кримінального аналізу. Аналітик сьогодні працює з розрізненими джерелами, включаючи зони бойових дій, окуповані території, цифрові відбитки злочинів. Його завдання – не лише узагальнити дані, а й «зшити» фрагменти у повну аналітичну картину, що дозволяє приймати точні оперативні та стратегічні рішення. Особливу увагу приділяється новим загрозам, пов'язаним з кіберзлочинністю, дезінформацією та використанням відкритих даних ворогом. Аналітик - це не просто офіцер, це особа, що робить рішення оперативних підрозділів та слідчих обґрунтованими та ефективними. Він здатний зіставити шматочки інформації, звернути увагу на деталі. Під час війни він має діяти у незвичному полі.

Мотив злочину часто не містить логічного пояснення, жертви давно були змушені залишити країну, докази перебувають на окупованій території, а злочинці відчувають безкарність. Окрім цього, аналітик постійно має справу з великим обсягом повідомлень про злочини. Від нього вимагається повна обізнаність у техніці, позивних, різновидах військової форми та інших деталях військових, причетних до злочину.

Департаментом кримінального аналізу Національної поліції України завершується розробка посібника «Розвідка відкритих джерел: Інструменти та техніка», який систематизує практичні підходи до роботи з OSINT-ресурсами у правоохоронній діяльності. Видання містить огляд методів пошуку та аналізу інформації, технік верифікації, інструментів автоматизації, а також розглядає специфічні напрями – соціальні мережі, геолокацію, криптовалюти, Big Data, ІПСО та розшук дітей. Особливу увагу приділено правовим аспектам та безпеці при використанні відкритих джерел. Посібник стане корисним фахівцям, які прагнуть підвищити ефективність OSINT-досліджень, а також є актуальним внеском у розвиток галузі з урахуванням сучасних викликів та технологій.

OSINT – це не просто збір публічної інформації. Це процес перетворення хаотичного цифрового шуму на достовірний, структурований і юридично значущий доказ. Сьогодні це одна з найпотужніших відповідей держави на виклики інформаційної війни, кіберзлочинності та транснаціонального тероризму.

Упевнений, що майбутнє кримінального аналізу лежить саме в точці перетину цифрового сліду, технологій та закону.

Винник Сергій,
аспірант кафедри менеджменту
та економічної безпеки
(Львівський державний університет
внутрішніх справ)

ВИКОРИСТАННЯ OSINT-ІНСТРУМЕНТІВ ДЛЯ ВИЯВЛЕННЯ ОБХОДУ САНКЦІЙ ТА МОНІТОРИНГУ ФІНАНСОВИХ ПОТОКІВ У БАНКІВСЬКОМУ СЕКТОРІ

У сучасних умовах ведення гібридної війни проти України, що супроводжується масштабними міжнародними санкціями проти держави-агресора, особливого значення набуває ефективне виявлення спроб обходу санкційних обмежень. При цьому банки залишаються не лише об'єктами регулювання у сфері протидії відмиванню коштів, але й ключовими агентами у виявленні сумнівних операцій. У цьому контексті інтеграція інструментів OSINT у систему фінансового моніторингу набуває стратегічного значення.

OSINT-дослідження, що передбачають отримання, обробку та аналіз даних з відкритих джерел, можуть суттєво підсилити спроможності банківських установ, регуляторів і підрозділів фінансової розвідки у виявленні ризикованих фінансових потоків, пов'язаних із санкційними суб'єктами. В умовах обмеженого доступу до закритих джерел інформації, відкриті дані – офіційні реєстри, судові рішення, витоки офшорної документації, міжнародні бази даних (OpenSanctions, Aleph, Sayari, ImportGenius, RuPEP тощо) – дають змогу виявити схеми маскування реальних бенефіціарів, зокрема через зміну юрисдикцій, використання проксі-компаній, пов'язаних осіб та транзитних рахунків.

Прикладом ефективного використання таких методів є практика фінансової розвідки в межах Європейського Союзу, де регулятори активно інтегрують OSINT-інструменти у процеси контролю за дотриманням санкційного режиму. У звітах Європейського парламенту (2022) наголошується на необхідності об'єднання фінансового моніторингу та OSINT-моніторингу для протидії обходу санкцій шляхом трансфертних схем, криптовалютних розрахунків або оформлення фіктивного експорту/імпорту [1].

В українському контексті, згідно зі звітом Державної служби фінансового моніторингу України за 2023 рік, було виявлено понад 100 транзакцій, які можуть бути пов'язані з особами, що перебувають у санкційних списках. При цьому особливу увагу приділяють автоматизованим алгоритмам виявлення «санкційних маршрутів» у платіжному трафіку, однак рівень залучення OSINT-технологій поки залишається обмеженим [2]. Водночас впровадження OSINT як частини ризик-орієнтованого підходу дозволило б підвищити точність таких виявлень, особливо у випадках, коли задіяно багатоетапні транскордонні операції з використанням третіх країн.

Типовими сценаріями обходу санкцій, які можуть бути виявлені шляхом OSINT-досліджень, є: реєстрація підприємств у юрисдикціях, не охоплених санкційним контролем; використання криптовалютних бірж для здійснення платежів в обхід SWIFT-системи; укладання фіктивних контрактів з метою легалізації товарів або послуг, що заборонені до постачання. Завдяки аналізу відкритих даних про корпоративні зв'язки, структуру власності, зовнішньоекономічну діяльність та фінансові операції можна швидко встановлювати зв'язки між фіктивними компаніями та фактичними суб'єктами, які перебувають під санкціями.

Особливої уваги заслуговує використання інструментів типу YouControl Sanctions Checker, TrapAggressor, OpenSanctions API, які дозволяють верифікувати контрагентів та перевіряти осіб/компанії на предмет присутності в санкційних списках ООН, ЄС, OFAC, Великобританії тощо. Окремі українські банки вже здійснюють апробацію автоматизованих рішень для такого попереднього аналізу, але відсутність єдиного протоколу взаємодії між банками, державними органами та розробниками OSINT-платформ ускладнює системне впровадження.

Загалом OSINT-інструменти доцільно розглядати як складову частину національної системи фінансового моніторингу та як ефективний інструмент превенції фінансових правопорушень, пов'язаних із порушенням або обходом санкцій. Рекомендовано на рівні Національного банку України та Держфінмоніторингу запровадити галузеві настанови щодо використання OSINT у банківському секторі, зокрема шляхом розробки ризик-профілів та модулів автоматичної перевірки контрагентів із залученням відкритих баз даних.

Таким чином, OSINT-дослідження можуть не лише посилити ефективність виявлення санкційних ризиків, а й забезпечити аналітичну основу для прийняття рішень щодо замороження активів, блокування рахунків та ініціювання фінансових розслідувань. Інтеграція відкритих джерел у механізми фінансового контролю є перспективним напрямом зміцнення фінансової безпеки України в умовах продовження російської агресії.

---

1. European Parliament (2022). The EU sanctions against Russia: Overview, implementation, challenges. URL: https://www.europarl.europa.eu

2. Державна служба фінансового моніторингу України (2023). *Звіт про діяльність у сфері фінансового моніторингу*. URL: https://www.sdfm.gov.ua

3. OpenSanctions. Global sanctions & persons of interest dataset. URL: https://www.opensanctions.org

Геліх Андрій,
здобувач вищої освіти
(Харківський національний юридичний
інститут імені Ярослава Мудрого)

OSINT-ДОСЛІДЖЕННЯ ЯК ІНСТРУМЕНТ ВИЯВЛЕННЯ, ДОКУМЕНТУВАННЯ ТА РОЗСЛІДУВАННЯ ВОЄННИХ ЗЛОЧИНІВ

Розвідка з відкритих джерел (OSINT) відіграє критично важливу роль у виявленні, документуванні та розслідуванні воєнних злочинів, зокрема в контексті збройної агресії Росії проти України. Завдяки аналізу інформації з відкритих джерел, таких як соціальні мережі, новинні портали та інші публічні ресурси, OSINT-спеціалісти можуть ідентифікувати осіб, причетних до злочинів, та збирати докази їхньої діяльності.

Агентство бізнес-розвідки Molfar є прикладом ефективного використання OSINT для викриття воєнних злочинців. З початку повномасштабного вторгнення Росії в Україну команда Molfar провела понад двісті аналітичних досліджень, спрямованих на ідентифікацію та документування злочинів російських військових. Зокрема, вони встановили особи понад 500 військових, причетних до масових убивств у Бучі, а також ідентифікували командирів та персонал авіабаз «Енгельс-2» та «Шайківка», які здійснювали ракетні обстріли українських міст. Molfar публікує зібрані дані у відкритому доступі та співпрацює зі світовими ЗМІ, щоб привернути увагу міжнародної спільноти до воєнних злочинів та сприяти притягненню винних до відповідальності.

У листопаді 2023 року Європол створив нову оперативну групу для підтримки розслідувань міжнародних злочинів, скоєних в Україні після російського вторгнення. До складу групи увійшли представники 14 країн, включаючи Німеччину, Нідерланди, Францію та США. Основним завданням цієї групи є збір та аналіз розвідувальної інформації з відкритих джерел для ідентифікації підозрюваних та встановлення їхньої причетності до воєнних злочинів, злочинів проти людяності та геноциду. Очолюють групу підрозділи боротьби з міжнародними злочинами поліції Нідерландів та Німеччини.

Важливість OSINT у розслідуванні воєнних злочинів підкреслюється можливістю отримання достовірних доказів, які можуть бути використані в міжнародних судах. Зокрема, аналіз супутникових знімків, відео та фотоматеріалів з місць подій дозволяє встановити хронологію подій та ідентифікувати винних. Крім того, OSINT сприяє виявленню та протидії дезінформації, яка часто використовується для приховування або виправдання злочинів.

Співпраця між державними та недержавними організаціями, які займаються OSINT-розслідуваннями, є ключовою для ефективного документування та розслідування воєнних злочинів. Обмін інформацією та координація дій між різними структурами дозволяє швидко реагувати на нові виклики та забезпечувати належне збереження та використання зібраних доказів.

Однак використання OSINT у розслідуванні воєнних злочинів супроводжується низкою викликів. По-перше, необхідно забезпечити автентичність та достовірність зібраної інформації, оскільки відкриті джерела можуть містити як правдиві, так і хибні дані. По-друге, важливо дотримуватися етичних норм та правових стандартів при зборі та використанні інформації, щоб не порушувати права людини та не наражати на небезпеку жертв або свідків злочинів.

Значну роль у розвитку OSINT-розслідувань відіграють технологічні інновації. Використання штучного інтелекту та машинного навчання дозволяє автоматизувати процеси збору та аналізу великих обсягів даних, що підвищує ефективність розслідувань. Крім того, розвиток технологій візуалізації та геолокації сприяє точнішому встановленню місць та обставин скоєння злочинів.

Важливо також зазначити роль громадянського суспільства та волонтерів у процесі OSINT-розслідувань. Багато ініціатив базується на співпраці з місцевими жителями, які надають інформацію з місць подій, що є надзвичайно цінним для встановлення істини та притягнення винних до відповідальності.

Таким чином, OSINT є потужним інструментом у виявленні, документуванні та розслідуванні воєнних злочинів. Його ефективне використання потребує тісної співпраці між державними органами, міжнародними інституціями, неурядовими організаціями та громадянським суспільством. Забезпечення достовірності та етичності в процесі збору та аналізу інформації є ключовими факторами успіху

в боротьбі за справедливість та притягнення винних до відповідальності.

---

1. Omelchenko V. Europol has created an OSINT working group to help Ukraine investigate Russia's war crimes | УНН. *Ukrainian National News (UNN)*. URL: http://unn.ua/en/news/europol-has-created-an-osint-working-group-to-help-ukraine-investigate-russias-war-crimes (дата звернення: 02.04.2025).
2. vkarpova7. Як працює osint-розвідка? Від бізнес-аналізу до оборони україни. *ISSP Training*. URL: https://www.issp.training/post/yak-pratsyuye-osint-rozvidka-vid-biznes-analizu-do-oborony-ukrayiny (дата звернення: 02.04.2025).
3. Важливість OSINT у документуванні воєнних злочинів в Україні - Освітній дім прав людини в Чернігові. *Освітній дім прав людини в Чернігові*. URL: https://ehrh.org/vazhlyvist-osint-u-dokumentuvanni-voyennyh-zlochyniv-v-ukrayini/?utm_source=chatgpt.com (дата звернення: 02.04.2025).

Гончаренко Олена,
кандидат економічних наук,
доцент кафедри світової економіки
(Державний торговельно-економічний університет)
Чернишенко Катерина,
здобувач вищої освіти
(Державний торговельно-економічний університет)

ДІПФЕЙК-ТЕХНОЛОГІЇ ЯК ІНСТРУМЕНТ КІБЕРВІЙНИ У СФЕРІ МІЖНАРОДНОЇ БЕЗПЕКИ

У сучасних умовах, коли цифрові технології займають центральне місце в міжнародних відносинах, діпфейк-технології (створення фальсифікованих відео та аудіоматеріалів за допомогою штучного інтелекту та алгоритмів глибокого навчання) стали однією з найбільших загроз для кібербезпеки та дипломатичної стабільності. Зловмисники використовують ці технології для створення високоякісних підроблених матеріалів, що дозволяють маніпулювати громадською думкою, поширювати дезінформацію і підривати довіру між державами. Нині спостерігаємо використання таких технологій для дискредитації політичних лідерів, втручання у виборчі процеси та ескалації міжнародних конфліктів. Водночас, міжнародне право ще не має єдиного механізму для регулювання боротьби з діпфейками, а технологічні компанії змогли лише частково впровадити алгоритми для виявлення подібних загроз. У цих умовах кібердипломатія стає вирішальним інструментом для вироблення міжнародних норм, сприяння співпраці між державами та інтеграції штучного інтелекту в боротьбу з цифровими загрозами для захисту національних інтересів у кіберпросторі.

Діпфейк-технології стали серйозним викликом для міжнародної безпеки та інформаційної стабільності, оскільки їх використання для створення фальшивого контенту загрожує демократичним процесам, маніпулюючи громадською думкою та підриваючи довіру до інституцій. Незважаючи на підвищену увагу до цієї проблеми, на міжнародному рівні досі відсутня єдина правова база для регулювання застосування цих технологій у дипломатії та міждержавних відносинах. Їх використання в дипломатії, зокрема для створення фальшивих заяв офіційних осіб і змінених відеозаписів

переговорів, становить особливу небезпеку [1]. Яскравим прикладом є фальшиве відео з Камалою Гарріс під час виборів у США 2024 р. та маніпулятивне відео із закликом до капітуляції України, створене після початку російського вторгнення в 2022 р. [2; 3].

Незважаючи на зростаючу увагу до цієї проблеми та активне її обговорення ООН, ОБСЄ та НАТО [4], єдина міжнародна правова база для регулювання використання таких технологій у міждержавних відносинах досі відсутня.

Одним із ключових аспектів є необхідність розробки міжнародних стандартів для маркування синтетичного контенту, що дозволить визначати його штучне походження. Такі ініціативи мають бути підтримані ефективним правовим механізмом, який визначатиме відповідальність за зловживання діпфейк-технологіями, зокрема у випадках маніпулювання виборчими процесами та дипломатичною комунікацією.

ЄС, США та Китай продемонстрували різні підходи до регулювання цього питання [5-7]. ЄС зобов'язав онлайн-платформи виявляти та маркувати синтетичний контент, тоді як США орієнтуються на координацію між державними органами та технологічними компаніями через ініціативу Deepfake Task Force. Китай застосовує суворі обмеження на створення та поширення такого контенту.

Незважаючи на технологічні досягнення у виявленні фальшивих відео та аудіозаписів, сучасні методи перевірки ще не інтегровані в робочі процеси міжнародних організацій та дипломатичних установ. Для ефективної боротьби з діпфейк-загрозами необхідно впровадити технології ШІ, такі як комп'ютерний зір та аудіоаналіз, які вже досягли значних успіхів у виявленні артефактів у синтетичному контенті [8].

Кібердипломатія є ключовим інструментом для забезпечення міжнародної співпраці в боротьбі з діпфейк-технологіями. Вона має сприяти розробці глобальних стандартів і механізмів відповідальності за їх використання, а також організовувати обмін даними між державами та технологічними компаніями. Це дозволить оперативно реагувати на інформаційні атаки та забезпечити довіру до міжнародних процесів.

Одним із перспективних кроків може стати створення спеціалізованої міжнародної структури, яка б моніторила використання діп-

фейків у міжнародних відносинах, подібної до Ради Безпеки ООН. Крім того, важливими є ініціативи, такі як Паризький заклик до довіри та безпеки в кіберпросторі, що встановлюють чіткі міжнародні принципи відповідальності за поширення фальшивого контенту [9].

Міжнародні організації, такі як ООН, ОБСЄ та НАТО, вже активно працюють над забезпеченням інформаційної безпеки та медіаграмотності, зокрема у контексті технологій діпфейк [10]. Однак відсутність єдиного глобального механізму ускладнює ефективну координацію зусиль на міжнародному рівні. Запровадження універсальних стандартів, подібних до GDPR, може підвищити відповідальність урядів і технологічних компаній за поширення маніпулятивного цифрового контенту.

Ключову роль у подоланні викликів, пов'язаних з діпфейк-технологіями, відіграють OSINT та кібердипломатія. Завдяки методам OSINT, таким як аналіз цифрових слідів, візуальний і аудіоаналіз, можна ефективно виявляти та аналізувати синтетичний контент, що суттєво підвищує здатність країн та міжнародних організацій вчасно реагувати на загрози. Водночас кібердипломатія має сприяти розробці глобальних стандартів і механізмів відповідальності, а також політичній координації між державами для впровадження санкцій проти злочинців.

Лише через тісну співпрацю між державами, міжнародними організаціями та технологічними компаніями можна створити комплексну систему для виявлення і боротьби з діпфейками, що забезпечить стабільність і довіру у міжнародних відносинах. Інтеграція передових OSINT-технологій у практику кібердипломатії має стати основою для ефективного захисту міжнародної безпеки в епоху цифрових загроз.

---

1. Руднєва А. Інноваційні інформаційні технології у виборчих політичних комунікаціях. *Епістемологічні дослідження в філософії, соціальних і політичних науках.* 2024. Т. 7, № 2.
2. Міненко Є. Організаційно-правовий аналіз забезпечення інформаційної безпеки як фактор суспільно-політичної стабільності. *Науковий часопис УДУ імені Михайла Драгоманова. Серія 22. Політичні науки та методики викладання соціально-політичних дисциплін.* 2023. № 22(33).
3. Іслам М. Б. Е., Хасіб М., Батул Х., Ахташам Н., Мухаммад З. Загрози штучного інтелекту для політики, виборів і демократії: фреймворк перевірки автентичності на основі блокчейну. *Blockchains*. 2024. Т. 2, № 4

4. Закон про оперативну групу по боротьбі з deepfake (*Deepfake Task Force Act*): закон США від 24.05.2022 № S.2559. URL: https://www.congress.gov/ congressional-report/117th-congress/senate-report/114/1 (дата звернення: 20.03.2025)..

5. Едвардс Л. Закон ЄС про штучний інтелект: короткий огляд його значення та сфери застосування. Штучний інтелект (*Закон ЄС про штучний інтелект*). 2021. Т. 1.

6. Хельдт А. П. Закон ЄС про цифрові послуги: Біла надія регулювання посередників. Регулювання цифрових платформ: глобальні перспективи управління Інтернетом. *Cham: Springer International Publishing*, 2022.

7. Положення про управління глибоким синтезом інтернет-інформаційних сервісів (Provisions on the Management of Deep Synthesis of Internet Information Services): *закон КНР від 03.11.2022*. URL: https://www.cac.gov.cn/2022-12/11/c_1672221949354811.htm (дата звернення: 20.03.2025).

8. Gambín, Á. & Y. Deepfakes: current and future trends / Gambín, Ángel & Yazidi, Anis & Vasilakos, Athanasios & Haugerud, Hårek & Djenouri, Youcef. // *Artificial Intelligence Review*. 2024. Т. 57, № 3. DOI:10.1007/s10462-023-10679-x

9. Романчук О. Штучний інтелект в епоху нових медій. *Вісник Львівського університету. Серія Журналістика.* 2018. С. 179-188.

10. Зміцнення здатності засобів масової інформації застосовувати стандарти журналістики і просувати медіаграмотність. *OSCE Secretariat Extra-Budgetary Support Programme for Ukraine.* URL: https://www.osce.org/files/f/documents/e/8/579181.pdf (дата звернення: 26.03.2025).

Горбатенко Андрій,
викладач
ВСП «Фаховий коледж
Інформаційних технологій»
(Національний університет
«Львівська політехніка»)

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ОРД: ІНТЕГРАЦІЯ МЕТОДІВ OSINT, ШІ ТА СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Сучасні реалії боротьби зі злочинністю, особливо у контексті посягань на національну безпеку України, в тому числі шляхом проведення розвідувальних заходів в інформаційній сфері, вимагають докорінної трансформації підходів до інформаційно-аналітичного забезпечення оперативно-розшукової діяльності.

Одним із ключових елементів такої трансформації є системне використання технологій розвідки на основі відкритих джерел – OSINT. Інтеграція OSINT у традиційні механізми ОРД створює принципово нові можливості для виявлення, документування та запобігання злочинам, зокрема в умовах гібридної війни.

Застосовуючи OSINT, оперативні підрозділи отримують змогу виявляти потенційні загрози, ідентифікувати підозрюваних осіб, встановлювати інформаційні зв'язки, моніторити місця їхнього перебування та фіксувати ознаки протиправної діяльності на етапі зародження загрози.

Одним із різновидів інформаційних технологій збору та аналізу інформації з відкритих джерел є ще один напрямок розвідки – HUMINT (human intelligence), у дослівному перекладі – «розвідка по людях». До таких технологій відносяться: моніторинг соціальних мереж, опитування, соціальний інжиніринг, за легендовані бесіди (під виглядом журналіста, клієнта, роботодавця тощо). У сучасному світі технології OSINT та HUMINT значно пов'язані між собою і використовують значну кількість технологічно подібних методів отримання необхідної інформації про об'єкт розвідки [1]. Методи OSINT дозволяють легально отримувати великі обсяги релевантної інформації із відкритих джерел: соціальних мереж, відкритих реєстрів, форумів, ЗМІ, блогів, баз даних та іншого цифрового контенту.

Окремого огляду заслуговує метод збирання розвідувальної інформації саме з комп'ютерних соціальних мереж, як різновид OSINT. Моніторинг в режимі реального часу оновлень в Instagram, Facebook, та інших соціальних мереж дозволяє одержати потрібну інформацію про вчинені злочини або злочини, які плануються. Всі відомості, які залишають окремі правопорушники в мережі становлять оперативний інтерес. Володіння цією інформацією дозволяє встановити злочинців та, за можливістю, припинити їх протиправну діяльність.

На відміну від таємної інформації, перевірену інформацію з відкритих джерел можливо розповсюджувати та використовувати без застосування відповідних грифів, що дає змогу здійснювати обмін такою інформацією, оскільки при її добуванні не використовуються приховані методи та секретні джерела. Але слід зазначити, що можливо використовувати лише інформацію, а не аналітичну довідку з цієї інформації [2, с. 112].

Відкриті джерела перетворилися на повноцінне поле оперативної роботи, що дає змогу оперативно розширювати інформаційну базу без порушення процесуальних норм, що особливо важливо для подальшої допустимості доказів у кримінальному провадженні.

Інтеграція OSINT потребує відповідної організації роботи: створення окремих аналітичних груп у складі оперативних підрозділів, використання спеціалізованого програмного забезпечення для пошуку, обробки і верифікації даних, розробки внутрішніх протоколів збору доказової інформації. Зібрані дані мають проходити ретельну верифікацію: перехресне підтвердження фактів, встановлення джерела первинної публікації, аналіз контексту появи інформації. Особливу увагу слід приділяти фіксації електронних доказів відповідно до вимог кримінального процесуального законодавства України (статті 84, 99 Кримінального процесуального кодексу України, далі – КПК України), забезпечуючи їх належність, допустимість, достовірність та достатність.

Інтеграція OSINT не повинна розглядатись як альтернатива класичним методам ОРД. Навпаки, комбінація відкритої розвідки із традиційними заходами – агентурною роботою (конфіденційним співробітництвом), спостереженням, іншими ОРЗ – дозволяє точніше планувати оперативні комбінації, знижувати ризики провалів,

зменшувати ймовірність викриття особового складу та підвищувати загальну результативність оперативно-розшукової діяльності.

Окремий напрямок розвитку – залучення технологій штучного інтелекту (ШІ) для автоматизації процесів збору, аналізу і візуалізації даних. Зокрема, ШІ дозволяє здійснювати ідентифікацію осіб за зображеннями, відстежувати їхню цифрову активність, виявляти приховані зв'язки у великих обсягах інформації. Практика роботи також показала надзвичайну ефективність створення штучних образів (профілів) із використанням ШІ для проведення оперативних комбінацій: наприклад, створення віртуальних акаунтів вигаданих осіб, жіночих образів для встановлення контакту із потенційними зловмисниками, використання підробленого жіночого голосу та фотографій. Така діяльність значно підвищує ймовірність отримання від противника цінної оперативної інформації без безпосереднього ризику для оперативника.

Соціальна інженерія в цьому аспекті є методом, що дозволяє шляхом психологічного впливу, маніпуляції довірою та емоціями, отримувати доступ до закритої інформації. Техніки викликання довіри, ефект співчуття, інсценування певних ситуацій – усе це стає органічною частиною сучасної оперативної роботи із застосуванням OSINT і доповняє його.

Стаття 34 КУ гарантує право кожної особи на вільний збір, зберігання, використання та поширення інформації у будь-якій формі на власний розсуд. В межах кримінального провадження порядок здійснення аналізу відкритих джерел інформації регламентується положеннями глави 21 Кримінального процесуального кодексу України. Зокрема, п. 4 ч. 4 ст. 258 КПК України визначає процесуальні засади проведення такої негласної слідчої (розшукової) дії, як зняття інформації з електронних інформаційних систем.

Разом із тим, впровадження OSINT у практику ОРД стикається і з низкою викликів, насамперед правового характеру. На сьогодні в українському законодавстві відсутня чітка регламентація процедур використання інформації з відкритих джерел у межах оперативно-розшукової та слідчої діяльності. Це створює ризики щодо допустимості зібраних даних у кримінальному процесі та потребує відповідних змін на рівні нормативно-правових актів, включаючи розробку типової інструкції щодо збору, фіксації та використання OSINT-даних у межах ОРД.

У перспективі розвиток напрямку OSINT має базуватися на кількох ключових засадах: створенні в оперативних підрозділах окремих аналітичних груп для роботи з відкритими джерелами, проходженні діючими оперуповноваженими курсів щодо правильного використання засобів OSINT із високим рівнем цифрової гігієни та навичками роботи із засобами ШІ, впровадженні спеціалізованого програмного забезпечення, розробці внутрішніх протоколів верифікації даних.

Інтеграція методів OSINT у систему інформаційно-аналітичного забезпечення ОРД є необхідною умовою підвищення ефективності протидії злочинам, що загрожують національній безпеці України. Системний підхід до використання відкритих джерел, поєднаний із класичними оперативно-розшуковими методами, соціальною інженерією та технологіями штучного інтелекту, формує нову якість оперативної діяльності.

Водночас розвиток цієї сфери має супроводжуватися вдосконаленням правового регулювання, підготовкою спеціалістів нового типу та впровадженням сучасних технічних рішень, що відповідають вимогам сьогодення задля захисту національної безпеки України.

---

1. Білобров А. В., Клімушин П. С. ВИКОРИСТАННЯ ТЕХНОЛОГІЙ OSINT ДЛЯ ОТРИМАННЯ ІНФОРМАЦІЇ. Протидія кіберзлочинності та торгівлі людьми: Збірник матеріалів Міжнародної науково-практичної конференції (27 травня 2020 року, м. Харків). Харків, 2020, с. 135-136.
2. Ісмайлов К. Ю. Особливості кримінальної розвідки з відкритих джерел як інструмент збирання оперативної інформації / К. Ю. Ісмайлов // Південноукраїнський правничий часопис. 2016. № 2. С. 110-113. http://nbuv.gov.ua/UJRN/Pupch_2016_2_32.

Горошко Олександр,
здобувач ступеня доктора філософії у галузі права
кафедри оперативно-розшукової діяльності
(Львівський державний університет
внутрішніх справ)
Мовчан Анатолій,
доктор юридичних наук, професор,
професор кафедри оперативно-розшукової діяльності
(Львівський державний університет
внутрішніх справ)

БОРОТЬБА З ОРГАНІЗОВАНОЮ ЗЛОЧИННІСТЮ В РЕГІОНІ СХІДНОГО ПАРТНЕРСТВА: ВИКЛИКИ ТА ПЕРСПЕКТИВИ

Правоохоронні органи Європи об'єднали зусилля під час Днів спільних дій EMPACT у Південно-Східній Європі (JAD SEE) 2024. Координаційний центр, створений у Сараєво, об'єднав фахівців із 26 країн, які діяли спільно проти основних загроз організованої злочинності в регіоні. У рамках операції, яка тривала під гаслом «Об'єднати сили проти організованої злочинності», понад 31 тисяча офіцерів поліції здійснювали перевірки як у фізичному просторі, так і в Інтернеті – у тому числі в темній мережі та на соціальних платформах. До кіберактивностей долучилися також прокурори з різних юрисдикцій, що дозволило значно посилити ефективність дій. Основними напрямами роботи стали боротьба з торгівлею людьми, контрабандою мігрантів, незаконною торгівлею наркотиками та зброєю, а також ліквідація діяльності злочинних мереж високого ризику.

Результати масштабної операції вражають: затримано 796 осіб, розпочато 316 розслідувань, вилучено 442 одиниці вогнепальної зброї, перевірено понад 655 тисяч осіб, транспортних засобів, поштових відправлень та об'єктів. Активну участь в операції JAD SEE 2024 взяли партнери із Західних Балкан, країни Східного партнерства, серед яких Молдова та Україна, а також Туреччина. Пліч-о-пліч працювали агентства та проєкти як країн ЄС, так і поза ним, створюючи справжній єдиний фронт у боротьбі з організованою

злочинністю. Проєкт охоплює правоохоронні органи, сектор безпеки, судову систему та прокуратуру країн Східного партнерства [1].

Європол відіграв важливу роль у проведенні цієї операції, направивши мобільні офіси з експертами, які здійснювали перевірку даних у режимі реального часу. До боротьби активно долучалися спеціалізовані пошукові підрозділи, кінологічні групи, експерти з методів приховування і фахівці з документальних шахрайств. Проєкт EU4FAST забезпечив створення координаційного центру в Сараєво та підтримав залучення країн Західних Балкан, Молдови, України, Туреччини, окремих держав-членів ЄС та Інтерполу до активної фази операції. Дана ініціатива реалізується під егідою Європейської мультидисциплінарної платформи проти злочинних загроз (EMPACT) – інструменту ЄС для боротьби з тяжкими злочинами та організованою злочинністю у глобальному масштабі. Успіх JAD SEE 2024 підкреслює силу спільного підходу і важливість дій, керованих розвідувальною інформацією, у протидії складним міжнародним злочинним мережам. Відтак, Європол розширює свою підтримку країнам Східного партнерства – Вірменії, Азербайджану, Молдові, Грузії та Україні – у боротьбі з організованою злочинністю, зокрема організація інвестує 1,8 мільйона євро у фінансування спеціального проєкту та бере на себе його управління. Проєкт «Боротьба з організованою злочинністю в регіоні Східного партнерства» має на меті посилити оперативні та стратегічні можливості країн регіону відповідно до ініціативи ЄС EMPACT. Особливий акцент робиться на зміцненні співпраці між країнами Східного партнерства та державами-членами ЄС [1].

Ініціатива сприятиме покращенню координації дій у боротьбі з міжнародною організованою злочинністю, розширенню співпраці з європейськими правоохоронними агенціями та впровадженню політичного циклу ЄС у сфері безпеки. Проєкт також допоможе залучити інші зацікавлені сторони в регіоні та забезпечити взаємодію з проєктами ЄС на місцях через тісну співпрацю з делегаціями Європейського Союзу.

Водночас 1 січня 2025 року Європол офіційно запустив другу фазу проєкту «Боротьба з організованою злочинністю в регіоні Східного партнерства», яка триватиме до кінця 2028 року. Мета нової фази – зміцнити досягнення першого етапу (2020–2024 роки), розширити партнерські мережі та зробити регіон безпечнішим для

громадян. У рамках цього проєкту Європол поглиблюватиме співпрацю між державами-членами ЄС, установами Європейського Союзу та країнами Східного партнерства. Особливу увагу приділять залученню країн-кандидатів до найкращих європейських практик у боротьбі з організованою злочинністю. На другому етапі передбачено: впровадження грантової програми для підтримки стратегічних і операційних заходів, зокрема в рамках Операційних планів дій EMPACT; проведення двосторонніх зустрічей із правоохоронними органами країн-партнерів для активізації співпраці; організація оперативних і стратегічних зустрічей між країнами Східного партнерства, ЄС та іншими міжнародними партнерами; підтримка участі дослідників із країн регіону в заходах та конференціях Європолу; проведення інформаційних сесій для нових національних координаторів EMPACT; сприяння транскордонним операціям за пріоритетними напрямами боротьби зі злочинністю в межах EMPACT. Завдяки активній координації та обміну інформацією Європол відіграє ключову роль у посиленні безпеки як у межах ЄС, так і за його кордонами [2].

Крім того, у січні 2025 року Європол і Євроюст оголосили про старт третьої фази проєкту SIRIUS – ініціативи, що вже шість років успішно допомагає національним правоохоронним і судовим органам працювати з електронними доказами. Нова фаза продовжить підтримувати правоохоронців, суди та постачальників послуг у навігації складним правовим середовищем. Проєкт сприятиме тіснішій співпраці між державним і приватним секторами, підвищуючи ефективність розслідувань у цифрову епоху. Зміни в законодавстві, зокрема прийняття Другого додаткового протоколу до Будапештської конвенції та погодження тексту Конвенції ООН про кіберзлочинність, істотно впливають на правила роботи з електронними доказами. У цьому контексті SIRIUS утвердився як європейський центр передового досвіду в галузі транскордонного доступу до цифрових даних. На сьогодні спільнота SIRIUS об’єднує компетентні органи з понад 50 країн, включаючи всі держави-члени ЄС, та співпрацює з більш ніж 220 постачальниками послуг. Проєкт підтримує понад 8500 представників правоохоронних і судових органів, надаючи їм доступ до інструкцій, тренінгів та інструментів для роботи з електронними доказами. У майбутньому, з урахуванням нових європейських та міжнародних правових рамок,

Європол і Євроюст планують розширити місію SIRIUS і збагатити портфоліо його послуг, забезпечуючи безперервну підтримку своїм партнерам під час важливого етапу трансформації [3].

У рамках третьої фази проєкту SIRIUS Європол і Євроюст зосередять зусилля на розробці нових інструментів розслідування, проведенні масштабних заходів та розширеному розвитку потенціалу національних правоохоронних і судових органів. Проєкт допоможе LEA та JA підготуватися до впровадження майбутнього законодавчого пакету ЄС щодо електронних доказів, а також до інших змін у правилах транскордонного доступу до цифрових даних. SIRIUS також планує розширити свою діяльність за межі ЄС, зміцнюючи співпрацю з третіми країнами. Такий підхід стане важливим кроком у боротьбі з організованою злочинністю та тероризмом у глобальному масштабі. Спираючись на багаторічний досвід і міцні партнерські мережі Європолу та Євроюсту, проєкт SIRIUS впевнено переходить у нову фазу, забезпечуючи, щоб європейські правоохоронні та судові органи залишалися лідерами в сфері інноваційних підходів до роботи з електронними доказами [3].

---

1. 796 arrests in massive EU action against organised crime URL: https://www.europol.europa.eu/media-press/newsroom/news/796-arrests-in-massive-eu-action-against-organised-crime

2. Eastern Partnership (EaP) project URL: https://www.europol.europa.eu/operations-services-and-innovation/eastern-partnership-project-eap

3. Europol and Eurojust launch Phase 3 of SIRIUS project URL: https://www.europol.europa.eu/media-press/newsroom/news/europol-and-eurojust-launch-phase-3-of-sirius-project

Гутник Аліна,
доктор філософії у галузі права,
інспектор Служби освітньої безпеки
(Калуський РВП ГУНП в Івано-Франківській області)

ШТУЧНИЙ ІНТЕЛЕКТ І ДЕЗІНФОРМАЦІЯ В УМОВАХ ВІЙНИ: ВИКЛИКИ ДЛЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Важливе місце під час війни посідає інформаційна безпека. Сьогодні, росія системно проводить дезінформаційну політику щодо України та активно використовує соціальні мережі провокуючи внутрішні конфлікти між громадянами. Окрім створення фейкових сторінок, дописів, агенти впливу використовують ШІ для створення максимально реалістичних зображень, які практично неможливо відрізнити від справжніх.

Росіяни спеціально створюють псевдопатріотичні групи та поширюють створені за допомогою ШІ зображення, неправдиві емоційні історії із життя українців тощо для інформаційних вкидів, розколу суспільства на тригерних темах, тестування аудиторії на вразливість до патріотичних та емоційних фейків. Потім на людей, які це поширюють чи коментують, можна таргетувати рекламу та планувати інші інфоатаки, використовуючи ці вразливості [1, с. 1099]. Тому, кожен повинен вміти перевіряти інформацію, яка поширюється в Інтернеті.

Одним із прикладів дезінформації, поширеної через соціальні мережі, є дописи на сторінці під ніком «Aljoan Monisit Orbuda» у Фейсбуці [2]. На сторінці найбільше лайків та коментарів під фото на яких зображено протезованих людей у військовій формі, або батьків і дітей у стані сильних емоцій. Всі ці дописи супроводжуються емоційними надписами, які підштовхують людей реагувати, ставити лайки та писати коментарі. Очевидно, що перш ніж поширювати такий контент чи реагувати на нього слід перевірити сам допис і обліковий запис.

Перевірка допису та зображення.

Написана інформація про подію чи людину є малоінформативною. Жодної конкретики та джерела інформації, що викликає сумніви у достовірності такої публікації.

Зображення згенероване ШІ має типові проблеми – непропорційні, перекручені об'єкти, неправильні тіні, розмиті або занадто деталізовані об'єкти (надписи), відсутність логіки тощо. Наприклад, на одному із фото у військового обидві ампутовані кінцівки виглядають ідеально гладкими, ніби пластиковими, а поруч окуляри та годинник як один об'єкт, також від хлопця падає надмірно велика тінь [3], на іншому – дівчина з двома (чомусь різними?) протезами, незрозумілі надписи на вивісках магазинів, дивні символи на цінниках, а люди позаду виглядають як манекени [4]. Отже, ці зображення – створені за допомогою ШІ.

Також для перевірки можна використати OSINT-інструменти:

1) Пошук за зображенням (Google Images, Yandex Images чи TinEye) – можна знайти де це зображення було опубліковано раніше, що допомагає визначити, чи не є воно фальшивим.

2) Аналіз метаданих (FotoForensics) – можна визначити, чи було зображення змінено після його створення, а також порівняти дані про формат і розмір файлу.

3) Перевірка на генерацію за допомогою ШІ (Hive Moderation або AI Or Not).

Аналіз профілю облікового запису.

Сторінка створена 09.04.2022, а основна країна проживання людей, які керують цією сторінкою – Індонезія. Цей профіль відстежує тільки 3 людей, натомість на нього підписано 35 тис. підписників. Основний контент – емоційно насичені матеріали через шокуючі зображення чи неправдиві новини, часто пов'язані з війною.

На обкладинці профілю розміщено фото жінки на фоні графіті. Здійснивши пошук за цим зображенням через Google Images вдалося встановити, що фото реальне і зроблене у Новій Каледонії. Оригінал цього фото розміщено на YouTube-каналі «Елла Австралия TV» [5]. Його авторка не публікує ні дезінформаційні матеріали, ні зазначає про наявність сторінки у Фейсбук (хоча вказує покликання на чотири інші соцмережі). Тож, розуміємо що на обкладинку використано оригінальне фото, скоріш за все, без дозволу її власниці.

Отже, знання інструментів OSINT є необхідним для всіх, хто користується соцмережами, адже дозволяє виявити фейкові аккаунти, неправдиві публікації та вберегти громадськість від дестабілі-

заційних маніпуляцій. Особливого значення набуває розвиток медіаграмотності серед усіх громадян, оскільки здатність розпізнавати дезінформацію є необхідною умовою підтримання інформаційної безпеки держави.

---

1. Басиста І., Гутник А., Хитра А. Розпізнавання DEEPFAKES як домінантна складова протидії інформаційним загрозам. *Сектор безпеки і оборони України на захисті національних інтересів: актуальні проблеми та завдання в умовах воєнного стану :* тези III Міжнародної науково-практичної конференції (Хмельницький, 21 листопада 2024 року). Хмельницький : Видавництво НАДПСУ, 2025. С. 1097–1099.
2. Aljoan Monisit Orbuda. *Facebook.* URL: https://www.facebook.com/profile.php?id=100080711082065 (дата звернення: 28.04.2025).
3. Допис користувача Aljoan Monisit Orbuda. *Facebook.* 28.04.2025. URL: https://www.facebook.com/share/p/16o5gRKLcC/ (дата звернення: 28.04.2025).
4. Допис користувача Aljoan Monisit Orbuda. *Facebook.* 26.04.2025. URL: https://www.facebook.com/share/p/15Tc2aFt9V/ (дата звернення: 28.04.2025).
5. ЭЛЛА АВСТРАЛИЯ СЕКОНД ХЕНД ПОИСК КЛАДА ШПЕРМЮЛЬ. *YouTube.* URL: https://www.youtube.com/@ellaaustralia (дата звернення: 28.04.2025).

Гуцуляк Юрій,
доктор філософії в галузі права,
старший викладач
кафедри кримінального процесу
та криміналістики факультету № 1
(Львівський державний університет
внутрішніх справ)

РОЛЬ OSINT-ДОСЛІДЖЕНЬ У ПІДВИЩЕННІ РІВНЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Останніми десятиліттями Україна відчуває на собі реальну необхідність захисту своєї національної безпеки. Необхідність стала носити характер не просто декларативного інституту у правозастосовному та правотворчому полі, а характеру реальних забезпечення та боротьби. Загрози національній безпеці є багатовекторними, що зумовлює необхідність розроблення дієвого інструментарію попередження, подолання та реагування на них.

Стаття 3 Закону України «Про національну безпеку України» визначає, що державна політика у сферах національної безпеки і оборони спрямована на захист: людини і громадянина - їхніх життя і гідності, конституційних прав і свобод, безпечних умов життєдіяльності; суспільства – його демократичних цінностей, добробуту та умов для сталого розвитку; держави – її конституційного ладу, суверенітету, територіальної цілісності та недоторканності; території, навколишнього природного середовища – від надзвичайних ситуацій.

Основними складовими забезпечення національної безпеки є:

1) захист державного ладу;

2) захист суспільного ладу;

3) забезпечення територіальної недоторканності та суверенітету;

4) забезпечення політичної та економічної незалежності нації;

5) забезпечення здоров’я нації;

6) охорона громадського порядку;

7) боротьба зі злочинністю;

8) забезпечення техногенної безпеки і захист від загроз стихійних лих [4, с.322].

Порушення вказаних складових в основному здійснюється шляхом вчинення кримінальних правопорушень. А захист зазначених об'єктів та правовідносин покладається на державні органи та посадових осіб, шляхом: створення дієвої системи превентивної діяльності; правового забезпечення охорони прав і свобод людини і громадянина, власності, громадського порядку та громадської безпеки, довкілля, конституційного устрою України від кримінально-протиправних посягань, забезпечення миру і безпеки людства, а також запобігання кримінальним правопорушенням (ст. 1 КК України); захисту особи, суспільства та держави від кримінальних правопорушень (ст. 2 КПК України).

Державна політика в контексті реагування за фактами, визначених в законі охоронюваних об'єктів, відбувається шляхом проведення досудового розслідування та подальшого судового розгляду, з тим щоб кожний, хто вчинив кримінальне правопорушення, був притягнутий до відповідальності в міру своєї вини.

З початком агресії рф проти України в лютому 2014 року гостро постало питання про документування (виявлення і фіксацію у встановленій формі інформації про певні події та обставини) [5, с. 73-74]. А з часу повномасштабного вторгнення у відкритій війні проти України, питання встановлення та фіксації фактів про вчинювані кримінальні правопорушення набуло нової актуальності, масовості та особливостей вчинення. Згідно даних Офісу Генерального прокурора станом на 23.10.2024 зареєстровано більш як 142000 злочинів, передбачених ст. 438 КК України, та понад 19600 кримінальних правопорушень проти основ національної безпеки України [7]. Значна частина злочинів вчиняється на окупованих територіях України. Належного доступу до можливості швидкого виявлення та фіксації доказів не має, що утруднює проведення досудового розслідування.

Такий стан речей вимагає вироблення нових підходів до усунення таких негативних факторів для розслідування кримінальних правопорушень. Слідча практика розслідування воєнних злочинів, які вчинені на окупованих територіях, показала, що мало не єдино можливим способом виявлення, отримання та фіксації доказів про обставини вчинення воєнних кримінальних правопорушень, а та-

кож про осіб, котрі могли б вчинити їх є моніторинг відкритих джерел в кіберпросторі. Іншими словами застосування OSINT.

Аналізуючи матеріали судових розглядів, котрі доступні на сьогоднішній день, а також чинне кримінальне процесуальне законодавство, мусимо констатувати, що в Україні ані слідчий інструментарій, ані чинне законодавство в повній мірі не виявились готовими до використання у кримінальних провадженнях інформації (фактичних даних) в доказуванні, отриманих поза джерелами доказів передбачених ч. 2 ст. 84 КПК України.

З одного боку, процесуальна форма та фундаментальні положення доказового права не дозволяють розширювати ні перелік джерел доказів, ні видів слідчих (розшукових) дій, котрі б відповідали змісту проведення OSINT. Це викликає численні запитання в правозастосовній практиці в процесі судового розгляду, з позиції допустимості використання даних отриманих в ході OSINT-досліджень.

На часі виникло комплексне завдання для суб'єктів правотворчої та правозастосовної діяльності. Основними напрямки якого є:

1. вдосконалення норм Кримінального процесуального кодексу у частині обставин визначення електронних (цифрових) даних як джерел доказів у кримінальному провадженні;
2. розроблення методики виявлення, фіксації та перевірки даних отриманих в ході процесуальної діяльності з OSINT;
3. розроблення технічного інструментарію роботи з електронними даними в кримінальному провадженні.

На наш погляд, це першочергові вектори, котрі повинні стати запорукою дієвого забезпечення національної безпеки України, шляхом здійснення розслідування кримінальних правопорушень, котрі направлені на її загрозу.

---

1. Закон України «Про національну безпеку України». URL: https://zakon.rada.gov.ua/laws/show/2469-19?find=1&text (дата звернення: 01.05.2025).
2. Кримінальний кодекс України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 01.05.2025).
3. Кримінальний процесуальний кодекс України. URL: https://zakon.rada.gov. ua/laws/show/4651-17#Text (дата звернення: 01.05.2025)
4. Кубецька О.М. Умови забезпечення національної безпеки держави / О.М. Кубецька, Т.М. Остапенко, Я.С.Палешко / Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2020. № 2 (105). С. 321-327.

5. Пашковський М. І. Документування міжнародних злочинів неурядовими організаціями і використання отриманої цифрової інформації у кримінальних провадженнях за статтею 438 КК України. Альманах наукових праць фахівців Науково-дослідного інституту вивчення проблем злочинності імені академіка В.В. Сташиса Національної академії правових наук України за результатами досліджень у 2022 р. / редкол.: В.С. Батиргареєва, В.І. Борисов, Д.П. Євтєєва та ін.; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України. Харків, 2023. С. 70–80.

6. Торбас О.О. OSINT при розслідуванні кримінальних правопорушень : підручник. Одеса : Вид-во «Юридика», 2024. 180 с.

7. Злочини, вчинені в період повномасштабного вторгнення рф. Станом на 23.10.2024. Офіс Генерального прокурора. URL: https://www.gp.gov.ua/storage/uploads/45127fca-e828-4f9f-a6a1-f3231cf26/warcrime-23102024ua.jpg.

Демедюк Сергій,
кандидат юридичних наук,
заступник Секретаря
(Рада національної безпеки і оборони України)

ІНТЕГРАЦІЯ OSINT В СИСТЕМУ КІБЕРБЕЗПЕКИ ДЕРЖАВИ: СТРАТЕГІЧНІ ТА ПРИКЛАДНІ АСПЕКТИ

Інформаційна відкритість сучасного цифрового середовища відкриває безпрецедентні можливості для збору, аналізу та інтерпретації даних, що формуються у відкритих джерелах. Open Source Intelligence (OSINT) перетворюється на невід'ємний інструмент забезпечення національної безпеки, а його інтеграція в систему кібербезпеки держави – на стратегічне завдання в умовах гібридної війни, цифрової трансформації та зростання ролі інформаційного простору як арени конфліктів. Для України, яка перебуває у стані збройної боротьби з агресором, ефективне використання OSINT має не лише оперативне, але й екзистенційне значення.

OSINT – це систематизована діяльність із добування, аналізу та інтерпретації інформації з відкритих джерел: інтернету, соціальних мереж, відкритих баз даних, супутникових знімків, засобів масової інформації, форумів, даркнету, офіційної звітності тощо. На відміну від закритих джерел (HUMINT, SIGINT тощо), OSINT не потребує прихованих методів добування інформації, однак вимагає високої експертизи для відсіву фейків, маніпуляцій та дезінформації.

У кібербезпековому вимірі OSINT забезпечує *раннє виявлення загроз* (включаючи ознаки кібератак, витоки даних, активність бот-мереж), *атрибуцію атак* (зокрема через збір даних про групи хакерів, їхні інфраструктури та цифрові відбитки), *оцінку вразливостей* критичної інфраструктури через аналіз відкритих технічних даних, *контррозвідувальне забезпечення* (виявлення дезінформаційних кампаній, фішингових кампаній та елементів інформаційно-психологічних операцій (ІПсО)).

Таким чином, OSINT виступає одночасно як превентивний, аналітичний та доказовий інструмент у системі кібербезпеки.

Для того щоб OSINT був ефективно інтегрований у державну систему кібербезпеки, необхідно сформувати загальнодержавну

концепцію, яка б визнавала відкриту розвідку як повноцінний елемент національного безпекового інструментарію. Таке визнання має знайти своє відображення у національних стратегічних документах, у тому числі з оновленою Стратегією кібербезпеки, Національним планом реагування на кіберінциденти та доктриною інформаційної безпеки. Важливо, щоб на рівні державної політики було визначено місце OSINT у структурі забезпечення інформаційної та кібербезпеки, з його використанням для виявлення дезінформаційних кампаній, інформаційно-психологічних операцій, а також у під час розслідування кіберзлочинів.

Важливою передумовою ефективної інтеграції OSINT є створення інституційної основи. В Україні досі не існує єдиного координаційного органу, який би відповідав за розвиток та системну реалізацію політики у сфері відкритої розвідки. Тому доцільним є створення *Національного центру OSINT*, який міг би функціонувати у структурі Ради національної безпеки і оборони або як окремий міжвідомчий орган у взаємодії з Державною службою спеціального зв'язку та захисту інформації, Службою безпеки України, Кіберполіцією, Міністерством оборони та іншими суб'єктами сектору безпеки. Такий центр міг би координувати зусилля різних структур, формувати спільну аналітичну базу, забезпечувати обмін результатами досліджень та забезпечувати відповідну стандартизацію діяльності у сфері OSINT.

Не менш важливою складовою інтеграції є розробка єдиних методологічних стандартів. В умовах великої кількості джерел та високого рівня інформаційного шуму необхідно впровадити критерії перевірки достовірності інформації, методики аналізу достовірності джерел, правила документування та архівування даних. Це також має включати процедури збереження доказової інформації, яка може бути використана у правовому процесі, а також визначення правових і технічних стандартів взаємодії OSINT-аналітиків із правоохоронними та розвідувальними структурами.

Технологічна база є ще одним ключовим чинником. Сучасна аналітика OSINT базується на використанні спеціалізованих програмних засобів, таких як системи автоматизованого збору даних (web crawlers), парсери, інструменти для виявлення цифрових відбитків (digital footprinting), платформи для аналізу соціальних мереж, системи аналізу супутникових знімків, а також інструменти

візуалізації та картографування зібраної інформації. Розвиток національної програмної інфраструктури у цьому напрямі потребує залучення інноваційного потенціалу вітчизняних компаній та стартапів, які вже активно працюють у сфері OSINT та кіберрозвідки.

Не менш важливою є підготовка відповідних кадрів. Станом на сьогодні кадровий потенціал у сфері відкритої розвідки є обмеженим. Відсутність спеціалізованих освітніх програм, невизначеність правового статусу OSINT-діяльності, а також недостатня кількість сертифікаційних курсів ускладнює процес формування професійної спільноти аналітиків. Потрібно розробити стандартизовані навчальні програми для студентів ІТ-спеціальностей, права та національної безпеки, ввести обов'язкову підготовку з елементами OSINT для співробітників кіберполіції, СБУ, військових аналітиків, а також запровадити систему післядипломної освіти та підвищення кваліфікації у цій сфері.

Юридичне регулювання є окремим та важливим питанням. Застосування OSINT у кримінальних провадженнях, оперативно-розшуковій та розвідувальній діяльності потребує чіткого врегулювання. На сьогодні законодавство України не визначає повноцінно статус відкритих джерел як доказів у судовому процесі. Це створює певну правову невизначеність. Необхідно внести відповідні зміни до Кримінального процесуального кодексу, закону про оперативно-розшукову діяльність, закону про розвідку, а також до підзаконних нормативних актів, що регулюють роботу спеціальних служб. Важливо забезпечити баланс між правом держави на захист безпеки та правом громадян на захист персональних даних, що є актуальним як у національному, так і в європейському контексті.

Окремої уваги потребує взаємодія держави з громадянським суспільством та волонтерськими ініціативами, які вже довели свою ефективність у сфері відкритої розвідки. Український досвід, зокрема діяльність таких спільнот, як InformNapalm, OSINT-UA, Molfar, Bellingcat та інших, показує, що громадські аналітики здатні оперативно і точно ідентифікувати ворожі угрупування, викривати схеми фінансування окупаційних адміністрацій, а також розкривати злочини, вчинені під час бойових дій. Держава має створити правові механізми залучення таких структур до офіційного процесу реагування на загрози, забезпечити підтримку їх діяльності, включно з технічними ресурсами, правовою допомогою та доступом до відкритих державних реєстрів.

Таким чином, інтеграція OSINT у систему кібербезпеки держави має розглядатися як складова загального реформування сектору національної безпеки. Вона повинна базуватися на чітко визначеній стратегії, інституційному забезпеченні, законодавчій підтримці, розвитку кадрового потенціалу та побудові сучасної технологічної інфраструктури. Лише за таких умов можна забезпечити ефективне використання відкритої інформації для виявлення, попередження та нейтралізації кіберзагроз, які дедалі більше стають ключовими інструментами сучасної війни.

Дуженко Олександра,
здобувач ступеня магістра
(Національна академія Служби безпеки України)

ВИКОРИСТАННЯ OSINT-ТЕХНОЛОГІЙ У КІБЕРПРОСТОРІ ДЛЯ ВИЯВЛЕННЯ І РОЗСЛІДУВАННЯ РОСІЙСЬКОЇ АГРЕСІЇ

Одним із шляхів забезпечення військової та стратегічної переваги є збір даних супротивника у кіберпросторі, це допомагає чинити опір та підривати превентивно плани ворога, виявляти та розслідувати воєнні злочини, що в подальшому формує масиви інформації, які збираються у доказову базу воєнних злочинів проти України. За допомогою певних інструментів та технологій кіберрозвідка можлива через відкриті джерела – OSINT (Open Source Intelligence). Величезний обсяг інформації, що міститься в домені з відкритим вихідним кодом, пропонує аналітикам достатньо доступних даних, надто цінних, щоб їх повністю відкинути. Варто лише поглянути на проникливі спостереження досвідчених професіоналів, які охоплюють усю розвідувальну спільноту та військову. Генерал-лейтенант Семюел В. Вілсон, колишній директор Розвідувального управління Міністерства оборони США, стверджує, що OSINT надає приблизно 90 відсотків інформації, яка використовується розвідувальною спільнотою.[1] Роберт Карділло, директор Національного агентства геопросторової розвідки, стверджував, що «несекретну інформацію більше не слід розглядати як доповнення до секретних джерел, а скоріше має бути навпаки».[2] Військова аналітика OSINT об'єднує у собі різні типи завдань: геопросторова розвідка, пошук військових злочинців, фактчекінг воєнних подій, розслідування воєнних злочинів. Головні цілі – отримання інформації про дислокацію та пересування формувань противника, його озброєння та техніку, особовий склад, бойові завдання та утримувані населені пункти. А в умовах сучасних конфліктів значну частину цієї інформації можна отримати, організувавши постійний моніторинг мережі Інтернет. Серед іншого, при плануванні та підготовці військових дій чи їх розслідування збоку окупанта доцільно використовувати сервіси для підвищення точності супутникових знімків. Симулятори сонячної системи, відстеження супутників, супутникові карти та їхні візуалізації. Мапи моніторингу інцидентів, ідентифікація боєприпасів, зброї, БПЛА, уніформи, екіпі-

рування, техніки тощо. Геопросторова розвідка: топографія, геологія, метеоаналізатори, рослинність, історичні карти, перегляд вулиць, карти для вираховування зі тінями, карти стихійних лих, океанів тощо. Ідентифікація/розпізнавання транспорту, відстеження суден, літаків, поїздів та громадського транспорту. Перевірка транспорту за країнами, міжнародна база даних викрадених транспортних засобів тощо. Більшість соціальних мереж надають можливість пошуку контенту за місцезнаходженням. Розслідування воєнних злочинів, важливим є встановлення факту злочину, визначення жертв та винуватців, подальша розвідка особистостей злочинців. Військова аналітика постійний процес збору даних: про злочинців, події в їхньому житті, пов'язаних осіб, загальні переміщення та навіть конкретне місцеперебування. Ця інформація потрібна для притягнення злочинців до відповідальності. Технології допомагають у пошуку полонених, безвісти зниклих або насильно депортованих, викрадених як військових так і цивільних осіб. Один з кейсів, як приклад виявлення, розслідування і підтвердження воєнного злочину російської армії проти цивільного населення - ідентифікація російської ракети, що знищила дитячу лікарню в Києві. Аналіз відкритих джерел, а також дані експертів з ракетної галузі вказали на те, що дитячу лікарню в Києві вразила крилата ракета Х-101, запущена Росією, що спростовує заяви проросійських джерел та осіб, які заперечували відповідальність та намагалися перекласти провину за інцидент на Україну. Аналіз, проведений Bellingcat з використанням відео із соціальних мереж, а також 3D-моделі ракети, вказує на те, що боєприпас був російською крилатою ракетою Х-101 . Цей аналіз узгоджується з думкою експертів, зокрема Фабіана Гоффмана , наукового співробітника з докторським ступенем в Університеті Осло, який спеціалізується на ракетних технологіях.[3]

Отже, набір інструментів та опанування навичок використання технологій OSINT задля військової розвідки дозволяє зібрати масивні дані та обробити їх для подальшого здійснення супротиву російській агресії, збирати масиви даних, що є підтвердженням здійснення воєнних злочинів, багато інструментів дозволяють, як виявляти так і розслідувати дані акти агресії, як в кіберпросторі, так і в реальному житті під час бойових дій або їх плануванні, також у запобіганні тих чи інших помилок стратегічного й тактичного характеру.

1. Libor Benes, «OSINT, New Technologies, Education: Expanding Opportunities and Threats. A New Paradigm,» *Journal of Strategic Security* 6, no. S3 (2013): S24, http://dx.doi.org/10.5038/1944-0472.6.3S.3. (дата звернення 21.04.2025)

2. Heather J. Williams and Ilana Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise* (Santa Monica, CA: RAND Corporation, 2018). (дата звернення 21.04.2025)

3. https://www.bellingcat.com/news/2024/07/09/russian-missile-identified-in-kyiv-childrens-hospital-attack/ (дата звернення 22.04.2025)

Єрмолаш Рєнат,
здобувач вищої освіти
(Харківський національний юридичний
інститут імені Ярослава Мудрого)

РОЗСЛІДУВАННЯ ВОЄННИХ ЗЛОЧИНІВ ЖУРНАЛІСТАМИ ЗА ДОПОМОГОЮ OSINT-ТЕХНОЛОГІЙ

Наразі OSINT став доволі сучасним та відомим терміном, який активно використовується в сучасній інформаційній війні. Простими словами, це розвідка з відкритих джерел. Тобто все, що ми бачимо в інтернеті, можна використовувати як інформацію для аналітики. Зокрема, під час розслідування воєнних злочинів OSINT допомагає ідентифікувати підозрюваних, встановлювати хронологію подій та знаходити докази. В цьому тексті, я розповім про те, як журналісти використовують OSINT для розслідування воєнних злочинів.

Журналісти, почали активно використовувати розвідку з відкритих джерел після початку війни в 2014 році. Тоді це стало початком для майбутніх гучних розслідувань. Одним з найвідоміших на той час справ було розслідування журналістів Bellingcat щодо можливих причетних до збиття рейсу MH17 «Малазійських авіаліній» у липні 2014 року. Слідча група заявила, що «Боїнг» збили з ракетної установки «Бук» проросійські бойовики. Тоді установку «Бук» вдалося ідентифікувати завдяки низці її унікальних рис, які прослідкували по фото- та відеоматеріалам, зокрема й з соцмереж очевидців. Вже потім, 19 червня 2019 р. прокуратура Нідерландів на основі розслідування JIT пред'явила звинувачення чотирьом підозрюваним: московитам Ігорю Гіркину, Сергію Дубинському, Олегу Пулатову і громадянину України Леоніду Харченку.

Звісно ж, українські журналісти теж активно почали використовувати OSINT-технології. Одними із таких, стали матеріали OSINT-ерів з медіапроєкту «Телебачення Торонто». Вони розслідували матеріали про воєнні злочини –наприклад, матеріал про Авдіївку і вихід наших військовослужбовців з позиції «Зеніт». Вони ідентифікували російського командира, який заходив на «Зеніт» і, ймовірно, віддав наказ убити полонених українців. В подальшому, ці дані можуть бути використані як докази в міжнародних судах.

Весь цей обсяг інформації який надають журналісти, дозволяє збирати докази порушень міжнародного гуманітарного права. Фіксувати факти обстрілів, наслідки атак на цивільну інфраструктуру, ідентифікувати підрозділи або окремих осіб, які можуть бути причетними до злочинів. В більшості випадків саме завдяки відкритим даним вдається підтвердити або спростувати злочини.

Також OSINT допомагає верифікувати контент. З початком активної інформаційної війни надзвичайно важливим стало перевірка джерел, місць й часу зйомки, геолокацій відео чи фото. Завдяки аналітичним інструментам журналісти перевіряють достовірність матеріалів і будують об'єктивну картину подій.

Звісно ж, використання цієї технології супроводжується серйозними викликами. Це і необхідність забезпечення достовірності інформації, і дотримування міжнародних правових стандартів при зборі та використанні інформації, для того щоб не порушувати права людини та не наражати на небезпеку жертв або свідків злочинів.

OSINT став революційним інструментом у сучасній журналістиці, особливо у сфері розслідування воєнних злочинів. Його цінність полягає в здатності швидко та точно фіксувати події, які відбуваються у важкодоступних або небезпечних для журналістів місцях. В умовах гібридної війни OSINT допомагає виявляти правду, спростовувати дезінформацію та доносити до суспільства достовірні факти.

Це робить журналістів не просто свідками, а й активними учасниками процесу встановлення справедливості, бо зібрані ними дані можуть бути використані не тільки у ЗМІ, але й у судах, включаючи міжнародні трибунали. Тому навичка роботи з відкритими джерелами є не лише професійною перевагою, а й моральним обов'язком журналіста в умовах війни.

---

1. MH17: Bellingcat назвала фігурантів збиття літака та їхні ролі - BBC News Україна. *BBC News Україна*. URL: https://www.bbc.com/ukrainian/news-48689274 (дата звернення: 09.04.2025).
2. OSINT-розслідувач «Телебачення Торонто» Анатолій Остапенко: «Треба ускладнити росіянам пошук інформації про нас». *ОПОРА - Громадянська мережа - вибори в Україні - Election in Ukraine*. URL: https://www.oporaua.org/vybory/osint-rozsliduvach-telebachennya-toronto-anatoliy-ostapenko-treba-uskladniti-rosiyanam-poshuk-informaciyi-pro-nas-25667 (дата звернення: 09.04.2025).

Желеховська Тетяна,
здобувач вищої освіти
(Львівський національний університет
імені Івана Франка)

ПРАВОВІ МЕХАНІЗМИ ПРОТИДІЇ КІБЕРЗАГРОЗАМ НА ОСНОВІ OSINT-АНАЛІТИКИ В УКРАЇНІ ТА ЗАРУБІЖНИХ КРАЇНАХ

У сучасному інформаційному суспільстві кіберзагрози набувають дедалі більшої складності та масштабності, становлячи реальну небезпеку для національної безпеки, економіки, критичної інфраструктури та приватного сектору. Традиційні механізми протидії кіберзлочинності вже не завжди здатні оперативно реагувати на новітні виклики цифрового середовища. У цьому контексті особливої актуальності набуває використання OSINT-аналітики для виявлення, моніторингу та попередження кіберзагроз.

OSINT (Open Source Intelligence) – це процес збору, аналізу і використання інформації, яка відкрито доступна. Ця інформація може бути отримана з різних джерел, таких як вебсайти, соціальні мережі, публічні бази даних, новинні ресурси, блоги тощо. Цей підхід застосовується в різних сферах, включаючи правоохоронну діяльність, розвідку, бізнес-аналітику, кібербезпеку та ін [1, с. 221]. У поєднанні з аналітичними інструментами, такими як штучний інтелект або машинне навчання, OSINT значно підвищує ефективність систем кіберзахисту. Особливо перспективним є використання OSINT у сфері критичної інфраструктури, фінансових установ, виборчих процесів та державного управління.

Історію OSINT можна простежити до середини 20-го століття, коли розвідувальні служби почали використовувати загальнодоступну інформацію на додаток до своїх традиційних джерел даних. У 1990-х роках Інтернет і широка доступність цифрової інформації значно розширили сферу застосування та потенціал OSINT. З розвитком соціальних мереж та інших онлайн-платформ OSINT стає все більш важливим інструментом для широкого кола організацій, у тому числі в області фінансової безпеки [2, с. 224].

Хоча OSINT базується на публічній інформації, його використання пов’язане з низкою юридичних ризиків. Зокрема, існує ймо-

вірність порушення права на приватність та захист персональних даних. Крім того, відкриті джерела можуть містити недостовірну або сфальсифіковану інформацію, що впливає на якість аналітики. Важливою проблемою є також відсутність чіткого правового регламенту для державних органів і приватних структур.

На сьогодні в українському законодавстві відсутнє окреме нормативне визначення або законодавча рамка, яка б комплексно регулювала використання OSINT-аналітики. Проте окремі положення, що мають дотичне відношення до збору й обробки відкритої інформації.

Зокрема, Закон України «Про інформацію» встановлює правові засади доступу до публічної інформації, її класифікацію, гарантії свободи інформації, а також передбачає обмеження щодо конфіденційної інформації [3].

В свою чергу Закон України «Про захист персональних даних» регламентує порядок обробки персональних даних, включаючи ті, що отримані з відкритих джерел, і встановлює правила збереження приватності громадян. Це має безпосередній вплив на правомірність використання OSINT, особливо якщо йдеться про ідентифікацію особи [4].

Водночас Кримінальний процесуальний кодекс України та законодавство про оперативно-розшукову діяльність не надають чіткого регламенту щодо допустимості результатів OSINT-розвідки як доказів у кримінальному процесі.

Правове поле використання OSINT в Україні є фрагментарним та потребує доповнення, особливо в контексті стрімкого розвитку технологій OSINT-аналітики у сфері кіберзахисту.

На міжнародному рівні спостерігається більш систематизований підхід до правового врегулювання OSINT. Наприклад, в Європейському Союзі ключовим документом є Загальний регламент про захист даних (GDPR), який регулює обробку персональних даних, навіть якщо вони були зібрані з відкритих джерел [5].

У країнах-членах ЄС збирання відкритих даних для OSINT-досліджень можливе лише за умови дотримання принципів пропорційності, мінімізації даних та інформованості суб’єкта даних. У Німеччині використання OSINT допускається в рамках строго визначених правових процедур, особливо для діяльності поліції та

спецслужб. Порушення законів про захист даних тягне за собою кримінальну відповідальність.

У США важливу роль відіграє Закон про свободу інформації (FOIA), який гарантує доступ до даних державних органів. OSINT широко застосовується у роботі спецслужб (наприклад, CIA або DHS), однак діє низка внутрішніх актів окремих штатів, які регламентують використання відкритої інформації в межах дотримання громадянських прав.

У Великій Британії використання OSINT регулюється Законом «Про захист даних» (Data Protection Act 2018), гармонізованим із GDPR. Водночас у національній стратегії кібербезпеки Великої Британії OSINT визнається ключовим інструментом у сфері запобігання загрозам та цифрової розвідки [6].

Отже, правове регулювання OSINT у світі демонструє тенденцію до системного врегулювання та інтеграції в національні стратегії кібербезпеки, тоді як в Україні ця сфера перебуває на етапі становлення і потребує чіткого правового оформлення з урахуванням міжнародних стандартів і практик.

---

1. Деревягін О.О. Використання OSINT інструментарію при розслідуванні кримінальних правопорушень проти власності. СБУ в умовах війни в Україні: сучасні реалії та інноваційні стратегії забезпечення національної безпеки: матеріали Міжнар. наук. -практ. конф. м. Київ, 4-5 лип. 2024 р. Київ : Алерта, 2024. С. 221–225.
2. Гриненко Ю.І. Використання OSINT-інструментів в аудиті : матеріали IX Міжнар. наук.-практ. конф., м. Київ, 8 груд. 2023 р. Київ, 2023. С. 224–226.
3. Про інформацію : Закон України від 02.10.1992 № 2657-XII // База даних «Законодавство України»/ ВР України. URL: https://zakon. rada.gov. ua/laws/show/2657-12#Text.
4. Про захист персональних даних : Закон України від 01 червня 2010 року № 2297 // База даних «Законодавство України»/ ВР України. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.
5. Регламент Європейського парламенту і Ради (ЄС) 2016/67 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних): Регламент, Міжнародний документ від 27 квітня 2016 року № 2016/679. *База даних «Законодавство України»*/ Офіційний вісник Європейського Союзу. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

Data Protection Act 2018 : United Kingdom Public General Act 2018 c. 12. London : The Stationery Office, 2018. – 339 p.

Захарчук Роман,
аспірант
(Київський університет права
НАН України «Міжнародне право»)

ЗВУКОВИЙ ТЕРОР ЯК МЕТОД КАТУВАННЯ: РОЛЬ OSINT-ДОСЛІДЖЕНЬ У ВИЯВЛЕННІ ВОЄННИХ ЗЛОЧИНІВ ТА ЗАБЕЗПЕЧЕННІ МІЖНАРОДНОЇ ВІДПОВІДАЛЬНОСТІ

Звуковий (акустичний) терор – новий вид психологічного насильства, який застосовується агресорами з метою деморалізації цивільного населення. Згідно з Конвенцією проти катувань, будь-яке навмисне заподіяння тяжких фізичних чи психічних страждань суворо заборонено «при будь-яких обставинах».

У рамках міжнародного права навмисне створення руйнівних звукових хвиль можна розглядати як тортури або нелюдське поводження, заборонені Римським статутом Міжнародного кримінального суду та Женевськими конвенціями. Дослідники ІЦ «Майдан Моніторинг» вводять поняття «акустичний терор» як цілеспрямоване створення звукових хвиль, що діють довільно й проти волі людини, викликають широкий спектр шкідливих наслідків і впливають на стан колективної свідомості. Вони наголошують, що «акустичний терор є складовою терористичної тактики», яку РФ застосовує у війні проти України.

В умовах сучасної війни РФ проти України звукові атаки стають елементом бойових дій. Постійні артилерійські обстріли та ракетні удари по житлових кварталах Харкова й інших міст створюють інтенсивні «звуки війни», що травмують населення ударними та акустичними хвилями. За спостереженнями, головна мета таких атак – «зламати колективну волю» та навіяти страх цивільному населенню.

Такі дії очевидно супроводжуються наслідками, подібними до тортур: люди скаржаться на зниження слуху, сильну тривожність, хронічні порушення сну і психічний стрес. Наприклад, за даними харківського дослідження, РФ «систематично бомбардувала Харків, вдень і вночі… породжуючи інтенсивні «звуки війни», які травмують людей ударними і звуковими хвилями». Таким чи-

ном акустичний терор постає реальною зброєю психологічного тиску під час обстрілів.

У контексті повномасштабної війни РФ проти України звуковий терор є надзвичайно актуальною темою. За оцінками місцевої влади, у Харкові на момент досліджень залишалося від півмільйона до семисот тисяч цивільних, і практично всі вони змушені постійно чути звуки вибухів та сирен.

Хронічне перебування під такими звуковими атаками призводить до стійкого підвищення тривожності і фрустрації населення. Як зауважує професор І. Рущенко, «ці кожний звук наносить травму людині… Це мікротравми: вони накопичуються, складаються, інтегруються, а їхні наслідки є негативними».

Крім фізичної шкоди, звуковий терор серйозно впливає на психологічну стійкість громадян та їхню готовність чинити спротив. У таких умовах ефективне документування випадків акустичного терору стає критичним для привернення уваги міжнародної спільноти та правосуддя.

Звуковий терор розглядається як форма жорстокого поводження з населенням. Його ознаки відповідають елементам злочинів проти людяності (катування) та воєнних злочинів (тяжкі порушення законів війни): це навмисне застосування надмірного звуку для заподіяння страждань, залякування цивільних і руйнування їхнього психологічного стану.

Конвенція проти катувань забороняє будь-яке навмисне заподіяння болю або страждань у будь-яких обставинах, а Римський статут (ст. 7, 8) та Женевські конвенції передбачають кримінальну відповідальність за тортури й нелюдське поводження під час збройних конфліктів.

Документовані факти звукового терору в Україні. Уже з перших місяців війни зафіксовано системні звукові напади на мирних жителів. Так, у звіті від 5 березня 2022 р. повідомлялося, що російська артилерія обстрілює спальні райони Харкова, прагнучи «зламати колективну волю» та залякати місто, використовуючи тактику акустичного терору, при якій вибухи чутні всюди й створюють враження обложеного міста.

Постійні російські бомбардування не обмежуються поодинокими ударами: наприклад, з березня 2022 по лютий 2023 ракетні удари по Харкову тривали з різною інтенсивністю, охоплюючи все місто і повторно травмуючи його жителів.

Багато людей були змушені покинути прифронтові міста через невпинні гучні вибухи.

Проведені дослідження вказують на прямий зв'язок між такими звуковими атаками і здоров'ям: наприклад, зафіксовано різке та хронічне зниження слуху, підвищення рівня тривожності, безсоння та інші невротичні стани у мешканців, що зазнали багаточасового впливу «звуків війни».

Відкриті джерела стають ключовим інструментом збору доказів акустичного терору. За словами експертів, OSINT передбачає «збір та аналіз відкритої доступної інформації: соціальних мереж, новин, супутникових знімків тощо», що дає змогу дослідникам відновлювати обставини, місце та час порушень.

Завдяки OSINT було зібрано численні відео й фото вибухів у житлових районах, а також свідчення очевидців. Інформаційний центр «Майдан Моніторинг» у межах документування воєнних злочинів зазначає, що один із ключових напрямів їхньої роботи – це «пошук, обробка та аналіз інформації, яка розміщена у відкритих джерелах», що тривало понад пів року.

Так, фотознімки руйнувань та оцінок пошкоджень історичних будівель були використані слідчими для підтвердження фактів воєнних злочинів РФ (зокрема, у виставковому проекті FRACTURE фіксується задокументована робота щодо Харкова). На основі зібраних даних фахівці пропонують створити карту акустичних подій міста (лог звуку вибухів), що стане новим інструментом супроводу порятункових операцій і подальшого аналізу: «пропонується створити звукову карту міста під час бойових дій, яку можна використовувати рятувальникам та слідчим».

Потенціал даних для міжнародної відповідальності. Зібрані у відкритих джерелах докази здатні лягти в основу розслідувань воєнних злочинів на міжнародному рівні. Наприклад, у юриспруденції Міжнародного кримінального суду вже враховується значення цифрових доказів війни в Україні: платформи соцмереж переповнені відео, фото та аудіозаписами обстрілів, що створюють «основу для цифрових доказів», на яку має спиратися Офіс прокурора.

Багато типів воєнних злочинів (цілеспрямовані удари по цивільних об'єктах, атаки на лікарні і школи, застосування забороненої зброї, тортури тощо) вже були задокументовані саме через OSINT-аналіз.

Таким чином, дані OSINT не лише підтверджують факти звукового терору, а й ідентифікують винуватців. Українські правозахисники зазначають: «розвідка за відкритими джерелами відіграє важливу роль у документуванні та розслідуванні воєнних злочинів», адже вона «допомагає встановити осіб, винних у воєнних злочинах». Саме тому матеріали з відкритих джерел можуть бути долучені до доказової бази у міжнародних процесах (наприклад, у справах МКС чи ad hoc трибуналів).

Акустичний терор у повномасштабній війні РФ проти України слід розглядати як новітню форму тортур та воєнних злочинів, оскільки він свідомо спрямований на доведення цивільного населення до страху і безсилля. Рамки міжнародного права (Конвенція проти катувань, Римський статут, Женевські конвенції) дозволяють кваліфікувати такі дії як злочини проти людяності та воєнні злочини. Ефективне розслідування цих злочинів неможливе без OSINT: відкриті джерела дають змогу документувати звукові атаки, створювати нові види доказів (наприклад, акустичні карти обстрілів) і відстежувати винних. Як зазначено експертами, завдяки OSINT «ми можемо продовжувати проливати світло на воєнні злочини, приносити справедливість жертвам та наближати заслужене покарання винних».

На основі зібраних даних громадські організації та правоохоронці можуть ініціювати міжнародні справи проти винних у застосуванні звукового терору.

---

1. Акустичний терор в контексті російсько-української війни: соціологічний вимір URL: https://maidan.org.ua/2024/04/akustychnyy-teror-v-kontekstirosiysko-ukrainskoi-viyny-sotsiolohichnyy-vymir/ (дата звернення: 08.03.2025).
2. Бандура А. Агресія: соціальне навчання і контроль над поведінкою / А. Бандура. – К. : Основи, 2000. – 376 с.
3. Висоцький О. Тероризм як соціальне явище : монографія / О. Висоцький. – Харків : Право, 2020. – 312 с.
4. Дідковська Л. Вплив звуку на психіку людини / Л. Дідковська // Психологія і сучасність. – 2019. – № 2. – С. 45–50.
5. Жижек С. Насильство: шість поглядів із боку / С. Жижек ; пер. з англ. – К. : Ніка-Центр, 2018. – 224 с.
6. Ковальчук І. Акустичні методи впливу у воєнних конфліктах / І. Ковальчук // Воєнна думка. – 2021. – № 4. – С. 23–31.
7. Мартинюк Р. Інформаційно-психологічна війна: технології впливу / Р. Мартинюк. – Львів : Світ, 2022. – 198 с.

8. Морган М. Сучасний тероризм / М. Морган ; пер. з англ. – К. : Критика, 2015. – 272 с.
9. Станішевський В. Психологічні аспекти акустичного впливу / В. Станішевський // Соціальна психологія. – 2020. – № 1. – С. 64–71.
10. Шевченко Л. Акустична зброя: міфи і реальність / Л. Шевченко // Безпека держави. – 2023. – № 3. – С. 14–19.

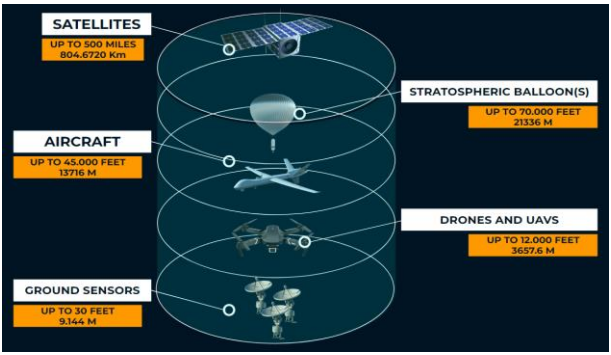
Земляков Роман,
старший викладач кафедри організації захисту інформації з обмеженим доступом (Національна академія Служби безпеки України)

СТРУКТУРА ГЕОПРОСТОРОВОЇ РОЗВІДКИ (GEOSPATIAL INTELLIGENCE) ПРИ ЗАСТОСУВАННІ КОМПЛЕКСНИХ СУПУТНИКОВИХ СИСТЕМ

Збір геопросторових даних, оперативне створення інтерактивних карт земної поверхні, та аналіз інформації про розташування об'єктів в досліджуваному секторі потребує розробки механізмів взаємодії між апаратною структурою, засобами зберігання, та обробки зображень, а також, аналітичних інструментів різного цільового призначення. Сфера геопросторової розвідки (Geospatial intelligence (далі – GEOINT)), призначена для оборонної аналітики, дослідження оптичних зображень різної роздільної здатності, та створення деталізованої характеристики об'єкта спостереження на земній поверхні на основі його периферійних, та фонових характеристик. Відповідні дані можуть надходити з різних джерел, що включають комплексні супутникові системи, аерозйомку та центри обробки інформації [1, с. 15-24].

На основі відповідних вимог виникає необхідність розробки єдиного механізму збору, аналізу, та інтерпретації даних (так званий DATA COLLECTION ANALYSIS INTERPRETATION PROCESSES), що можна розподілити на етапи отримання, обробки, деталізації інформації за допомогою комплексних супутникових систем оптичної фото розвідки, аеророзвідки та подальшого аналізу отриманої інформації на основі інструментів аналізу зображень та моніторингу даних земної поверхні [1, с. 15-57].

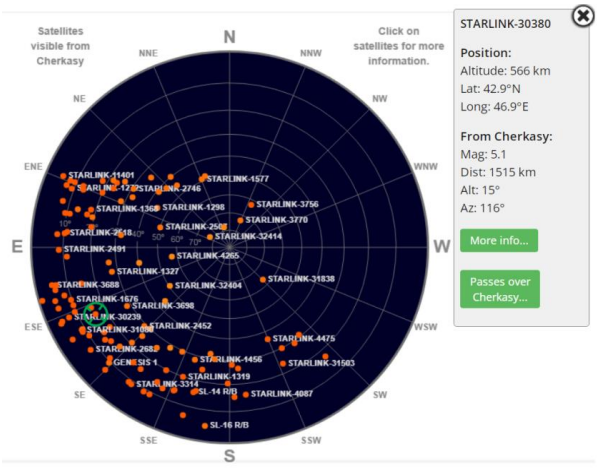
Проведення процедур геопросторової розвідки потребує застосування сукупності апаратів, що мають різне цільове призначення – платформ дистанційного зондування (REMOTE SENSING PLATFORMS), що надають величезні обсяги даних ширшій групі систем та інструментів, які виконують чітко визначені функції із дослідження даних і пошуку периферійних характеристик об'єкта спостереження [1, с. 15-57, 2].



Первинний аналіз зображення в результаті отримання даних оптичної розвідки різного апаратного складу повинен базуватись на дослідженні бібліотек даних супутникової та аеророзвідки, в тому числі за допомогою інструментів з відкритим кодом (Soar, EOS Land Viewer та аналоги). Головним завданням даного етапу є визначення та характеристика фонових елементів зображення, в тому числі об'єктів першої категорії (природного походження): рельєф місцевості, масивні об'єкти природного походження (прибережна лінія, річки, озера та інше); об'єктів другої категорії (техногенного походження – статичні об'єкти) – незмінювані рукотворні об'єкти, головним призначенням пошуку яких є фонова орієнтація на карті оптичного зображення (зазвичай на основі рукотворних статичних об'єктів створюється сітка моніторингу за переміщенням основного об'єкта аналізу); об'єктів третьої категорії (техногенного походження – динамічні об'єкти) – змінювані або об'єкти що були чи знаходяться в процесі переміщення (зазвичай до даної групи і відносять основний об'єкт спостереження на основі геопросторової розвідки) [1, с. 15-57, 3].

Для отримання деталізованої інформації, що буде максимально наближеною до реального часу (визначеного часу отримання розвідувальної інформації) є необхідним розроблення сітки супутникових та інших апаратів (в ході проведення аналізу моделюється використання оптичних зображень із супутникових орбітальних систем), які мають встановлені необхідні орбіти і циркулюють над визначеним периметром місцевості моніторингу. Для проведення даної операції та створення сітки циркулювання супутників над

необхідною місцевістю є доцільним використання інструментів відстеження космічних об'єктів на навколоземних орбітах (Stuff in Space та аналоги) [1, с. 15-57, 4].



Другим етапом аналізу даних оптичної розвідки є визначення візуальних особливостей об'єкта спостереження, відповідно до географічного розташування, часу створення зображення, кута нахилу земної поверхні по відношенню до Сонця або Місяця та рельєфу місцевості. В якості основних інструментів визначення параметрів сонячного та місячного світла при взаємодії з об'єктом спостереження у досліджуваній місцевості та часі доцільним є застосування ресурсів

Suncalc та Mooncalc, що призначені для надання точної інформації про точку спостереження, включаючи, час сходу та заходу сонця та кут нахилу тіні у визначений час [1, с. 85-120, 5].

Окремою складовою процедури дослідження даних оптичної розвідки є створення системи периферійних географічних особливостей, що включають видове зображення рельєфу (на основі чого складається об'ємна карта рельєфу зональної місцевості), пошук та дослідження медіа контенту із відкритих джерел інформації, що географічно пов'язані із об'єктом спостереження та схеми логістичних маршрутів, що можуть бути використані, або використовуються динамічним об'єктом спостереження для переміщення. При цьому створюється модель опису досліджуваного сектору земної поверхні, на основі якої будується аналітика щодо об'єкта спостереження в результаті геопросторової розвідки [1, с. 85-120, 6, 7].

Варто зробити висновок, що процедури геопросторової розвідки як єдиний механізм потребує розподілу на кілька етапів дослідження об'єкта спостереження, що характеризуються застосуванням спеціального інструментарію, який націлений на комплексний опис місцевості, виявлення характерних точок рельєфу та периферійних особливостей рукотворного походження. При цьому важливим залишається моніторинг та актуалізація апаратного забезпечення (супутників), що циркулює на геостаціонарних та інших навколоземних орбітах над досліджуваною місцевістю, від чого в першу чергу буде залежати якість отриманих оптичних зображень та оперативність формування актуалізованих даних геопросторової розвідки.

---

1. Robert M. Clark. Geospatial Intelligence: Origins and Evolution. Georgetown University Press: 2020. 320 c.
2. NASA Earth Science GIS Data Tools. URL: https://www. earthdata. nasa.gov/learn/gis/data-tools (дата звернення: 28.04.2025);
3. EOS Land Viewer. URL: https://eos.com/landviewer/?lat= 50.1155 &lng=8.6842&z=11 (дата звернення: 03.04.2025);
4. In-The-Sky. URL: https://in-the-sky.org/satmap_worldmap.php (дата звернення: 03.04.2025);
5. In-The-Sky. URL: https://www.suncalc.org/#/49.428,32.0466,3/ 2025.05.03 /23:19/ 1/3 (дата звернення: 03.04.2025);
6. Mooncalc. URL: https://www.mooncalc.org/#/49.43,32.0493,3/2025.05.03/ 23:20/1/3 (дата звернення: 03.04.2025);
7. Britannica: Radio telescope. URL: https://www.britannica. com/science/ radio-telescope (дата звернення: 29.04.2023).

Зоренко Дмитро,
доцент спеціальної кафедри № 2
Інституту Служби безпеки України
(Національний юридичний університет
імені Ярослава Мудрого)

ВИКОРИСТАННЯ GITHUB-ІНСТРУМЕНТІВ У РАМКАХ OSINT-ДОСЛІДЖЕНЬ

Як відомо, GitHub – один з найбільших вебсервісів для спільної розробки програмного забезпечення [1] та ключових платформ для доступу до різноманітних OSINT-інструментів, які автоматизують збір, аналіз і візуалізацію даних, отриманих з відкритих джерел.

GitHub-утиліти відрізняються гнучкістю: більшість з них написано на мові програмування Python, що дозволяє легко адаптувати їх під конкретні дослідницькі задачі. Відкритий код забезпечує прозорість алгоритмів, активна онлайн-спільнота швидко виправляє виявлені вразливості, додає нові функції. Деякі проєкти, як Emora, навіть пропонують графічну оболонку для користувачів, які не володіють інтерфейсом командного рядку (англ. Command line interface, CLI). Для комплексних розслідувань інструменти можна комбінувати через прикладний програмний інтерфейс (англ. Application Programming Interface, API) для роботи зі сторонніми платформами (наприклад, Maltego) або скрипти, створюючи їх персоналізовані послідовності для скорочення часу досліджень.

Здійснений аналіз дозволяє стверджувати, що GitHub-інструменти для OSINT мають низку унікальних функцій, що суттєво розширюють можливості розвідки з відкритих джерел:

- збір інформації – Skiptracer призначений для пошуку інформації про особу або організацію в Dark Web, White Pages, Craig-?list, витоках даних; Subfinder виявляє приховані піддомени через пасивні джерела, що корисно для аналізу інфраструктури об’єкту; theHarvester агрегує дані з поштових серверів, соцмереж і DNS-записів, спрощуючи початкову розвідку; Photon автоматизує краулінг вебсторінок, агрегуючи посилання, метадані та контакти; Holehe перевіряє, чи зареєстровано email на понад 100 популярних вебсайтах, дозволяючи встановити цифровий слід облікових запи-

сів; у «темній мережі» Prying Deep сканує .onion-сайти, а OnionScan аналізує їхню безпеку;

- аналіз соціальних мереж – Sherlock знаходить акаунти за username у 100+ соцмережах, включаючи маловідомі платформи; Social Analyzer аналізує профілі з виведенням результатів щодо активності користувачів, розміщеною ними інформації чи контенту; Twint збирає дані з X/Twitter без API, дозволяючи аналізувати твіти, хештеги та мережі зв'язків; GHunt досліджує активність користувачів на GitHub через історію комітів (керування версіями продукту) та ключові слова;

- автоматизація, візуалізація та інтеграція даних – SpiderFoot об'єднує 200+ модулів для моніторингу загроз, аналізу потенційних атак і візуалізації зв'язків між об'єктами; Amass будує карту мережі цілі, комбінуючи дані з сертифікатів SSL, архівів WHOIS і сканерів портів; MetaDetective аналізує метадані файлів, виявляючи приховану інформацію;

- спеціалізовані пошукові інструменти – PhoneInfoga перевіряє номери телефонів через соцмережі та бази даних; ClatScope досліджує геолокацію, паролі й витоки даних, телефони, електронні пошти та інше (понад 70 типів даних); OsintStalker збирає інформацію з Facebook, включаючи геотеги; для електронної пошти Zehef відстежує історію використання, а EmailEnricher ідентифікує ймовірного власника; інструменти типу Shodan аналізують мільйони пристроїв, що недоступне при ручній роботі; gitGraber сканує публічні репозиторії GitHub на предмет API-ключів, токенів, паролів, конфіг-файлів, інших витоків.

Отже, більшість OSINT-інструментів на GitHub орієнтовані на збір відкритої інформації, але деякі надають доступ до унікальних або складно агрегованих даних (наприклад, трекінг літаків чи кораблів). Вказані утиліти постійно вдосконалюються, з'являються нові рішення, що розширюють можливості дослідників. Тому вивчення та регулярне оновлення знань про такі OSINT-інструментів є важливою складовою роботи фахівця в сфері розвідки з відкритих джерел.

Хоча GitHub-утиліти для OSINT пропонують значні переваги, але вони мають і певні обмеження – можуть містити шкідливий код або збирати дані щодо користувачів; приблизно половина проєктів мають обмежену підтримку, проблеми з налаштуванням, неповний або взагалі відсутній опис, що ускладнює їхнє використан-

ня. Деякі інструменти (наприклад, для деанонімізації осіб) призначені для вирішення пошукових завдань, що подекуди суперечать етичним нормам чи порушують закони про конфіденційність персональних даних певних країн. Безкоштовні версії продуктів з відкритим вихідним кодом часто поступаються платним аналогам у швидкості та глибині аналізу, дають помилкові спрацьовування через обмежені алгоритми перевірки. Дається в знаки й залежність від зовнішніх прикладних програмних інтерфейсів – зміни в API соцмереж або пошукових систем роблять подібні інструменти непрацездатними.

Отже, GitHub-утиліти є потужним ресурсом для OSINT, особливо в контексті автоматизації пошуку, доступу до маловідомих джерел, а також бюджетності. Однак їх використання вимагає обережності: перевірки коду на безпеку, дотримання правових норм та критичної оцінки отриманих відомостей. Для професійних розслідувань кращою практикою стає поєднання можливостей подібних ресурсів з платними платформами, що дозволяє забезпечити прийнятну достовірність результатів та належне опрацювання даних.

Перспективи розвитку використання GitHub-утиліт в OSINT у найближчому майбутньому виглядають достатньо обнадійливими та багатогранними. По-перше, зростатиме популярність і доступність інструментів, що не потребують глибоких технічних навичок, як-от Google Dorking та Social Media Intelligence Tools, що спрощує залучення новачків у сферу OSINT. По-друге, посилення інтеграції GitHub-інструментів з іншими платформами та сервісами через API, що дозволить створювати кастомізовані рішення для комплексних розслідувань із мінімальним втручанням користувача. По-третє, зростання ролі штучного інтелекту й машинного навчання для потреб систематизації та узагальнення зібраних відомостей, що значно підвищить точність і швидкість обробки великого масиву даних, а також формулювання висновків на цій основі.

Таким чином, GitHub-утиліти в OSINT будуть ставати більш потужними, інтегрованими, зручними і безпечними, що відкриватиме широкі перспективи для їхнього застосування, в тому числі, і для вирішення прикладних завдань в сфері забезпечення державної безпеки.

---

1. GitHub: матеріал з Вікіпедії. URL: https://uk.wikipedia.org/wiki/GitHub (дата звернення: 01.05.2025).

Іванова Роксолана,
кандидат юридичних наук, доцент,
професор кафедри міжнародного та європейського права
(Хмельницький університет управління та права
імені Леоніда Юзькова)

ВИКОРИСТАННЯ OSINT У МОНІТОРИНГУ ДІЯЛЬНОСТІ МІЖНАРОДНИХ ФІНАНСОВИХ ОРГАНІЗАЦІЙ ЯК ІНСТРУМЕНТ ЗМІЦНЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

У разі гібридної війни, економічної нестабільності та фінансового тиску на національну економіку відстеження міжнародних валютних операцій та установ стає життєво важливим елементом національної безпеки. OSINT став безцінним ресурсом для аналітиків і практикуючих юристів, які прагнуть відстежувати, аналізувати та оцінювати фінансові ризики, пов'язані з транснаціональною злочинною діяльністю, корупцією чи ухиленням від санкцій.

Відомо, що Міжнародний валютний фонд, Світовий банк, Національний фонд боротьби з розповсюдженням тероризму та Європейський банк реконструкції та розвитку створюють і поширюють великі обсяги відкритих даних, звітів, перевірок відповідності, оцінок ризиків, аудитів проектів тощо. Ці документи містять відповідну інформацію, яку можна збирати, обробляти та аналізувати за допомогою методів OSINT для обслуговування державних і юридичних осіб.

З юридичної точки зору та точки зору безпеки, цінність OSINT у цій сфері полягає в тому, що вона допомагає:

Відстежувати фінансову діяльність і ступінь відкритості держав і організацій;

Виявлення невідповідностей та потенційних корупційних ризиків або зловживання міжнародною допомогою;

виявлення зв'язків між суб'єктами санкцій та кредитними організаціями, які їх фінансують;

Попередня ознака очевидної нової економічної небезпеки або нестабільності;

Супровід дізнань за підозрою у фінансуванні організованої злочинності чи тероризму.

Прозорість і підзвітність для України, яка перебуває під значною міжнародною фінансовою допомогою, є надзвичайно важливими через стан її післявоєнної відбудови. Інструменти OSINT можуть допомогти відстежити, чи цілеспрямовано витрачаються міжнародні кошти, особливо в таких критичних сферах, як оборона, інфраструктура та енергетика. Аналіз доступних даних про закупівлі з оцінок FATF і джерел фінансових новин може висвітлити певний рівень неефективності або зловживання.

Автоматизовані системи OSINT, які використовують машинне навчання та штучний інтелект для аналізу наборів даних, є одним із помітних кроків вперед для цих інструментів. Ці системи можуть стежити за міжнародним рухом коштів, перевіряти бази даних державних закупівель і тендерів, відстежувати офшори та підставні компанії та виявляти приховані зв'язки між політично відомими особами (PEP).

Крім того, співпраця громадських груп та інших організацій громадянського суспільства з правоохоронними органами на основі даних OSINT надає більшої сили боротьбі з економічними злочинами. Інші території, які працювали разом з Україною в цій сфері, вже досягли успіху, коли мова йде про повернення активів і застосування санкцій.

Відділення фінансового аналізу, засновані на OSINT, у багатьох штатах не мають законодавчої бази. Таким чином, необхідно:

Сприяти комплексній національній політиці щодо застосування OSINT для економічної розвідки;

Навчати аналітиків і юристів наборам навичок OSINT з державного сектору;

Створення правової політики щодо використання та включення OSINT-інформації в судові процедури;

Проекти міжнародних угод, які регулюють двосторонній та багатосторонній обмін даними OSINT про фінансові злочини.

Як зазначалося, використання OSINT для відстеження та моніторингу міжнародних фінансових установ та їх діяльності виходить за рамки простого технічного підходу, а радше є стратегічним імперативом. Коли OSINT використовується в рамках закону, OSINT пропонує чудові важелі для захисту національних інтересів, підзвітності та перешкоджання збитковим фінансовим операціям, спрямованим на Україну.

1. Financial Action Task Force. *FATF Guidance on Digital Transformation of AML/CFT.* Paris: FATF, 2021.

2. World Bank. *Open Data Catalog.* URL: https://data.worldbank.org

3. IMF. *Annual Report 2023: Promoting Economic Stability and Growth.* Washington, D.C.: IMF, 2023.

4. OSINT Foundation. *Guide to Open Source Intelligence in the Public Sector.* London: OSINT Foundation, 2022.

5. Transparency International. *Financial Secrecy Index 2022.* Berlin: TI Secretariat, 2022.

6. UNODC. *Combating Money Laundering and the Financing of Terrorism: A Comprehensive Training Guide.* New York: United Nations, 2020.

7. FATF. *Ukraine Mutual Evaluation Report.* Paris: FATF, 2022.

Ігнатьєв Борис,
доцент кафедри управління
та інформаційно-аналітичного забезпечення
оперативно-розшукової діяльності
(Національна академія Служби безпеки України)

РЕКЛАМНІ ІДЕНТИФІКАТОРИ ПРИСТРОЇВ ЯК РИЗИК ДЛЯ ОПЕРАЦІЙНОЇ БЕЗПЕКИ ОСІНТ-ДІЯЛЬНОСТІ СУБ'ЄКТІВ РОЗВІДУВАЛЬНОГО СПІВТОВАРИСТВА УКРАЇНИ

В сучасних умовах мобільні пристрої виконують не лише комунікаційні функції, але й перетворюються на багатофункціональні інструменти, здатні збирати та передавати персональні і поведінкові дані про їхніх власників. Одним із менш очевидних, але надзвичайно важливих аспектів стратегії збору таких даних є система рекламних ідентифікаторів – так звані Mobile Advertiser IDs (MAIDs), серед яких найбільш поширеними є Apple IDFA (Identifier for Advertisers) та Google Advertising ID. Система MAIDs була розроблена як інструмент для підвищення конфіденційності користувачів, замінюючи постійні ідентифікатори пристроїв на унікальні, змінні та керовані користувачем ідентифікатори. Такий механізм мав сприяти ефективному таргетуванню реклами, забезпечивши при цьому певний рівень приватності користувача. Однак на практиці він став підґрунтям для побудови детальних профілів поведінки користувачів та, побічно, став елементом стеження за ними.

Основною метою MAIDs є забезпечення транслювання персоналізованої рекламної інформації без залучення даних, що дозволяють ідентифікувати особу користувача, а також надання йому реальних механізмів контролю за використанням технологій трекінгу, з правом на обмеження або відмови від збору даних про його активність. Однак низка досліджень вказують на систематичне зловживання цими механізмами: мобільні додатки з'єднують MAIDs із постійними ідентифікаторами пристроїв, такими як IMEI, Android ID, MAC-адреси, що порушує принципи анонімності та дозволяє відстежувати користувача незалежно від його дій. Такі порушення фіксуються в значних обсягах – за даними

дослідницької групи AppCensus [1], лише на платформі Android понад 18 000 додатків порушують політику конфіденційності Google, передаючи MAIDs разом з іншими унікальними ідентифікаторами пристрою.

Одним із ключових механізмів, що сприяє передачі цих даних, є система Real-Time Bidding (RTB) – аукціон в реальному часі, у межах якого рекламодавці змагаються за можливість показати рекламу конкретному користувачу. Кожен запит у межах RTB передає великий обсяг даних про користувача, зокрема його геолокацію, MAIDs, модель пристрою, інформацію про мобільного оператора та інші відомості. Навіть якщо користувач вимкнув точне визначення місцезнаходження, система може використовувати IP-адресу або попередньо зібрані координати для визначення його ймовірного місця перебування. Як результат, ці дані стають доступними численним стороннім організаціям, зокрема і брокерам даних, які зберігають їх у своїх сховищах даних для подальшої монетизації або передають урядовим та комерційним замовникам [2].

Досить ілюстративним у зазначеному контексті є досвід фахівця з кібербезпеки, описаний у авторському блозі в статті «Tracking myself down through in-app ads» [3]. Автор, навіть не маючи активованих сервісів локації, зафіксував передачу даних про своє місцезнаходження рекламній мережі Unity Ads через гру Stack. Попри відсутність встановлених у операційній системі застосунків, що розповсюджуються компанією Meta, його пристрій регулярно передавав дані на сервери Facebook через сторонні SDK (Software Development Kit). Встановлено, що мобільна реклама може передавати настільки точні дані, що їх аналіз дозволяє визначити не лише будівлю, а й поверх, на якому перебуває користувач. Дослідник, використовуючи доступні інструменти, також з'ясував, що для точного відстеження людини через RTB достатньо витрат у межах кількох доларів. Зазначене робить цю технологію потенційно небезпечною для використання спецслужбами противника, окремими організаціями, групами і особами як інструмент спостереження.

Зважаючи на обсяги та чутливість інформації, що збирається й передається з використанням MAIDs, а також активну фазу збройної агресії рф проти України, оцінюємо витоки таких даних як ймовірний внутрішній програмно-технічний ризик високого рівня

впливу на особисту та операційну безпеку OCIHT-персоналу суб'єктів розвідувального співтовариства України. Адже саме поєднання MAIDs з точною геолокацією дозволяє виявляти місця проживання, маршрути пересування, пункти постійної та тимчасової дислокації співробітників вітчизняних спецслужб. Ворожі структури можуть таргетувати рекламу, яка насправді слугує для спостереження, використовуючи дешеві та загальнодоступні засоби мобільного маркетингу. Із відкритих комерційних пакетів можна купити дані, зібрані з ігор, навігаційних застосунків, соціальних платформ і на їх основі визначити, наприклад, хто відвідує конкретні об'єкти критичної інфраструктури, пункти постійної чи тимчасової дислокації військовослужбовців тощо. Деякі брокери даних, як показують злами і журналістські розслідування, продають таку інформацію без належної перевірки або навіть з порушенням законодавства.

Одним із наочних прикладів журналістського розслідування щодо викриття незаконної або напівлегальної торгівлі геолокаційними даними, пов'язаними з рекламними ідентифікаторами, є **розслідування Vice Motherboard** про компанію **X-Mode Social (пізніше перейменованої на Outlogic)** [4]. У ньому йдеться про те, що X-Mode збирала надзвичайно точні дані про переміщення користувачів через мобільні застосунки (зокрема, Tinder, Grindr, Muslim Pro), а потім продавала ці дані третім сторонам, включно з державними підрядниками, що працювали з урядовими установами США. Розслідування виявило, що передача цих даних здійснювалася без належної згоди користувачів та часто в обхід стандартів прозорості. У 2024 році **Федеральна торговельна комісія США (FTC)** винесла постанову проти **X-Mode/Outlogic** [5], заборонивши компанії продавати точні геолокаційні дані, які можна було використати для ідентифікації осіб, оскільки це порушувало принципи доброчесної обробки персональної інформації.

На рівні користувача (OCIHT-персоналу) повна ізоляція від таких ризиків неможлива без глибоких системних змін. Водночас, мінімізація ризиків є досяжною за рахунок: видалення або регулярного скидання MAIDs через налаштування пристрою; блокування або обмеження фонових доступів до геолокації (особливо для застосунків, які не потребують її функціонально);

відмови від встановлення неперевірених застосунків; використання VPN та надбудов, призначених для блокування трекерів і рекламного контенту [6]; встановлення мобільного моніторингу мережевого трафіку для виявлення небажаних передач даних.

На рівні організації (суб'єктів розвідувального співтовариства України) критично важливо впроваджувати корпоративні політики безпеки на кшталт технологій MDM (Mobile Device Management) для контролю і захисту особистих мобільних пристроїв, а також доступу до спеціалізованих додатків через захищений репозиторій. Технологія MDM дозволяє контролювати не лише самі пристрої, але й встановлені на них застосунки, забезпечуючи таким чином комплексний захист. Цей підхід подібний до практик, що використовуються у військових структурах інших країн, зокрема армії США, де такі технології впроваджені для підвищення кіберзахисту військовослужбовців. Міністерство оборони України активно впроваджує технологію MDM у відповідь на критичні проблеми витоку інформації через особисті пристрої військових, які часто використовуються для фотографування та пересилання документів, включаючи матеріали з обмеженим доступом, фотографії військових позицій та техніки [7]. Також доцільно застосовувати системи моніторингу активності пристроїв і регулярно проводити навчання та інструктажі OCINT-персоналу з розвитку цифрових компетентностей і неухильного дотримання вимог цифрової гігієни. У випадку використання BYOD-підходів (Bring Your Own Device) [8], слід передбачити окрему сегментацію мережі, обмеження на зберігання службових даних на мобільних пристроях та можливість централізованого керування доступом.

Таким чином, рекламні ідентифікатори мобільних пристроїв, які були впроваджені як компроміс між потребами ринку та конфіденційністю, на практиці перетворилися на потужний інструмент стеження, що становить високий ступінь ризику як для особистої безпеки OCINT-персоналу, так і для операційної безпеки у межах OCINT-діяльності суб'єктів розвідувального співтовариства України. Їх широке комерційне використання, технічна складність контролю та надзвичайно низький поріг входу для спецслужб противника, окремих організацій, груп і осіб потребують ухвалення ефективних рішень та вжиття заходів

контролю з метою управління цим ризиком, що загалом сприятиме убезпеченню ОСІНТ-активів (персоналу та інфраструктури) суб'єктів розвідувального співтовариства України.

---

1. Egelman S. Ad IDs Behaving Badly. 2019. 14 лютого. URL: https://web.archive.org/web/20221107190711/https://blog.appcensus.io/2019/02/14/ad-ids-behaving-badly (Дата звернення: 21.04.2025).

2. Federal Trade Commission. FTC Finalizes Order Banning Mobilewalla from Selling Sensitive Location Data. 2025. 14 січня. URL: https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-finalizes-order-banning-mobilewalla-selling-sensitive-location-data (Дата звернення: 21.04.2025).

3. Tim Sh. Everyone knows your location: tracking myself down through in-app ads. 2025. 01 лютого. URL: https://timsh.org/tracking-myself-down-through-in-app-ads (Дата звернення: 21.04.2025).

4. Cox J. Inside the Industry That Unmasks People at Scale. 2021. 14 липня. URL: https://www.vice.com/en/article/industry-unmasks-at-scale-maid-to-pii (Дата звернення: 21.04.2025).

5. Federal Trade Commission. FTC Order Prohibits Data Broker X-Mode Social and Outlogic from Selling Sensitive Location Data. 2024. 09 січня. URL: https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data (Дата звернення: 21.04.2025).

6. Rathika Palanisamy, Azah Anir Norman, Miss Laiha Mat Kiah. BYOD Security Risks and Mitigation Strategies: Insights from IT Security Experts. 2022. 08 лютого. Journal of Organizational Computing and Electronic Commerce. Volume 31, 2021 - Issue 4. Pages 320-342. URL: https://doi.org/10.1080/10919392.2022.2028530 (Дата звернення: 21.04.2025).

7. Ukrainian Military Pages. Міноборони отримає віддалений контроль над особистими смартфонами військових... лише заради їх безпеки. 2024. 2 вересня. URL: https://www.ukrmilitary.com/2024/09/big-bro-with-you.html (Дата звернення: 28.04.2025).

8. Gema Howell (NIST), Joshua Franklin (NIST), Vincent Sritapan (DHS), Murugiah Souppaya (NIST), Karen Scarfone (Scarfone Cybersecurity). NIST SP 800-124 Rev. 2. Guidelines for Managing the Security of Mobile Devices in the Enterprise. Information Technology Laboratory. Computer Security Resource Center. May 2023. URL: https://nvlpubs.nist.gov/nistpubs/ Speci-?lPublications/NIST.SP.800-124r2.pdf (Дата звернення: 21.04.2025).

Калганова Олена,
кандидат юридичних наук, доцент,
завідувач кафедри фінансових розслідувань
та економічної безпеки Навчально-наукового
інституту економічної безпеки та митної справи
(Державний податковий університет)
Свінціцька Юлія,
доктор філософії у галузі права,
старший викладач кафедри фінансових розслідувань
та економічної безпеки Навчально-наукового
інституту економічної безпеки та митної справи
(Державний податковий університет)
Желтухіна Анастасія,
провідний фахівець навчальної лабораторії
фінансових розслідувань Навчально-наукового
інституту економічної безпеки та митної справи
(Державний податковий університет)

ВИКОРИСТАННЯ OSINT-ІНСТРУМЕНТІВ ПІД ЧАС ДОСУДОВОГО РОЗСЛІДУВАННЯ

В умовах стрімкого розвитку інформаційних технологій та цифрової комунікації розвідка з джерел відкритої інформації (далі – OSINT) стала важливим невід'ємним інструментом у практиці виявлення, розслідування та запобігання вчиненню кримінальних правопорушень різних спрямувань. За сучасних обставин, коли значна частина суспільної, комерційної та особистої діяльності відбувається в публічному інформаційному просторі, зокрема в мережі Інтернет, збирання, аналіз та використання відкритих джерел набуває все більшої актуальності для цілей досудового розслідування.

У рамках аналітичної розвідки збирання первинної інформації може бути здійснено наступними способами: комп'ютерна розвідка в мережі Інтернет; комп'ютерна розвідка в автоматизованих банках даних та інформаційних системах різних форм власності; вивчення публікацій в ЗМІ [4, с. 447].

Ефективність цього методу полягає в тому, що громадяни добровільно та за власною ініціативою публікують свої анкетні дані, дату народження, місце проживання, коло спілкування, інтереси, а також особисті фотографії та відео, створюючи таким чи-

ном великий масив цифрових даних. Ці дані містять антропометричні ознаки зовнішності, анкетну інформацію, зображення місць проживання та інше. Завдяки тому, що ця інформація є відкритою, правоохоронні органи можуть безперешкодно використовувати її для оперативних цілей. Аналіз цих даних дає змогу отримувати орієнтовну інформацію, а іноді й одразу ідентифікувати особу [5, с. 145].

Моніторинг у реальному часі оновлень на таких платформах, як Facebook, Twitter та інших соціальних мережах дає змогу правоохоронним органам отримати необхідну інформацію про скоєні або ті, що готуються, злочини. Усі дані, що залишають правопорушники в Інтернеті, є важливими для оперативної роботи. Знання цієї інформації дає можливість правоохоронцям ідентифікувати злочинців та, за можливості, запобігти їхній протиправній діяльності [1, с. 588; 2, с. 111].

Достатньо великий обсяг інформації, яка прямо не стосується вчиненого кримінального правопорушення, але може надати непрямі докази, також можливо отримати із соціальних мереж суб'єкта. Наприклад, публічний акаунт в мережі Instagram розповість про найближче коло спілкування особи, розташування житла, роботи та гео-дані улюблених місць проведення вільного часу. Достатньо популярна на теренах нашої держави мережа Linkedin надасть інформацію про працевлаштування та колег досліджуваного суб'єкта.

Окрім соціальних мереж особливу увагу варто приділити місцевим чатам у месенджерах та Telegram-каналах, де місцеві жителі розміщують відеозаписи та інформацію про правопорушення, фотографії осіб, котрі порушують громадський порядок або вчиняють протиправні діяння. Даний інструмент часто використовується правоохоронцями для моніторингу і відслідковування осіб, які мають яскраво виражену антисоціальну девіантну спрямованість.

З метою отримання криміналістично-значущої для оперативних працівників інформації використовуються різноманітні пошукові системи. Серед них є універсальні системи, такі як Google, Yandex, Yahoo, Ask, а також спеціалізовані інструменти для пошуку мультимедійного контенту, зокрема TinEye та Bing, які здатні знаходити фотографії, ілюстрації, малюнки, відео та аудіофайли. [3, с. 83].

Розпізнавання обличчя являє собою старий і поширений спосіб ідентифікації, що базується на унікальних рисах обличчя та формі черепа кожної людини. Комп'ютер автоматизує цей процес, використовуючи біометричні дані замість фото. Оскільки метод спирається на фізіологічні характеристики, він відноситься до статичних методів біометрії. Це найбільш інтуїтивно зрозумілий спосіб ідентифікації, схожий на те, як люди розпізнають одне одного. Останнім часом розроблені методи, що використовують інфрачервоне світло для сканування обличчя, тому метод також називають ідентифікацією за геометрією обличчя [6, с. 134].

Використовуючи програму по типу PimEyes, користувач завантажує зображення суб'єкта або об'єкта, інформацію стосовно якого планується отримати, та впродовж декількох хвилин отримує посилання на всі відкриті джерела в мережі Інтернет, які містять таке або подібне візуальне відображення.

В даний час існує чотири основні методи розпізнавання особи, які розрізняються складністю реалізації та метою застосування: метод автоматичної обробки зображення особи; «eigenfaces» (нім. «власне обличчя»); аналіз відмінних рис; аналіз на основі нейронних мереж [6, с. 135] Особливий інтерес становить технологія автоматичної ідентифікації особи людини на основі нейронних мереж за елементами зовнішності за її відображенням на фотографії або відеозаписі, яка має широке комерційне та наукове застосування. Дана технологія цікава тому, що може здійснюватися без контакту з об'єктом пошуку. У всесвітній мережі є онлайн-сервіси пошуку осіб за елементами зовнішності серед масиву фотозображень, що містяться у популярних соціальних мережах («Search4faces», «VK.watch» та ін.) на особистих сторінках осіб. За результатами пошуку сервіси надають користувачу масив, що складається з переліку максимально схожих осіб, із відсотковим зазначенням збігу зовнішності обличчя знайденої особи з досліджуваною [7, с. 156].

Для використання деяких інструментів на території України необхідним є встановлення спеціальних VPN-сервісів, які зашифровують трафік користувача та дозволяють відвідувати ресурси, обмежені за геопросторовим принципом.

Таким чином, розвідка з відкритих джерел та її інструментарій дає можливість: встановити особу правопорушника за фотографією; встановити місцезнаходження розшукуваного суб'єкта за

допомогою соціальних мереж, особистих сторінок особи та її знайомих; встановити коло знайомств підозрюваного, історію пересувань за допомогою геопозиціонування. Можемо стверджувати, що використання OSINT-ресурсів у ході досудового розслідування відкриває нові можливості для отримання доказової інформації без застосування обмежувальних заходів, що порушують приватність особи. Це сприяє підвищенню якості обраної тактики досудового розслідування, пришвидшенню процесу встановлення істини у кримінальному провадженні та розширює аналітичний потенціал слідчих органів. Застосування OSINT-інструментів забезпечує більш ефективне виявлення зв'язків між учасниками подій, аналіз інформаційного середовища та моніторинг цифрової активності підозрюваних.

---

1. Албул С.В. Обмін інформацією між суб'єктами оперативнорозшукової діяльності: сучасні проблеми та шляхи вирішення. *Актуальні проблеми кримінального права, процесу, криміналістики та оперативнорозшукової діяльності*. Хмельницький: Вид-во НАДПСУ, 2021. С. 587–589.
2. Ісмайлов К. Ю. Особливості кримінальної розвідки з відкритих джерел як інструмент збирання оперативної інформації. *Південноукраїнський правничий часопис*. 2016. № 2. С. 110-113.
3. Минько О. В., Іохов О. Ю., Оленченко В. Т., Власов К. В. Використання технологій OSINT для отримання розвідувальної інформації. *Системи управління, навігації та зв'язку*. 2016, Вип. 4 (40). С. 81-84.
4. Мовчан А.В. Поняття та сутність аналітичної розвідки як особливої форми інформаційно-аналітичної роботи в ОРД. *Науковий вісник ЛьвДУВС.* 2012. № 3. С. 443-450.
5. Щурат Т. Напрями використання OSINT в оперативно-розшуковій діяльності. *Роль та місце правоохоронних органів у розбудові демократичної правової держави*. Одеса: ОДУВС, 2022. 174 с. С.144-146.
6. Нечипоренко О. В., Корпань Я. В. Біометрична ідентифікація і автентифікація особи за геометрією обличчя. *Вісник Хмельницького національного університету.* 2016. № 4. С. 133-138.
7. Одерій О. В., Кожевніков О. А. Отримання криміналістично значущої інформації шляхом аналізу відкритих інтернет-джерел. *Правовий часопис Донбасу*. 2020. № 4. С. 154-156.

Кардашевський Юрій,
доктор філософії у галузі права,
керівник відділу внутрішнього контролю
(Національне агентство з питань запобігання корупції)

OSINT В СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ТА ДІЯЛЬНОСТІ ОРГАНІВ ПРАВОПОРЯДКУ

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.

У той же час, OSINT в контексті економічної безпеки можна визначити як процес збору, аналізу та використання публічно доступної інформації, що стосується різних аспектів економічної діяльності, з метою забезпечення національної безпеки та економічної стабільності. Це може включати дані з фінансових звітів, публічних оголошень, корпоративних повідомлень, баз даних, соціальних мереж та медіа-ресурсів.

Завдяки використанню OSINT у сфері економічної безпеки, органи правопорядку отримують можливість:

– виявляти потенційно небезпечні економічні операції, у тому числі відмивання грошей, фінансування тероризму, шахрайство, контрабанду та інші види економічних злочинів;

– проводити моніторинг діяльності компаній та організацій, під час якого виявляти незаконні схеми або порушення фінансових правил;

– аналізувати макроекономічні показники, що дозволяє прогнозувати загрози для економічної безпеки, такі як економічні кри-

зи, валютні спекуляції чи інші ризики, що можуть вплинути на стабільність національної економіки;

– використовувати дані для прогнозування злочинних дій, а також для попередження і своєчасного реагування на можливі загрози в економічному середовищі.

Процес збору економічних даних за допомогою OSINT є багатогранним і включає кілька основних етапів. Перш за все, потрібно чітко визначити, яку інформацію необхідно зібрати та для яких цілей вона буде використовуватися. Для цього важливо враховувати специфіку економічної безпеки і можливі загрози, з якими стикаються органи правопорядку.

Основні джерела даних для збору через OSINT включають:

– *публічні фінансові звіти та оголошення компаній*: компанії та організації публікують фінансові звіти, які містять інформацію про їхні доходи, витрати, активи та зобов'язання. Ці дані допомагають виявити аномалії або порушення, такі як маніпуляції з фінансами або непрозорі операції;

– *соціальні мережі та онлайн-платформи*: дані з таких платформ, як LinkedIn, Facebook, допомагають виявити зв'язки між підприємцями, політиками, банками, злочинними групами. Аналіз публічних комунікацій дає можливість виявити не тільки зв'язки, але й схеми організації злочинної діяльності;

– *бази даних та реєстри*: державні реєстри та публічні бази даних, такі як реєстрація компаній, банківські звіти, реєстрація прав власності та інші, є важливим інструментом для перевірки законності діяльності підприємств та осіб, зокрема виявлення фальшивих компаній або підозрілих фінансових операцій;

– *медіа-ресурси*: новини, статті, прес-релізи та інші публікації в медіа часто містять інформацію про незаконні або сумнівні економічні операції. Зокрема, фінансові скандали, розслідування й аналітичні матеріали можуть дати важливі вказівки для розслідувань;

– *інтернет-форуми та платформи для обміну інформацією*: на різноманітних форумах і спеціалізованих платформах часто обговорюються нелегальні або сумнівні економічні практики, що може бути корисним для органів правопорядку при виявленні незаконної діяльності.

Для того, щоб зібрана інформація мала реальну цінність для правоохоронних органів, необхідно застосовувати методи аналізу

та обробки даних. Зокрема, використання спеціалізованих інструментів для обробки великих обсягів даних (Big Data) допомагає виявляти патерни, тенденції та зв'язки між різними елементами інформації.

Однією з основних функцій OSINT у системі економічної безпеки є своєчасне виявлення потенційних загроз, які можуть призвести до порушень стабільності економічної системи. Це включає як прогнозування загроз, так і своєчасне реагування на них.

OSINT дозволяє:

– виявляти нелегальні фінансові операції, такі як відмивання грошей чи фінансування тероризму, аналізуючи фінансові потоки, транзакції та інші економічні дані;

– виявляти корупційні схеми, зокрема у державному секторі, завдяки моніторингу публічної інформації про діяльність державних службовців, контрактів, закупівель та інших економічних аспектів;

– виявляти й розслідувати шахрайські схеми в бізнесі, такі як фальшиві компанії, фіктивні фінансові операції, схемні інвестиції або маніпуляції на ринку цінних паперів;

– проводити моніторинг конкурентної діяльності, що дозволяє виявляти порушення антимонопольного законодавства або незаконні угоди між компаніями.

Завдячуючи інструментам OSINT можна не лише виявити загрози, але й прогнозувати їх, надаючи органам правопорядку час для реагування та вжиття заходів.

Хоча OSINT має великий потенціал, його використання в системі економічної безпеки не позбавлене низки проблем та викликів. Зокрема:

– *перевантаження інформацією*: великий обсяг даних, що надходить з відкритих джерел, може ускладнити процес аналізу та прийняття рішень. Важливо вміти фільтрувати корисну інформацію від неактуальних даних;

– *правові та етичні питання*: збір публічної інформації нерідко не супроводжується чіткими правовими межами, що може створити ризик для прав людини, зокрема порушення приватності. Важливо дотримуватися балансу між інтересами безпеки та правами громадян;

– *маніпуляції з інформацією*: дані з відкритих джерел можуть бути неповними або маніпульованими, що ставить перед органами правопорядку завдання з перевірки та верифікації цієї інформації;

– *кіберзагрози*: при зборі та обробці даних через інтернет існує ризик кіберзагроз, зокрема атак на системи збору даних, витоків інформації або хакерських атак.

Забезпечення безпеки є ключовим аспектом при використанні OSINT в економічній безпеці. Оскільки OSINT часто включає роботу з чутливою інформацією, необхідно впроваджувати низку заходів для захисту даних:

– *шифрування та захист каналів зв'язку* (для забезпечення безпеки передачі даних потрібно використовувати шифрування інформації та захищені канали зв'язку);

– *анонімність слідчих та аналітиків* (органи правопорядку повинні забезпечити анонімність своїх співробітників при зборі даних, щоб уникнути витоків або ризиків для особистої безпеки);

– *захист від кіберзагроз* (необхідно регулярно оновлювати програмне забезпечення та впроваджувати заходи для захисту від кібератак, таких як впровадження фаєрволів і систем виявлення вторгнень).

Підсумовуючи вище зазначене, можна стверджувати, що OSINT відіграє важливу роль у системі економічної безпеки, надаючи органам правопорядку потужні інструменти для збору, аналізу та моніторингу економічної інформації з відкритих джерел. Це дозволяє ефективно боротися з економічною злочинністю, виявляти порушення і сприяти збереженню стабільності економічної системи. Однак для ефективного використання OSINT необхідно подолати численні виклики, пов'язані з великим обсягом інформації, правовими питаннями та забезпеченням безпеки. Розвиток інструментів і методологій OSINT, а також впровадження належних заходів безпеки, дозволять органам правопорядку покращити свою діяльність і досягти кращих результатів у забезпеченні економічної безпеки.

Кісіль Зоряна,
доктор юридичних наук, професор,
заступник директора навчально-наукового інституту
управління, психології та безпеки
(Львівський державний університет
внутрішніх справ)
Кісіль Роман-Володимир,
кандидат юридичних наук,
науковий співробітник
науково-дослідної лабораторії
OSINT-досліджень та безпекової аналітики
навчально-наукового інституту управління,
психології та безпеки
(Львівський державний університет
внутрішніх справ)

ЗАСТОСУВАННЯ МЕТОДІВ OSINT В ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Перспективи застосування інформації власне із соціальних мереж в оперативних цілях є досить великими. Існує низка продуктивних алгоритмів щодо збору й аналітики цієї інформації із відкритих джерел, котрі необхідно взяти на озброєння співробітникам поліції оперативних підрозділів. Задля ефективної реалізації завдань, котрі поставлені перед оперативними підрозділами, необхідно не лишень підвищувати рівень грамотності діючих співробітників у царині комп'ютерної техніки та тактики одержання необхідної інформації з мережевих джерел, але й повсякчас удосконалювати інструменти пошуку, створювати додаткове, спеціалізоване програмне забезпечення, котре є придатним задля проведення аналізу власне за допомогою застосування даних із оперативних баз органів та підрозділів Національної поліції.

Одним із найважливіших інструментів задля проведення інформаційних операцій виступає OSINT – «розвідка за відкритих джерел», як один із векторів розвідки, котрий включає: пошук, вибір та збір розвідувальної інформації, отриманої із загальнодоступних джерел, та аналіз цієї інформації [1, с. 22].

Концепція OSINT позиціонується з двох чільних понять, а саме: 1) відкрите джерело; 2) загальнодоступна інформація [2, с. 123].

До факторів, які впливають на процес планування й підготовки ведення OSINT відносять: 1) ефективне інформаційне забезпечення; 2) релевантність; 3) доступність інформації; 4) спрощення процесів збирання даних; 5) обсяг; 6) якість; 7) ясність; 8) легкість використання; 9) мінімальна вартість.

Нині органах правоохорони західних держав функціонують спеціальні підрозділи, котрі здійснюють розвідку на підґрунті відкритих джерел інформації, а саме: Scotland Yard OSINT, Royal Canadian Mounted Police OSINT, OSINT unit of New York Police Department, OSINT unit of the Los Angeles County Sheriff's Department, британська BBC Monitoring, ізраїльський Хатсав, австралійське Управління національних оцінок [3].

Відповідно до вимог ст. 34 Конституції України, кожен має право вільно збирати, зберігати, використовувати й поширювати інформацію усно, письмово або в інший спосіб – на власний розсуд [4]. У межах кримінального провадження здійснення аналізу відкритих джерел інформації регламентовано главою 21 Кримінального процесуального кодексу України, зокрема в контексті розкриття порядку проведення такої негласної слідчої (розшукової) дії, як зняття інформації з електронних інформаційних систем [5].

У ч. 3 ст. 214 КПК України задекларовано, що проведення досудового розслідування (здійснення слідчих (розшукових) дій) до відкриття кримінального провадження не допускається та тягне за собою відповідну відповідальність (щодо досудового слідства виняток становить лише огляд місця події) [5].

З іншої сторони, положеннями ст. 9 Закону України «Про оперативно-розшукову діяльність» встановлено загальну заборону на проведення оперативно-розшукових заходів без запровадження оперативно-розшукової справи [5].

Задля об'єктивності застосування OSINT в учинах поліцейських відомств необхідно розмежовувати власне принципи одержання інформації з відкритих джерел та загально-правові, котрі співвідносяться не лишень із розвідувальною й правоохоронними учинами але й із будь-котрими царинами суспільних взаємовідносин; відомчі, котрі є характерними лишень для підрозділів, котрі здійснюють поліцейську оперативно-розшукові чи слідчі учини виключно у межах кримінального провадження. Застосування ме-

тодів OSINT у низці європейських країнах є власне невід'ємною частиною поліцейських учинів.

Водночас, нині, пропоновані для OSINT програмно-технологічні рішення сприяють:

– зібранню даних із соціальних мереж (Facebook, Twitter, Youtube);

– аналізові зібраної інформації;

– агрегуванні одержаної інформації з мережі Інтернет;

– оцінюванні достовірності інформації;

– моніторинг у та розпізнаванню ідентичності в мережі Інтернет, зокрема, і за допомогою геолокації;

– учинів із інформацією, одержаної з невидимого веб-простору (dark web, hidden web, deep web).

Відкриті джерела охоплюють значну кількість інформації, яка є необхідною, що сприяє осмисленню об'єктивних й суб'єктивних чинників, котрі є пов'язаними, зокрема, із здійсненням інформаційних операцій. Водночас, задля підвищення ефективності розвідувальних учинів відкрита інформація використовується у комплексі власне із конфіденційними ресурсами.

Отож, OSINT є сукупністю способів і методів розшуку інформації у загальнодоступних джерелах інформації. Чільними перевагами OSINT є власне доступність джерел і відсутність матеріальних затрат щодо отримання зазначеної інформації. Застосовуючи методи OSINT, співробітники поліцейських підрозділів мають можливість: встановити особу делінквента за фотографією; місцезнаходження особи; коло знайомств та зацікавлень підозрюваного, історію переміщень за допомогою аналізу геопозиціонування.

Застосування OSINT у сфері правоохоронної діяльності є важливим та перспективним вектором, який сприяє отриманню цінної інформації задля забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку. Розвиток технологій та методів OSINT, а також вирішення існуючих викликів та обмежень, сприятиме більш ефективному використанню цього інструменту для захисту держави та її громадян.

---

1. Williams, H.J. Defining second generation open source intelligence (OSINT) for defense enterprise. National Defense Research Institute Report. RAND Corporation, Santa Monica, California, 2018. 63 с.

2. Open Source Intelligence Tools and Resources Handbook/ i-Intelligence, 2018. 327 c.

3. Kyselov, A., & Kovalevska, O. (2022). An investigation of effective police communication. law enforcement roles requiring language skills. Methodological bases of studying the processes of general mental laws in human interaction with the environment. International Science Group. Boston: Primedia eLounch. https://doi.org/10.46299/ ISG.2022.MONO.PSYCHOL.1/Pp. 39-47.

4. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

5. Кримінальний процесуальний Кодекс України від 13 квітня 2012 року. Відомості Верховної Ради України (ВВР), 2013, № 9-10, № 11-12, № 13, ст.88: https://zakon.rada.gov.ua/laws/show/4651-17#n2036.

6. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 року. Відомості Верховної Ради України (ВВР), 1992, № 22, ст.303 URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text.

Коваль Тимур,
заступник начальника слідчого відділу
(Управління Служби безпеки України
в Сумській області)

НОВІТНІ МЕТОДИ РОЗСЛІДУВАННЯ ВОЄННИХ ЗЛОЧИНІВ

Анотація

Стаття присвячена аналізу новітніх методів розслідування воєнних злочинів в Україні. У центрі уваги – інформаційні системи, які дозволяють ефективно працювати з великим обсягом даних та враховувати контекстуальні елементи складу злочину. Розглянуто приклад бази даних «Відтворення» та переваги використання систем Delta, Palantir, Промінь+ та i2. Автори доводять, що ефективне розслідування неможливе без професійної аналітики та візуалізації. У статті наведено докази з міжнародних досліджень, які підтверджують ефективність використання графічних інструментів у сфері кримінальної юстиції.

Ключові слова: воєнні злочини, стратегічне планування розслідування, інформаційні системи, OSINT, мапування, контекстуальний елемент злочину, візуалізація доказів, кримінальний аналіз.

Постановка проблеми

Розслідування воєнних злочинів в Україні після 24.02.2022 поставило перед органами досудового розслідування нові виклики. Ці злочини мають специфічні ознаки, зокрема обов'язкову наявність контекстуального елементу складу злочину, що потребує особливої доказової бази та аналітичного підходу. Традиційні методи розслідування виявилися недостатніми для роботи з великими обсягами даних, які виникають під час документування воєнних злочинів.

Так, згідно ст. 216 КПК розслідування злочинів, передбачених ст. 436, 437-447 КК України належить до компетенції органів безпеки, тобто здійснюється слідчими Служби безпеки України (далі – СБУ). В певних випадках (за суб'єктним складом) такі злочини можуть розслідуватися Державним бюро розслідувань.

Статтею 2 ЗУ «Про Службу безпеки України» передбачено, що до завдань Служби безпеки України також входить попередження, виявлення, припинення та розкриття кримінальних право-

порушень проти миру і безпеки людства, тероризму та інших протиправних дій, які безпосередньо створюють загрозу життєво важливим інтересам України.

Із вказаних норм можна зробити висновок, що основний тягар у попередженні, виявленні, припиненні та розкритті кримінальних правопорушень за вказаною категорією злочинів лягає на органи досудового розслідування та оперативні підрозділи СБУ.

Органи досудового розслідування та прокуратура, які займаються досудовим розслідуванням міжнародних злочинів, через свою специфіку, тільки починають формувати певні стандарти і усталену практику. Зазначена категорія злочинів досить суттєво відрізняється від інших злочинів, передбачених КК України. Вказані обставини вимагають від нас реагувати на виклики, з якими до 24.02.2022 так масово не стикалася кримінальна юстиція і окремі її інституції зокрема.

Існує усталений вираз: «Ви не можете керувати тим, що ви не вимірюєте». Саме глибокий аналіз, окрім іншого, в рамках кримінальних проваджень, дозволить ефективно здійснювати попередження, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства.

Міжнародні злочини, мають окремий обов'язковий елемент складу злочину, контекстуальний, що підлягає доказуванню в рамках кожного кримінального провадження. Тому, особливу увагу у розслідуванні вказаної категорії злочинів потрібно приділяти саме контексту подій, в яких вчинено той чи інший злочин. Розслідування вказаної категорії злочинів вимагає спеціалізованих технічних навичок для аналізу доказів, таких як цифрова криміналістика, кібераналіз, геопросторовий аналіз та аналіз великих даних, що складно вмістити в одному слідчому.

Враховуючи ці обставини, сьогодні важко уявити ефективне розслідування воєнних злочинів без сучасних інформаційних систем. У наш час, коли масштаби злочинних дій значні, а обсяг інформації – надзвичайно великий, традиційні методи розслідування вже не можуть забезпечити належний рівень ефективності та оперативності. Використання інформаційних систем стало ключовим фактором для швидкого, точного та ефективного розслідування воєнних злочинів.

Виклад основного матеріалу

Практика розслідування вказаної категорії злочинів змусила органи безпеки України створити базовий «Стратегічний план розслідування», що розрахований орієнтовно на 6 місяців розслідування. Зазначений план включає обов'язкові блоки оперативних, слідчих (розшукових) та процесуальних дій, які, на нашу думку, мають бути проведені у кожному кримінальному провадженні. До таких блоків-завдань ми відносимо, окрім інших, наступні: Завдання №1 (Належне оформлення протоколу огляду. Вжиття вичерпних заходів щодо вилучення уламків), Завдання №2 (визнання осіб потерпілим, їх допити), Завдання №3 (Призначення необхідних експертиз, а саме СМЕ, вибухово-технічні, будівельні, та інших), Завдання №4 (Проведення допитів свідків, слідчих експериментів), Завдання №5 (Надсилання запитів до компетентних органів з метою отримання інформації про засоби і механізм ураження). На основі цих базових слідчих (розшукових) та процесуальних дій слідчі приймають рішення щодо подальшого процесу розслідування. З часом блоки завдань поповнилися наступними: «Проведення слідчо-аналітичної роботи (огляди відкритих джерел, OSINT, встановлення кола потенційних підозрюваних)» та «Робота в інформаційних системах таких, як «Дельта», «Palantir», «Промінь+», «Стрибо», «TeleZip360».

Підрозділами органів безпеки для таких цілей найбільш активно використовуються такі основні програми з екосистеми військових продуктів, як «Дельта», продукти технологічної компанії, яка спеціалізується на розробці програмного забезпечення для аналізу великих обсягів даних, а саме «Palantir», інформаційна система «Промінь+» та візуальне аналітичне середовище i2 Analyst's Notebook.

- **Delta** є системою, що забезпечує інтеграцію та аналіз інформації з різних джерел у реальному часі, що дає змогу оперативно виявляти зв'язки та взаємозалежності подій на фронті та у тилу.
- **Promin+** – українська інформаційна система, призначена для збору, зберігання та аналізу великої кількості структурованих і неструктурованих даних, що істотно прискорює роботу слідчих.
- **i2 Analyst's Notebook** – це міжнародна система аналітики, що дозволяє будувати детальні візуальні схеми та мережеві графіки для ідентифікації осіб, структур та злочинних зв'язків.

Методика роботи з інформаційними системами передбачає:

• Збір та структурування інформації у базах даних, де кожен факт, свідчення чи доказ фіксується у відповідних полях.

• Мапування подій на інтерактивних картах для створення просторово-часових моделей, що значно спрощує аналіз ситуації та встановлення контекстуальних зв'язків.

• Контекстуальний аналіз інформації, який дозволяє визначити, які події були взаємопов'язані і як вони вплинули на вчинення злочину, створюючи таким чином повну та обґрунтовану доказову базу.

Конкретним прикладом ефективності таких підходів є регіональна база даних «Відтворення», яка успішно застосовується в Сумській області. По суті, структурована база даних «Відтворення» – це регіональна реляційна база даних. Вона містить інформацію про більшість подій, пов'язаних з воєнними діями ворога на території Сумської області. Станом на сьогодні це більше 4000 рядків-подій. Вони стосуються 40 днів тимчасової окупації області. В середньому це 100 блоків фактичних обставин на один день перебування ворога на нашій території. Фактичні обставини зафіксовані у фото, відео матеріалах, показаннях свідків, потерпілих, військовополонених, результатах OSINT-досліджень, інформації сил оборони України, даних операторів мобільного зв'язку, космічного агенства, трофейних документах, інших джерелах. І ця база постійно наповнюється. Крім цього, на основі зібраних даних слідчими відділами здійснюємо мапування. Такий інструмент дає можливість створювати карти подій за певні проміжки часу, що значно спрощує уявлення слідчого, прокурора, слідчого судді і суду про фактичні обставини і події, що відбувалися.

Дослідження показують, що використання графіків і схем значно покращує сприйняття та засвоєння інформації. Наприклад, дослідження Університету Канзасу виявило, що візуальні пояснення покращують розуміння складних систем. Інше дослідження, опубліковане в журналі «Frontiers in Psychology», показало, що студенти, які використовували графіки для вивчення фізичних та економічних концепцій, покращили своє розуміння на 25-30% у порівнянні з тими, хто використовував лише текстові матеріали.

А воєнний злочин - це, досить часто, складна система рішень одних злочинців та бездіяльності інших. Значна частина злочинів

фактично вчинена організованою групою. І без інформаційно-аналітичних систем та аналітиків, які б професійно генерували бази даних, схеми і графіки для розуміння і прогнозування складних систем прийняття рішень ворогом, що не корелюють зі здоровим глуздом, нам не обійтися. Це потрібно слідчому, прокурору, суду.

Завдяки цьому слідчі можуть швидко знаходити необхідну інформацію, перевіряти взаємозв'язки подій та ефективно проводити розслідування.

Збройні сили України, Державна прикордонна служба України, розвідувальні органи України та інші інституції активно залучені до процесу виявлення воєнних злочинців в Україні. Кожна із цих структур щомісяця отримує сотні запитів на інформацію, щодо подій, які пов'язані з воєнними злочинами. Чи є здоровий глузд у тому, щоб запитувати одну й ту ж інформацію у розвідувальних та інших органів сотню разів у окремих провадженнях, якщо контекст подій був один? Певно, що ні. Отримавши одного разу таку інформацію і систематизувавши її, розумніше було б використовувати її сотні разів. Такі інформаційні системи, як Дельта, Промінь+, i2 Analyst's Notebook надають можливість слідчим більш ефективно здійснювати досудове розслідування злочинів за рахунок візуалізації інформації та використання напрацювань наших колег з інших регіонів і інституцій.

Відтворивши одного разу події у відповідній системі, зазначений аналітичних продукт можна використовувати у десятках, а то і сотнях кримінальних проваджень, що об'єднані одним контекстом.

Застосування бази даних «Відтворення» та зазначених інформаційних систем дозволило значно скоротити час розслідувань, підвищити точність та якість зібраних доказів. Такий підхід сприяє оперативності та результативності роботи слідчих груп.

Окремо слід зазначити, що використання вищевказаних інформаційних систем і інформації про контекст подій дає можливість стороні обвинувачення на ранніх стадіях розслідування приймати обґрунтовані рішення щодо об'єднання матеріалів кримінальних проваджень. Це дає змогу більш концентровано підходити до розслідування, не витрачати марно процесуальний час і не множити непотрібні процесуальні документи.

Для підвищення ефективності розслідувань регіональними органами безпеки створюються так звані «Базу знань». У хмарному

сховищі збережено і доступно кожному слідчому відповідно до свого напрямку відповідні схеми та аналітичні документи, що відображають регіональний контекст подій об'єднаний певними часовими проміжками. Це схеми встановленої структури окремої армії ворога, чи нижчих у ієрархії підрозділів, маршрути руху територією України окремих підрозділів та командирів ворога, місця знищення ворожої техніки, аналітичні документами за результатами аналізу документів окупаційних військ держави-агресора, що отримані в рамках кримінальних проваджень, списки особового складу військових частин ворога і т.д.

На підтвердження ефективності використання різного роду інформаційних систем у досудовому розслідуванні міжнародних злочинів слід звернутися до ряду наукових та корпоративних досліджень.

Якщо брати до уваги дослідження Гарвардського університету, людина запам'ятовує приблизно 80% з того, що бачить та робить, і лише 20% з того, що читає. Наприклад, графіки та діаграми можуть суттєво спростити розуміння статистичних даних, надаючи візуальне зображення тенденцій або співвідношень.

Зображення можуть швидше передавати інформацію та бути більш зрозумілими. Дослідження Nielsen Norman Group вказують, що користувачі витрачають лише 20% часу на читання тексту на веб-сторінках, але вони швидше схильні звертати увагу на візуальні елементи. Інформація у вигляді графічних елементів також допомагає зменшити когнітивне навантаження.

Якщо звести це до конкретного прикладу: при порівнянні сухого тексту на сторінці і графіку, що пояснює ту ж інформацію, шанс, що користувач запам'ятає та зрозуміє дані з графіку, може бути у 4-5 разів більший.

Графічна інформація робить сприйняття легшим і ефективнішим!

Щоб краще зрозуміти різницю між сприйняттям графічної інформації та сухого тексту, візьмемо дослідження від 3M Corporation. Вони виявили, що мозок обробляє візуальну інформацію у 60 000 разів швидше, ніж текстову інформацію.

Дослідження у Stanford University показало, що графічна візуалізація даних підвищує ефективність розуміння на 45%, у порівнянні з текстовими даними. Тобто людина може зрозуміти візуаль-

ні дані майже вдвічі швидше і краще, ніж якщо б це було представлено у вигляді сухого тексту.

Однак, використання вищевказаних інформаційних систем потребує значного часу для навчання і опанування. А ще маємо враховувати, що вони створені для виконання складних, системних завдань. На нашу думку, створення інформаційно-аналітичного сектору у структурі слідчих підрозділів регіональних органів безпеки є необхідним кроком для ефективного розслідування міжнародних злочинів та використання новітніх методів розслідування.

Отже, переваги використання інформаційних систем очевидні:

- Підвищення точності та якості розслідувань.
- Значна економія часу і ресурсів завдяки структурованості інформації та швидкому доступу до неї.
- Посилення ефективності слідчих дій за рахунок візуалізації та систематизації великих масивів даних.
- Потенціал для представлення чітких та переконливих доказів у міжнародних судових інстанціях.

Для успішної реалізації цих переваг критично важливим є залучення до роботи кваліфікованих аналітиків, які здатні професійно структурувати та обробляти інформацію. Розвиток цієї сфери не просто важливий, він необхідний для ефективного правосуддя у справах щодо міжнародних злочинів.

---

1. Закон України Про Службу безпеки України URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text;
2. Філоненко Т., Гюльмагомедов Д. Тридцять і більше відсотків додаткової ефективності кримінальної юстиції приховано у щоденних процедурах органів правопорядку, які потребують налаштування та спрощення. URL: https://justtalk.com.ua/post/napadnik--ne-golkiper-to-chomu-zh-slidchij-mae-buti-menedzherom;
3. Бурангулов В. А. Сутність кримінального аналізу. Південноукраїнський правничий часопис, 2023;
4. БОЛВІНОВ, С. (2024). Практичні аспекти застосування інформаційних систем під час розслідування воєнних злочинів (на прикладі системи SORC)1 *Вісник Кримінологічної асоціації України*, *32*(2), 531–543. https://doi.org/10.32631/vca.2024.2.38$
5. Бобек, Е., Тверскі, Б. Створення візуальних пояснень покращує навчання. Cogn. Research 1 , 27 (2016). https://doi.org/10.1186/s41235-016-0031-6;
6. Зоренко, Д.С. Кульчицька, Л.О. Лех, Р.В. Червяков, О.І. Використання інструментів та методів OSINT для отримання пошукової інформації. URL: https://dspace.nlu.edu.ua/handle/123456789/20299;

7. Брюкнер С., Златкін-Троїчанська О., Кюхеманн С., Кляйн П. та Кун Дж. (2020) Зміни в розумінні студентами цифрово представлених графів та їх візуальній увазі у двох областях вищої освіти: постреплікаційне дослідження.
Front. Psychol. 11:2090. URL: https://doi.org/10.3389/fpsyg.2020.02090;
8. Капустіна М.В., Демидова Є.Є., Латиш К.В.. Використання сучасних інформаційних технологій при розслідуванні воєнних злочинів URL: https://doi.org/10.32782/2524-0374/2023-4/134;
9. How People Read Online: The Eyetracking Evidence URL: https://www.nngroup.com/reports/how-people-read-web-eyetracking-evidence/

Ковчі Аттіла,
прокурор Управління
процесуального керівництва
досудовим розслідуванням та підтримання
публічного обвинувачення
(Генеральна інспекція
Офісу Генерального прокурора)

РОЛЬ І МІСЦЕ OSINT В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ, КЕРОВАНІЙ АНАЛІТИЧНОЮ РОЗВІДКОЮ (ILP)

У сучасному світі, де технології та інформація є основними рушіями соціально-економічного розвитку, правоохоронні органи стають залежними від інноваційних підходів до збору та аналізу даних. Одним з таких підходів є інтеграція розвідки з відкритих джерел (OSINT) в аналітичну розвідку, яка лежить в основі сучасної правоохоронної діяльності. Особливо актуальним цей підхід є в контексті інтеграції з так званою керованою аналітичною розвідкою (Intelligence-Led Policing, ILP), яка забезпечує ефективне управління інформацією та прийняття рішень на основі даних. В умовах, коли злочинність стає все більш складною та глобалізованою, роль OSINT в ILP стає незамінною.

Правоохоронна діяльність, керована аналітичною розвідкою (ILP), передбачає, перш за все, стратегічний менеджмент, що фокусується на аналізі та інтерпретації розвідувальних даних для прийняття рішень. Вона передбачає не лише оперативне реагування на злочини, але й націлену, проактивну роботу з прогнозування злочинної діяльності та запобігання її вчиненню. Підхід ILP забезпечує інтеграцію аналітичних даних з різних джерел для формування стратегії боротьби з злочинністю.

OSINT, або розвідка з відкритих джерел, – це процес збору, аналізу та використання публічно доступної інформації з Інтернету, медіа, публікацій, соціальних мереж, офіційних документів та інших джерел. Оскільки ця інформація доступна для широкої аудиторії, вона є важливим елементом у створенні повної картини для правоохоронних органів, особливо в межах аналітичної розвідки.

Інтеграція OSINT в ILP створює потужний інструмент для правоохоронних органів, що дозволяє не тільки швидко реагувати

на події, але й прогнозувати майбутні злочини, зокрема організовані, терористичні та кіберзлочини. Для ефективної роботи в цьому напрямку правоохоронні органи мають здатність обробляти великий обсяг даних, швидко виділяти важливу інформацію та використовувати її для прийняття оперативних рішень.

OSINT відіграє важливу роль у зборі інформації про злочинні групи, осіб, організації та події, що можуть вплинути на безпеку держави. Важливою особливістю OSINT є те, що він забезпечує доступ до величезних обсягів даних, які можуть бути використані для прогнозування злочинної діяльності, виявлення схем, зв'язків між злочинцями та їх діяльністю, а також для виявлення потенційних загроз.

У контексті ILP, OSINT може використовуватися для:

ідентифікації ключових осіб у злочинних організаціях або терористичних групах, їхніх зв'язків і місцезнаходжень;

моніторингу соціальних мереж для виявлення активності потенційних злочинців або терористів, що поширюють загрози або агітують за насильницькі дії;

аналізу публічно доступних даних для виявлення змін у схемах діяльності злочинців, таких як переміщення або зміна тактики.

Завдяки можливості збирати та аналізувати відкриту інформацію, правоохоронці можуть оперативно реагувати на зміни у поведінці злочинних елементів, що дозволяє зменшити час між виявленням загрози та її нейтралізацією.

Існує багато конкретних прикладів застосування OSINT у правоохоронній діяльності. Одним з них є виявлення потенційних загроз через соціальні мережі та інші відкриті джерела. Наприклад, використання технологій для моніторингу Twitter, Facebook та інших платформ дозволяє виявити осіб, які планують вчинення злочинів або, навпаки, вже активно залучені до кримінальної діяльності.

Ще одним важливим аспектом є використання OSINT для аналізу тенденцій злочинності та прогнозування її розвитку. Зібрані з відкритих джерел дані, такі як відомості про судові процеси, статистика злочинності та коментарі громадськості, дозволяють створювати моделі, які прогнозують найбільш ймовірні місця та типи злочинів у майбутньому.

Крім того, OSINT допомагає правоохоронним органам відслідковувати зміни у діяльності терористичних груп або злочинних

організацій, виявляти нові стратегії та методи, що використовуються для вчинення злочинів. Це дозволяє правоохоронцям адаптувати свої методи боротьби з новими викликами.

Для ефективного використання OSINT в рамках ILP правоохоронним органам необхідно володіти спеціалізованими інструментами та технологіями, які дозволяють збирати, обробляти та аналізувати великі обсяги даних з різних відкритих джерел. До таких інструментів відносяться:

платформи моніторингу соціальних мереж, які дозволяють відстежувати публікації, коментарі та інші взаємодії, що можуть свідчити про підготовку злочинів або терористичних актів.

інструменти аналізу великих даних (Big Data), які допомагають знаходити закономірності та взаємозв'язки між різними елементами даних, що зберігаються у відкритих джерелах;

машинне навчання та штучний інтелект, які дозволяють автоматизувати процеси аналізу та виявлення загроз у реальному часі;

системи геолокації для відстеження переміщення осіб чи об'єктів на основі публічних даних.

Ці інструменти надають правоохоронним органам можливість не лише швидко реагувати на злочинні дії, але й здійснювати їх прогнозування, що є важливим елементом аналітичної розвідки.

Хоча OSINT має величезний потенціал для застосування в ILP, існують певні виклики та обмеження, з якими стикаються правоохоронні органи при його використанні. Одним із головних викликів є *недосконалість технологій* збору та аналізу даних. Не всі доступні джерела є надійними, і існує великий ризик отримання недостовірної або неповної інформації.

Ще однією проблемою є *порушення прав людини*. Відкрита інформація з соціальних мереж і інших джерел може містити приватні дані, що можуть бути використані без згоди осіб, про яких йдеться. Це ставить під сумнів етичні та правові аспекти використання OSINT у правоохоронній діяльності.

З точки зору ILP, важливо забезпечити *правову визначеність* щодо того, які дані можуть бути використані, а також чітко визначити правила та процедури, за якими здійснюється збір і обробка інформації.

Інтеграція OSINT в ILP має величезний потенціал для розвитку правоохоронної діяльності. Перспективи цього процесу пов'язані з подальшим вдосконаленням технологій збору та обробки даних, розвитку аналітичних платформ, а також з ростом співпраці між державними органами і приватним сектором, зокрема в частині надання технічних засобів для збору відкритих даних.

У майбутньому важливо зосередити увагу на розробці *етичних стандартів і правових норм* щодо використання OSINT в правоохоронній діяльності, що дозволить забезпечити баланс між ефективністю боротьби зі злочинністю та захистом прав і свобод громадян.

Отже, роль OSINT у правоохоронній діяльності, керованій аналітичною розвідкою (ILP), є критично важливою для ефективного управління інформацією та прийняття рішень на основі даних. Інтеграція відкритої розвідки з відкритих джерел в ILP дозволяє правоохоронним органам не лише швидко реагувати на злочини, але й прогнозувати їх, забезпечуючи більш проактивний підхід до боротьби зі злочинністю. Однак для повної реалізації потенціалу OSINT необхідно подолати технічні, правові та етичні виклики, що стоять на шляху його ефективного використання в правоохоронній діяльності.

Колесников Максим,
здобувач вищої освіти
(Національний юридичний університет
імені Ярослава Мудрого)

OSINT У РОЗКРИТТІ ВОЄННИХ ЗЛОЧИНІВ

У сучасних війнах величезні обсяги інформації потрапляють у відкритий доступ через ЗМІ, соцмережі, супутникові знімки та інші джерела. Відкриті дані стали важливим ресурсом для розвідки з відкритих джерел (англ. Open source intelligence, OSINT) – концепції, методології й технології добування та використання військової, політичної, економічної та іншої інформації з відкритих джерел, без порушення законів у сфері національної безпеки та розслідувань [1]. Особливо актуальним OSINT стає у сфері міжнародного права під час розслідування воєнних злочинів, адже цифровізація позбавила воєнних злочинців можливості повністю приховати свої дії: інформація про злочини майже миттєво з'являється в інтернеті. Це відкриває нові можливості для документування та притягнення винних осіб до відповідальності, але водночас ставить питання щодо перевірки розслідувачами достовірності таких даних та використання їх як доказів у судовому процесі.

Воєнні злочини – це грубі порушення міжнародного гуманітарного права (напр., умисне спрямування нападів на цивільні об'єкти, страти полонених, застосування забороненої зброї тощо), для доведення яких традиційно збирали свідчення, речові докази, висновки експертів. Сьогодні ж до цього переліку додалися цифрові сліди, що фіксуються у відкритих джерелах. Величезна кількість матеріалів із зон конфліктів, оприлюднених безпосередніми свідками або навіть самими учасниками подій, перетворює соціальні мережі та інші платформи на своєрідні «архіви» воєнних злочинів. Так, цифрові сліди уже використовуються для винесення реальних вироків. Наприклад, у Фінляндії Гельсінський окружний суд визнав колишнього командира неонацистської групи «Русич» Войслава Тордена винним у вбивствах українських бійців і засудив його до довічного ув'язнення [2]. Інші волонтери в перші місяці війни в Україні створювали бази даних російських військових, підрозділи

яких причетні до масових убивств в Бучі під час наступу на Київ [3].

OSINT-розслідування воєнних злочинів спирається на різноманітні методи збору даних: моніторинг соціальних мереж (Facebook, Twitter, Telegram тощо) для виявлення відео/фото з місця подій, аналіз супутникових знімків руйнувань, зіставлення геолокацій та часових міток, пошук даних про військових у відкритих реєстрах. Наприклад, міжнародні групи журналістів «Bellingcat» використовують аналіз відеозаписів з різних ракурсів та супутникових фото для реконструкції хронології атак і ідентифікації відповідальних осіб/підрозділів [2]. Важливим етапом є перевірка достовірності отриманих даних: щоб відфільтрувати фейки та ворожі інформаційно-психологічні операції, вони застосовують відповідні стандартизовані підходи. Зокрема, контент зіставляють з кількох незалежних джерел, перевіряють метадані файлів, використовують зворотний пошук зображень для виявлення першоджерела, аналізують тіні та погодні умови на відео для підтвердження часу зйомки. Для систематизації цих підходів розроблено спеціальні процедури. Так, протокол Берклі (Berkeley Protocol) щодо цифрових розслідувань з відкритих джерел визначає стандарти для пошуку, збирання, зберігання, перевірки та аналізу відкритих джерел, щоб такі дані могли бути використані як докази в судових процесах [4].

Подібні розслідування істотно підвищили прозорість та оперативність документування воєнних злочинів. Якщо раніше від моменту вчинення злочину до судового рішення проходили роки, то зараз доказові матеріали збираються майже одразу після події. У такий спосіб можна зберегти актуальні свідчення, які з часом могли б бути втрачені або спотворені. Крім того, OSINT демократизував процес розслідування – тепер не лише державні органи, а й незалежні журналісти та навіть волонтери з усього світу можуть робити внесок у виявлення фактів злочинів [4].

OSINT як інструмент розслідування воєнних злочинів став невід'ємною частиною сучасної системи правосуддя у сфері збройних конфліктів. Розвідка з відкритих джерел сприяє швидкому виявленню й документуванню фактів, підкріплює традиційні докази цифровими слідами злочинів та розширює коло залучених суб'єктів. Попри існуючі виклики OSINT-розвідка вже довела свою ефективність. У міру вдосконалення стандартів перевірки і спів-

праці між OSINT-спільнотою та правовими інституціями, роль відкритих даних у міжнародних розслідуваннях лише зростатиме, сприяючи невідворотності правосуддя за найтяжчі злочини.

---

1. Open-source intelligence. Wikipedia. URL: https://en.wikipedia.org/wiki/Open-source_intelligence (дата звернення: 27.04.2025).

2. Мокренюк С. Докази з поля бою: роль Збройних сил України та можливості розвитку. Українська правда. 06.06.2023. URL: https://www.pravda.com.ua/columns/2023/06/6/7405597/ (дата звернення: 27.04.2025).

3. Жуков Є. Екс-командир «Русича» засуджений у Фінляндії до довічного ув'язнення. Deutsche Welle. 14.03.2025. URL: https://www.dw.com/ru/ekskomandir-rusica-osuzden-v-finlandii-na-poziznennoe-zaklucenie/a-71919685 (дата звернення: 28.04.2025)

4. Preserving Social Media Evidence of Mass Atrocities. Berkeley Human Rights Center. URL: https://humanrights.berkeley.edu/projects/preserving-social-media-evidence-of-mass-atrocities (дата звернення: 28.04.2025).

Колесник Олексій,
начальник Управління кримінального аналізу,
майор поліції
(ГУНП у Львівській області)

ВИКОРИСТАННЯ ІНСТРУМЕНТАРІЮ OSINT У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ ДЛЯ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ПРАВОПОРЯДКУ

У сучасному інформаційному суспільстві, де цифрові технології стрімко розвиваються, правоохоронні органи стикаються з новими викликами у сфері забезпечення національної безпеки та правопорядку. Одним із ефективних інструментів у боротьбі зі злочинністю є розвідка з відкритих джерел (OSINT), яка дозволяє збирати, аналізувати та використовувати інформацію з публічно доступних джерел для оперативного реагування на загрози.

OSINT (Open Source Intelligence) – це збір, аналіз, обробка даних які знаходяться у загальному доступі, але ці данні завжди специфічні, тобто зібрані та структуровані особливим способом, задля відповіді на конкретне питання [1, ст. 379].

Як зазначають Серватовський А. В., Онищенко Ю.М. та Макаренко П.В., у США сформована розгалужена мережа центрів і пунктів, що ведуть OSINT-розвідку та надають відомості більш ніж 7 тис. споживачам розвідувальних даних. І це не що інше, як результат скоординованих дій законодавчої і виконавчої влади, спрямованих на проведення цілеспрямованої політики в галузі забезпечення національної безпеки. Подібні структури є на всіх рівнях [1, ст. 380].

Ізраїль також використовує «OSINT» в першу чергу для аналізу військової спроможності противника. В структурі військової розвідки існує окремий спеціальний підрозділ для аналізу відкритих джерел інформації «Hatsaf», який збирає інформацію лише для військових цілей [1, ст. 380].

У Великобританії за допомогою «OSINT» цивільні журналісти служби BBC Monitoring здійснюють первинний збір інформації, яка в подальшому потрапляє до співробітників спецслужб для її використання за конкретними напрямами досліджень [1, ст. 380].

На сьогоднішній день OSINT активно та успішно використовується інформаційно-аналітичними підрозділами провідних країн світу. Дані щодо відсоткового співвідношення продуктивності відкритих джерел інформації підтверджують необхідність і актуальність використання досвіду США та європейських країн у вирішенні оперативних, тактичних і стратегічних завдань силових структур [2, ст. 109].

Використовуючи методи OSINT, можливим є:

- встановити особу, яка вчинила злочин, за фотографією;
- встановити місцезнаходження особи, яка перебуває в розшуку, за допомогою соціальних мереж, зокрема особистих сторінок як розшукуваної особи, так і кола її знайомих;
- встановити коло знайомств та інтересів особи тощо [2, ст. 109].

Під час розслідування злочину та встановлення підозрюваного можуть застосовуватись соціальні мережі для пошуку профілів, що відповідають опису ймовірних осіб, а також для відстеження їхньої онлайн-активності чи діяльності окремих груп. Наприклад, у справі, що стосується терористичного акту, можливе використання Facebook для виявлення користувачів, які поширювали радикальні політичні заяви або відвідували ресурси, пов'язані з терористичною діяльністю [3, ст. 265].

Використання відкритих джерел також може бути ефективним для встановлення мотивів злочину. Наприклад, у процесі розслідування вбивства ЗМІ можуть надати інформацію про жертву або підозрюваного, зокрема про можливі конфлікти між ними, що висвітлювались у газетах [3, ст. 265].

Цей інструмент дозволяє правоохоронним органам отримувати актуальні дані без порушення законодавства про конфіденційність та приватність.

В Україні правоохоронні органи активно впроваджують OSINT у свою діяльність. Зокрема, підрозділи Національної поліції використовують технології OSINT для протидії кримінальним правопорушенням, що дозволяє ефективно виявляти та документувати злочини, зокрема в умовах воєнного стану. Також OSINT застосовується для аналізу соціальних мереж та моніторингу інформаційного простору.

Підрозділи кримінального аналізу Національної поліції України активно впроваджують OSINT у свою діяльність. Кримінальний

аналіз, доповнений OSINT, дозволяє виявляти структури та зв'язки організованих злочинних угруповань. Це сприяє ефективному плануванню оперативно-розшукових заходів та запобіганню злочинності. У контексті збройної агресії проти України, OSINT став ключовим інструментом для документування воєнних злочинів. Підрозділи кримінального аналізу використовують відкриті джерела для збору доказів, що мають юридичну силу в міжнародних судах.

Тома М. Г. та Василова О. В. зазначають, що OSINT дає можливість проводити online-розслідування та віднайти цифрові сліди кримінальних правопорушень, доповнюючи дані з супутника.

Різні за розміром обсяги інформації, необхідні для порушення кримінального провадження, так і для подальшого розслідування воєнних злочинів та злочинів проти людяності, вже знаходяться у відкритому доступі. Просто відповідна інформація та її частини/фрагменти знаходиться ніби у тіні. Спеціалісти, що працюють у OSINT фрагментарно збирають цю інформацію у загальну картину відтворюючи реальність. До прикладу, з відкритих джерел ми дізнаємося про рух військових рф, зброї, стратегію ворога і навіть можемо дізнатись їхні майбутні кроки [4, ст. 908].

OSINT відіграє критичну функцію у виявленні та документуванні різноманітних доказів воєнних злочинів під час збройної агресії рф в Україні, його можливості у використані загальнодоступної інформації змінила методи підходу у розслідувані порушень прав людини та воєнних злочинів [4, ст. 909].

Незважаючи на переваги, використання OSINT супроводжується низкою викликів, зокрема: необхідність верифікації інформації, ризики порушення прав людини, а також потреба в спеціалізованому навчанні кадрів. Перспективи розвитку OSINT в Україні пов'язані з удосконаленням законодавства, впровадженням сучасних технологій та міжнародною співпрацею.

Інтеграція OSINT у правоохоронну діяльність є важливим кроком у зміцненні національної безпеки та правопорядку. Забезпечення ефективного використання цього інструменту потребує комплексного підходу, що включає правове регулювання, технічне оснащення та підготовку фахівців. Підрозділи кримінального аналізу та Департамент кримінального аналізу Національної поліції України відіграють ключову роль у цьому процесі, сприяючи впровадженню аналітичних підходів у правоохоронну діяльність.

1. Серватовський А. В., Онищенко Ю.М., Макаренко П.В. Міжнародний досвід використання OSINT. Актуальні питання протидії кіберзлочинності та торгівлі людьми: збірник матеріалів Всеукр. наук.-практ. конф. (23 листоп. 2018 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2018. С. 379-382.

2. Ліхтанська А. П., Михайлов В. О. Використання OSINT в кримінальному праві України. DICTUM FACTUM. 2024. № 1. С. 105–111. doi: 10.32703/2663-6352/2024-1-15-105-111.

3. Городовиков О. О. «Використання відкритих джерел (OSINT) під час кримінального аналізу» // Матеріали Всеукраїнської науково-теоретичної конференції студентів і аспірантів «Україна і світ: гуманітарно-технічна еліта та соціальний прогрес», 18–19 квітня 2024 р. Харків: НТУ «ХПІ», 2024. С. 263–265.

4. «Інструменти OSINT: фіксація воєнних злочинів в Україні» // Журнал «Актуальні проблеми політики», 2025. – № 136.

Копитко Марта,
доктор економічних наук, професор,
завідувач кафедри менеджменту та економічної безпеки
навчально-наукового інституту управління, психології та безпеки
(Львівський державний університет
внутрішніх справ)
Вінічук Марія,
кандидат економічних наук, доцент,
професор кафедри менеджменту та економічної безпеки
навчально-наукового інституту управління, психології та безпеки
(Львівський державний університет
внутрішніх справ)

СТРАТЕГІЧНІ ПРІОРИТЕТИ ВИКОРИСТАННЯ ІНСТРУМЕНТАРІЮ РОЗВІДКИ З ВІДКРИТИХ ДЖЕРЕЛ ПРИ ВИЯВЛЕННІ ЗАГРОЗ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ

Виклики і небезпеки сучасності, які пов'язані із повномасштабним вторгненням російської федерації на територію незалежної та суверенної України, мають вагомий негативний вплив на соціально-економічних розвиток країни та обумовлюють посилення ризиків і загроз, що призводить до зниження рівня національної безпеки. Зазначені тенденції істотно поглиблюються глобальними геополітичними трансформаціями та інформаційною агресією по відношенню до України, внаслідок чого активізуються кіберзагрози (атаки на державні реєстри та на критичну інфраструктуру), гібридні загрози (поєднання економічних, політичних, військових та інформаційних загроз), а також розгортається інформаційна війна на фоні постійної дезінформації, пропаганди та фейків, а також активізації терористичної діяльності, вербування та поширення екстремістського контенту.

Окреслені обставини вимагають вчасного реагування та постійного моніторингу інформації, доступної із відкритих джерел таких як ЗМІ, соціальні мережі, блоги, наукові публікації, аналітичні дослідження, урядові й корпоративні звіти, геопросторові та супутникові дані, з метою оперативного виявлення інформаційних операцій, деструктивної активності, переміщення військової техніки та підготовки терактів або диверсій. Використання інструмента-

рію розвідки з відкритих джерел дає можливість виявляти та відстежувати загрози національній безпеці України зовнішнього і внутрішнього характеру та вчасно попередити їх негативну дію через виявлення цих фейків, маніпуляцій, встановлення джерел поширення ворожої пропаганди та формування стратегії інформаційної протидії дестабілізуючим впливам.

В стратегічній перспективі використання інструментарію розвідки з відкритих джерел може забезпечити ефективну підтримку діяльності правоохоронних й розвідувальних органів у зборі доказових матеріалів у кримінальних провадженнях, в процесі розслідування шпигунських дій та терористичних актів, при аналізі підозрілої діяльності фізичних і юридичних осіб.

Не менш важливою технологія розвідки з відкритих джерел є при забезпеченні кібербезпеки на національному рівні, адже її інструментарій є ефективним засобом виявлення витоку інформації, моніторингу хакерських форумів та даркнету, а також для ідентифікації вразливостей критичної інфраструктури та для оцінки ризиків при формуванні державної політики безпеки й плануванні відповідей на гібридні загрози.

Інструменти розвідки з відкритих джерел на сучасному етапі запроваджуються у систему виявлення транснаціональних загроз, однак, в даному керунку Україна є досить слабкою та потребує міжнародної допомоги і підтримки щодо посилення її участі у глобальній безпековій архітектурі.

Таким чином, на підставі зазначеного, можна виокремити основні стратегічні пріоритети використання інструментарію розвідки з відкритих джерел при виявленні загроз національній безпеці України, а саме: (1) інституалізація розвідки з відкритих джерел в системі національної безпеки та її інтеграція в діяльність Центру протидії дезінформації; (2) розвиток інноваційних технологій розвідки з відкритих джерел, формування національної системи збору даних та впровадження штучного інтелекту; (3) налагодження механізмів обміну даними із міжнародними урядовими та неурядовими організаціями, а також участь у міжнародних розвідувальних ініціативах; (4) підвищення інформаційної грамотності; (5) забезпечення дотримання норм законодавства щодо захисту персональних даних; (6) розвиток нормативно-правової бази у сфері використання інструментарію розвідки з відкритих джерел.

Використання інструментарію розвідки з відкритих джерел дозволить вчасно виявляти та ідентифіковувати загрози національній безпеці України, посилювати обороноздатність країни та приймати виважені управлінські рішення щодо формування системи зміцнення національної безпеки.

Користін Олександр,
доктор юридичних наук, професор,
заслужений діяч науки і техніки України
(Інститут дослідження кібервійни)

OSINT В СИСТЕМІ АНАЛІТИЧНОЇ РОЗВІДКИ ОРГАНІВ ПРАВОПОРЯДКУ: МЕТОДОЛОГІЇ ТА БЕЗПЕКА СЛІДЧОГО

В умовах стрімкого розвитку цифрових технологій та глобалізації злочинності, органи правопорядку стикаються з необхідністю адаптації своїх методів до нових реалій. Одним з найбільш перспективних і важливих інструментів у цьому процесі є використання розвідки з відкритих джерел (OSINT) у системі аналітичної розвідки. Це дозволяє правоохоронним органам ефективно збирати, обробляти та використовувати інформацію для попередження, виявлення і розслідування злочинів. Водночас, застосування OSINT у слідчій діяльності ставить перед органами правопорядку низку викликів, зокрема щодо методології збору даних та забезпечення безпеки слідчого під час обробки та використання цієї інформації.

OSINT (Open Source Intelligence) – це процес збору, аналізу та використання публічно доступної інформації з відкритих джерел для розвідки та аналітики. У контексті діяльності органів правопорядку OSINT включає збір даних з інтернет-ресурсів, соціальних мереж, відкритих баз даних, медіа-джерел та публічних звітів. Оскільки ця інформація є публічною та доступною для загалу, вона є важливим інструментом для виявлення злочинних груп, організацій та схем їхньої діяльності.

Основними принципами використання OSINT у системі аналітичної розвідки є:

прозорість джерел – інформація повинна бути доступною для громадськості без порушення законодавства або етичних норм;

достовірність – необхідно підтвердити достовірність отриманої інформації через верифікацію джерел і співставлення даних з іншими незалежними джерелами;

аналіз та інтеграція – OSINT не лише збирає інформацію, але й інтегрує її в загальну аналітичну модель для формування розвідувальних висновків, які можуть бути використані для прийняття рішень.

Інтеграція OSINT у слідчу діяльність значно підвищує ефективність розслідувань, оскільки дає змогу правоохоронним органам працювати з великим обсягом інформації, що надходить з різних джерел. Зокрема, використання OSINT у слідстві дає можливість:

виявлення злочинців та їхніх зв'язків – відкриті джерела дозволяють визначити коло осіб, пов'язаних з конкретними кримінальними правопорушеннями, вивчити їхнє минуле, а також виявити зв'язки між ними, що допомагає розплутати складні кримінальні схеми;

моніторинг діяльності злочинних організацій – соціальні мережі, форуми та інші відкриті джерела дозволяють відстежувати діяльність злочинних груп, фіксувати інформацію про їхні наміри, переміщення та інші аспекти діяльності;

прогнозування злочинних дій – на основі зібраної інформації можна передбачити можливі злочини, виявити тенденції у поведінці кримінальних груп і своєчасно вжити заходів для їх попередження.

Важливою перевагою є те, що OSINT дозволяє розслідувачу діяти проактивно, ще до вчинення злочину, використовуючи інформацію про плани та наміри злочинців, які можуть бути опубліковані у відкритих джерелах.

Методи збору OSINT можна поділити на кілька основних категорій:

– *моніторинг соціальних мереж*: дослідження платформ, таких як Facebook, Twitter, Instagram, LinkedIn, для виявлення публікацій, коментарів та спілкування між підозрюваними особами. Зазвичай такі дані містять інформацію про можливі зв'язки між особами та їхні злочинні наміри.

- *використання спеціалізованих пошукових систем*: пошук за допомогою спеціальних інструментів, таких як Google Dorking, для отримання конкретної інформації з відкритих джерел, у тому числі з баз даних та інших архівів.

- *аналіз візуальної інформації*: аналіз фотографій, відео та інших мультимедійних матеріалів, які можуть бути знайдені в інтернеті. Це може включати визначення місцезнаходження об'єктів, осіб або подій, що важливо для розслідування.

- *інформаційні платформи та інструменти OSINT*: спеціалізовані інструменти для збору та аналізу публічно доступних даних,

такі як Maltego, Shodan, SpiderFoot та інші. Ці інструменти автоматизують процес збору даних та надають можливість аналізувати величезні обсяги інформації.

Процес аналізу даних передбачає не лише їхній збір, а й верифікацію та порівняння з іншими джерелами. Важливими аспектами є також створення баз даних, класифікація інформації та побудова зв'язків між елементами даних для подальшої аналітики.

Один з найважливіших аспектів використання OSINT у слідчій діяльності – це забезпечення безпеки слідчого та захисту інформації. Хоча OSINT заснований на відкритих джерелах, слідчі можуть стикатися з низкою ризиків, зокрема:

- *захист конфіденційної інформації*: під час роботи з OSINT слідчий може збирати дані, які стосуються приватних осіб або організацій. Це може включати конфіденційну інформацію, яка може бути використана не за призначенням.

- *ризик витоку інформації*: під час обробки та аналізу відкритих джерел важливо забезпечити захист даних від витоку або несанкціонованого доступу. Особливо важливо гарантувати безпеку при роботі з інструментами збору та зберігання даних.

- *захист від кіберзагроз*: використання інтернет-ресурсів для збору OSINT може бути пов'язане з ризиками кібератак. Злочинці можуть намагатися ввести фальшиву інформацію або маніпулювати даними, що можуть призвести до неправильних висновків або порушень процесу слідства.

- *збереження анонімності слідчого*: під час збору даних важливо забезпечити анонімність слідчого, щоб уникнути потенційних загроз для його безпеки з боку злочинців, які можуть виявити його активність.

З метою мінімізації цих ризиків правоохоронні органи повинні впроваджувати спеціальні заходи безпеки, такі як використання зашифрованих каналів зв'язку, впровадження політики конфіденційності та проведення навчання для слідчих.

Збір і використання даних з відкритих джерел має низку етичних та правових аспектів, які потрібно враховувати. Зокрема, важливо дотримуватися таких принципів:

- *дотримання прав людини*: збір і використання даних не повинно порушувати основні права громадян, зокрема право на при-

ватність. Слідчі повинні діяти в межах дозволеного законом і уникати несанкціонованого збору приватної інформації.

- *чітке дотримання законодавства*: збирання та використання даних з відкритих джерел повинно відповідати законодавству країни, особливо в частині захисту даних та боротьби з кіберзлочинністю.

- *прозорість процесів*: слідчі повинні діяти в межах встановлених процедур і стандартів, щоб їхня діяльність була прозорою та підзвітною громадськості.

Таким чином, правильне застосування OSINT в рамках слідчої діяльності дозволяє не лише підвищити ефективність розслідувань, а й зберегти високі етичні стандарти в процесі збору та обробки даних.

OSINT є важливим і необхідним інструментом в системі аналітичної розвідки органів правопорядку, оскільки дозволяє збирати важливу інформацію з відкритих джерел для розслідування та попередження злочинів. Однак ефективне використання цього інструменту вимагає чіткого розуміння методології збору та аналізу даних, а також уваги до забезпечення безпеки слідчого та етичних норм. Правоохоронні органи повинні активно вдосконалювати свої методи роботи з OSINT, щоб максимально використовувати його потенціал для забезпечення правопорядку і безпеки громадян.

Король Юля,
здобувач вищої освіти
(Львівський державний університет
внутрішніх справ)
Науковий керівник:
Ревак Ірина,
доктор економічних наук, професор,
завідувач науково-дослідної лабораторії OSINT-досліджень
та безпекової аналітики
навчально-наукового інституту управління,
психології та безпеки
(Львівський державний університет
внутрішніх справ)

РОЛЬ OSINT У СУЧАСНІЙ РОЗВІДЦІ ТА ПРОТИДІЇ АГРЕСІЇ РФ ПРОТИ УКРАЇНИ

Open Source Intelligence (OSINT), тобто розвідка на основі відкритих джерел, є ключовим інструментом у сучасній системі безпеки, що використовується для збору, аналізу та верифікації інформації з публічно доступних джерел. У контексті повномасштабної агресії рф проти України, OSINT став важливим компонентом державної та громадянської оборони, що дозволяє оперативно реагувати на виклики гібридної війни.OSINT OSINT – комплекс заходів, інструментів і методів для отримання та аналізу інформації з загальнодоступних джерел щодо певних осіб або організацій, неформальних груп, а також фактів, подій чи процесів [1, с. 4]. Вперше термін OSINT був використаний військовими і розвідувальними службами для позначення збору стратегічно важливої, але загальнодоступної інформації з питань національної безпеки [2].

Завдяки швидкому розвитку інформаційних технологій та інтернету, OSINT отримав новий поштовх, що зробило його важливим інструментом у сфері інформаційної безпеки, боротьби з тероризмом та у різних галузях комерційної діяльності [3, с. 678]. За результатами різних експертних оцінок, американські розвідувальні служби з відкритих джерел добувають від 35 % до 95 % розвідданих даних [4].

В умовах протидії загрозам з боку країни-терориста особливого значення набуває комплексна імплементація інструментів та

методів OSINT в повсякденну діяльність сектору безпеки і оборони нашої держави. Це допоможе виявляти обсяги та маршрути пересування військ агресора, викривати зрадників та колаборантів, розвінчувати фейки ворожої пропаганди, збирати доказову базу геноциду українців. Технології OSINT активно використовуються від початку російської збройної агресії проти України [1, с. 5].

Зокрема, аналітики OSINT спільноти Bellingcat у 2014–2022 рр. документували докази присутності регулярних підрозділів ЗС рф на Донбасі, використовуючи геолокацію фотографій, аналіз супутникових знімків і соцмереж. Під час повномасштабного вторгнення 2022 року ці підходи були масштабовані: 24 лютого 2022 року OSINT-аналітики в реальному часі фіксували пересування колони техніки рф у напрямку Києва, що підтверджувалося супутниковими даними компаній Maxar і Planet Labs.

Платформа GeoConfirmed забезпечила геолокацію відео обстрілів цивільної інфраструктури, що дозволило оперативно передавати дані до міжнародних правозахисних структур. Спільнота InformNapalm продовжує ідентифікувати російських військовослужбовців, причетних до воєнних злочинів, шляхом аналізу профілів у соцмережах, фото- та відеоматеріалів. Крім того, група Molfar активно займається виявленням дезінформаційних кампаній у цифровому середовищі, аналізуючи бот-мережі, фейки у Telegram та TikTok.

OSINT також активно використовується Збройними силами України та Силами безпеки для верифікації цілей, відстеження логістичних маршрутів противника, і навіть підготовки ударів по військових об’єктах – наприклад, низка ударів по аеродромах у Криму супроводжувалась ретельною OSINT-підготовкою.

Технологія OSINT в Україні відіграла важливу роль у підриві політичної стратегії росії в Україні. З початку лютого розвідка США голосно попереджала, що росія буде використовувати провокації як привід для початку війни в Україні. Прагнучи керувати міжнародним наративом і виправдовувати збройне втручання, росія робить хибні напади, звірські злочини та звинувачує в цьому українців. Однак, за допомогою OSINT ці інциденти щоразу викривають, що послаблює здатність путіна впливати на міжнародну реакцію на його вторгнення. Саме OSINT дозволяє українським військовим відстежувати пересування, плани та операції рашистів. Супутникові знімки надали українцям інформацію про

райони, атаковані російськими військами. Незашифровані радіохвилі та мобільні телефони дозволяють ЗСУ прослуховувати російські повідомлення [5].

Технологія OSINT показала, що російські військові атакували та націлювалися на мирних жителів та цивільні об'єкти, що значно збільшило міжнародну підтримку України [5].

Один із прикладів документування воєнного злочину рф проти України за допомогою OSINT-методів стосується обстрілу пологового будинку в Маріуполі 9 березня 2022 року. Після нападу міністерство оборони рф намагалося заперечити свою причетність, стверджуючи, що в будівлі перебували лише «бойовики» та що пологовий будинок давно не функціонував. Проте численні відкриті джерела дозволили встановити факт злочину. Зокрема, журналісти, OSINT-дослідники з Bellingcat і незалежні волонтери зібрали фото- й відеосвідчення очевидців, супутникові знімки до і після обстрілу, а також геолокаційні докази, що підтвердили точне місце удару. Відео з постраждалими вагітними жінками (одна з яких згодом померла від отриманих травм разом із ненародженою дитиною) було верифіковано за допомогою цифрових інструментів аналізу метаданих, тіней і погодних умов. Крім того, вдалося ідентифікувати тип боєприпасу, використаного при ударі [6].

Усе це дозволило кваліфікувати обстріл як цілеспрямовану атаку на цивільний об'єкт – пологовий будинок, що є грубим порушенням Женевських конвенцій та класифікується як воєнний злочин.

Отже, технологія OSINT відіграє надзвичайно важливу роль у сучасній розвідці, зокрема в умовах збройного конфлікту. Її методи дозволяють ефективно збирати, перевіряти й аналізувати інформацію з відкритих джерел для викриття воєнних злочинів, виявлення ворожої активності та протидії дезінформації. Український досвід доводить, що OSINT – це потужний інструмент у боротьбі за правду, безпеку та справедливість. OSINT є не лише допоміжним елементом у сучасній розвідці, а й ефективним інструментом стратегічного рівня. Його впровадження в структури національної безпеки України, а також синергія з громадянським суспільством, значно підвищують ефективність протидії збройній та інформаційній агресії рф. Подальший розвиток OSINT-підрозділів, інтеграція з кібер- та військовою розвідкою, а також міжнародна співпраця

створюють потенціал для формування стійкої системи безпеки нового покоління.

---

1. Використання інструментів та методів OSINT для отримання пошукової інформації: практичний порадник / Д. С. Зоренко, Р. В. Лех, Д. О. Кулик, О. І. Червяков ; Служба безпеки України, Інститут підготовки юридичних кадрів для Служби безпеки України Національного юридичного університету імені Ярослава Мудрого. 4-те вид. Харків, 2023.
2. Дослідження на основі відкритих джерел або OSINT: де використовується і в чому небезпека. 16.06.2021. URL: https://www.eset.com/ua-ru/about/newsroom/blog/business-security/issledovaniye-na-osnove-otkrytykh-istochnikov-ili-osint-gde-ispolzuyetsya-i-v-chem-opasnost-ru/
3. Open source intelligence tools and resources handbook. URL: https://i- intelligence.eu/uploads/public-documents/OSINT_Handbook_June-2018_Final.pdf
4. Яровой Т.С. OSINT як перспективний інструмент контролю за лобістською діяльністю в контексті державної безпеки. URL: https://maup.com.ua/assets/files/expert/6/18.pdf
5. Як OSINT впливає на війну в Україні? URL: https://itedu.center/ua/blog/articles/osint/?srsltid=AfmBOoo8dPyqgeSiT3FQJ4cWjxO3wkOhWYXqddYIJqTeITzJ5vdKZ7t6
6. Hospitals Bombed and Apartments Destroyed: Mapping Incidents of Civilian Harm in Ukraine. URL: https://www.bellingcat.com/news/2022/03/17/hospitals-bombed-and-apartments-destroyed-mapping-incidents-of-civilian-harm-in-ukraine/?utm_source=chatgpt.com

Коростельова Лілія,
головний спеціаліст Управління з питань осіб, безвісти зниклих за особливих обставин (Міністерство внутрішніх справ України)

РОЛЬ OSINT-ДОСЛІДЖЕНЬ У ПОШУКУ ЗНИКЛИХ БЕЗВІСТИ ГРОМАДЯН УКРАЇНИ: ВИКОРИСТАННЯ ВІДКРИТИХ ДЖЕРЕЛ ІНФОРМАЦІЇ ДЛЯ ВСТАНОВЛЕННЯ МІСЦЕЗНАХОДЖЕННЯ ОСІБ В УМОВАХ ВІЙНИ

Open Source Intelligence (OSINT) як комплекс інструментів збору інформації на основі відкритих джерел набуває важливого значення у правоохоронній діяльності. Використання OSINT дозволяє виявляти потенційні загрози, аналізувати великі бази даних (Big Data) та забезпечувати оперативне реагування на правопорушення. Проте правові аспекти її застосування залишаються недостатньо врегульованими, що створює виклики для правоохоронних органів. Значення OSINT суттєво зростає на фоні сучасних реалій інформаційних війн та гібридних загроз, які стали невід'ємною частиною міжнародних конфліктів, зокрема у контексті повномасштабного вторгнення країни-агресора в Україну. Це зумовлено швидким розвитком цифрових технологій, які дозволяють здійснювати моніторинг та аналіз інформації в реальному часі. Тому, вивчення генезису OSINT не лише допомагає зрозуміти її еволюцію, але й дає змогу вказати на інструменти, які можуть бути використані для протидії сучасним безпековим викликам, таким як боротьба з організованою злочинністю та злочинами проти основ національної безпеки [1].

У процесі дослідження генезису OSINT та застосування у правоохоронній діяльності було проаналізовано низку наукових праць, серед яких роботи таких дослідників як О. Ангельська [2], О. В. Дикий [3], Думчиков М. О. [4], А. Главацька, М. М. Горбач, М. Кирстя, А. О. Кисельов ,О. Є. Користін,Т. І. Коробейнікова, С. О. Мартинюк, І. А. Симак та інших вчених, що стали фундаментом для подальшого аналізу.

В умовах повномасштабної війни в Україні питання ідентифікації зниклих безвісти осіб набуло особливої актуальності. Тра-

диційні методи пошуку часто виявляються недостатніми через відсутність документів або пошкодження тіл. Тому наразі активно застосовуються інноваційні технології, зокрема системи розпізнавання обличчя та аналіз відкритих джерел інформації (OSINT).

Використання систем розпізнавання обличчя та аналізу відкритих джерел інформації є важливими інструментами у розшуку безвісти зниклих осіб в Україні. Ці технології дозволяють ефективно ідентифікувати осіб, спростовувати дезінформацію та сприяти правосуддю. Однак їх застосування повинно супроводжуватися дотриманням етичних норм та прав людини.

Застосування і ідентифікація пошуку зниклого безвісти є важливим інструментом в отримуванні інформуванні про людину, останнє місцезнаходження, переміщення людини та інші.

Використовуючи методологію OSINT працівниками Управління з питань безвісти зниклих за особливих обставин МВС України було знайдено 1769 осіб, які зникли під час бойових дій.

Отже, підсумовуючи вище зазначене можна зробити висновок, що аналіз відкритих джерел інформації дозволяють ефективно ідентифікувати зниклих осіб та отримувати важливі дані для розслідувань.

---

1. Басалик, С. А., Туз, О. С., & Тищук, В. В. (2025). Генезис інструментів OSINT та окремі аспекти їх використання у правоохоронній діяльності. *Український політико-правовий дискурс*, (9). URL: https://doi.org/10.5281/zenodo.15086041 (дата звернення 25.04.2025)

2. Главацька А., Ангельська О., Опірський І. Дослідження технологіївикористання OSINT як нової загрози з деанонімізації особи в інтернет просторі.*Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка"*.2024. No 1 (25), С. 19-50. DOI: https://doi.org/10.28925/2663-4023. 2024.25. 1950 (дата звернення 25.04.2025)

3. Дикий О. В., Сидорчук В. В. Поняття OSINT та суміжні категорії theconcept of OSINT and related categories. *Юридичний науковий електронний журнал*. 2024. No 9, С. 332-335. DOI: https://doi.org/10.32782/2524-0374/2024-9/78 (дата звернення 26.04.2025)

4. Думчиков М. О. Використання OSINT технологій для виявленнякорупційних правопорушень: сучасні підходи та виклики. *Академічні візії. Секція Право.* 2024. No 36, С. 1-6. DOI: https://doi.org/10.5281/zenodo.13928363 (дата звернення 26.04.2025)

Кульчицька Людмила,
співробітник
(Служба безпеки України, Апарат Голови)
аспірант ДНУ «Інститут інформації, безпеки і права
Національної академії правових наук України»

OSINT-СТРАТЕГІЇ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Розвідка з відкритих джерел (Open Source Intelligence – OSINT) стала, напевно, найуживанішим напрямом отримання даних різними суб'єктами та у різних сферах суспільного життя: від спеціальних служб до бізнеса і журналістських розслідувань та від документування воєнних злочинів, припинення спеціальних інформаційних операцій до перевірки контрагентів і викриття корупціонерів.

У секторі безпеки і оборони термін "OSINT" використовується у значенні окремої розвідувальної дисципліни (або дисципліни зі збору даних), що передбачає отримання даних з відкритих джерел, їх обробку, аналіз та поширення для задоволення розвідувальних потреб.

Більшість науковців погоджуються, що OSINT як окрема розвідувальна дисципліна зародилася в США. Водночас, в Україні з відновленням державності у 1991 році отримання даних з відкритих джерел також було повсякденною практикою оперативно-службової діяльності, проте, на відміну від США, без структурного виділення аж до останнього часу [1].

Найбільш системні описи змісту та процедурного наповнення OSINT викладені у збірниках «NATO Open Source Intelligence Handbook» (2001), "NATO Open Source Intelligence Reader" (2002), «NATO Intelligence Exploitation of the Internet» (2002), «Open Source Intelligence Tools and Resources Handbook» (2020), а також у стандартах 6522 «Спільна союза доктрина з питань розвідки з відкритих джерел» (AJP-2.9, 2019) і 6537 «Тактика, техніки та процедури розвідки з відкритих джерел OSINT» (AIntP-22, 2022). Важливо зазначити, що саме ці стандарти імплементовані в Україні, формуючи керівні принципи та регламентуючи процеси застосування OSINT у національному секторі безпеки і оборони [2].

Зокрема, AJP-2.9 та AIntP-22 визначають сукупність загальнорекомендованих тактик, технік та процедур із провадження на оперативному рівні стандартизованого OSINT-процесу. У них розкривається роль розвідувального циклу як ключової методики збору, обробки, аналізу пошукової інформації.

Вказані стандарти насамперед є настановами для об'єднаного командування й штабів НАТО. Однак аналіз Стратегії розвідспільноти США на 2024-2026 роки "Розвідка першої необхідності: Розкриття цінності OSINT" показав узгодженість термінів, застосовуваних у документації НАТО та Стратегії OSINT США. Так, джерелом OSINT є дані двох типів джерел:

1) Загальнодоступні (або публічно доступні) дані (Publicly Available Information).

У Доктрині AJP-2.9 пояснюється, що під цими даними розуміється будь-яка інформація, яку постять в інтернеті, публікують в медіа, транслюють в етері (радіо, телебачення) або надають для загального споживання (газети, плакати, білборди) або стенограми публічних зустрічей чи виступів [3].

2) Дані, що мають певне обмеження доступу.

У глосарії НАТО 2014 року вони названі "іншими джерелами інформації, що мають певні обмеження доступу або поширення серед громадськості" [4]. У Доктрині AJP-2.9 це "інформація обмеженого публічного поширення - матеріал, доступний для громадськості за певну плату" [5]. Дуже подібно, але ще лаконічніше, цей тип джерел визначено в Стратегії OSINT США – комерційно доступні джерела (Commercially Available Information) [6].

Стратегія OSINT США визначає такі чотири цілі, діяльність на досягнення яких має посилити інформаційні спроможності і розкрити потенціал розвідки з відкритих джерел:

- координація отримання даних з відкритих джерел, щоб уникнути дублювання дій, та розширення обміну результатами, методиками їх отримання, оцінками публічно і комерційно доступних джерел, щоб забезпечити ефективне використання ресурсів розвідспільноти;
- запровадження інтегрованого управління збором інформації з відкритих джерел в рамках розвідспільноти, щоб підвищити швидкість та поінформованість, уникаючи при цьому дублювання зусиль;

− впровадження інновацій в OSINT – розробка застосування сучасних інструментів, таких як штучний інтелект, машинне навчання, технології розпізнавання та обробки мови для виконання OSINT-завдань;

− розвиток кадрів та технологій OSINT наступного покоління, що передбачає створення і розвиток спільних стандартів роботи з інформацією, які відповідають динаміці змін технологічного середовища відкритих даних.

У Стратегії багаторазово наголошується, що розвідспільнота має переглянути свої стосунки з бізнес- та академічними колами, щоб використовувати ті передові можливості, що розробляються та застосовуються у приватному секторі та йдеться про потребу не допустити розвитку такого виклику як дублювання однорідної діяльності [7].

Ознайомлення із зазначеними документами показує, що Україна, стикаючись з подібними викликами (нераціональне застосування сил і засобів через дублювання), дія яких посилюється через агресію російської федерації, водночас має успішні і потужні напрацювання в сфері OSINT, які розроблені для відсічі збройній агресії. Йдеться про напрацювання механізмів взаємодії з громадським та приватним сектором, створення власних OSINT-платформ ситуаційної обізнаності тощо. Однак досі невирішеними залишається питання уніфікації підходів до проведення OSINT та координації цієї діяльності, чому мало би сприяти напрацювання загальнодержавної стратегії OSINT в органах сектору безпеки і оборони.

На наше переконання, вказана стратегія має включати такі елементи як:

− розбудова OSINT-інфраструктури для забезпечення інформаційних потреб тактичного та стратегічного рівнів: створення систем збору, аналізу, поширення (обміну) інформації за уніфікованими підходами в секторі безпеки і оборони;

− розробка та застосування інноваційних технологічних рішень зокрема на основі ШІ для здобування, обробки, аналізу даних з відкритих джерел;

− підвищення рівня професіоналізму - навчання особового складу можливостям OSINT, володіння OSINT-інструментарієм, обмін досвідом, напрацьованими унікальними методиками, успішними практиками та засвоєними уроками на основі невдач;

− подальше посилення співпраці з іноземними партнерами, приватним сектором, громадянським суспільством, академічними колами з питань проведення OSINT та розробки OSINT-інструментарію;

− застосування OSINT-спроможностей для протидії рф: документування злочинної діяльності держави-агресора, викриття ворожих ІПСО, відслідковування діяльності, що підлягає санкціям, по всьому світу та у взаємодії з іноземними партнерами.

В умовах сьогодення OSINT – це не рутинна кабінетна робота, а прикладна та високорезультативна розвідувальна дисципліна, що дозволяє отримати відомості про ворога без ризику для життя. Разом з тим вона потребує колосальних ресурсів та часу для аналізу даних і визначення їх впливу на національну безпеку нашої держави. Зважаючи на це, OSINT стала обов'язковою складовою професійної діяльності співробітників як Служби безпеки України сектору безпеки і оборони України. Методологія українського OSINT інтегрує визнані міжнародні підходи, чинні стандарти НАТО та безцінний практичний досвід, отриманий під час відсічі повномасштабній збройній агресії РФ.

Розробка, прийняття та подальше втілення в життя стратегії OSINT сектору безпеки і оборони України дозволить максимально ефективно використати потенціал розвідки з відкритих джерел для забезпечення національної безпеки України і досягнення стратегічної переваги над поточними та майбутніми супротивниками, геополітичними конкурентами та іншими суб'єктами, чия діяльність спрямована проти національних інтересів України.

---

1. Використання інструментів та методів OSINT для отримання пошукової інформації : практичний порадник. 5-те вид., переробл. та доповн. / Зоренко Д. С., Кульчицька Л. О. та ін. Харків : Видавець О. А. Мірошниченко, 2024. 80 с.

2. Перелік прийнятих чинних стандартів НАТО, передбачених Цілями партнерства, в Міністерстві оборони України, Збройних Силах України та інших складових сектору безпеки і оборони. [сайт] URL: https://www.mil.gov.ua/content/mil_standard/0752024_Perelik_standartiv_NATO.pdf

3. Allied Joint Doctrine for Open-Source Intelligence. Chapter 1. Open Source intelligence fundamentals. Section 2. Explanation and clarification of terms. URL: https://standards.globalspec.com/std/14361963/ajp-2-9

4. Базові поняття стратегічних комунікацій: стандарти на основі документів НАТО (англо-український та українсько-англійський словник) / [Л. Компанцева та ін.]. Київ : Нац. акад. СБУ, 2019. 335 с.

5. Allied Joint Doctrine for Open-Source Intelligence. Chapter 1. Open Source intelligence fundamentals. Section 2. Explanation and clarification of terms. URL: https://standards.globalspec.com/std/14361963/ajp-2-9

6. The IC OSINT Strategy 2024-206 “The INT of First Resort: Unlocking the Value of OSINT”. URL: https://www.dni.gov/files/ODNI/ documents/IC_ OSINT_Strategy.pdf

Кучеренко Анастасія,
здобувач вищої освіти
(Національна академія Служби безпеки України)
Науковий керівник:
Жевелєва Ірина,
кандидат юридичних наук, доцент
(Національна академія Служби безпеки України)

ЗАКОНОДАВЧЕ РЕГУЛЮВАННЯ КОНКУРЕНТНОЇ РОЗВІДКИ В УКРАЇНІ

Конкурентна розвідка (КР) – це процес збору та аналізу інформації виключно з відкритих і легітимних джерел з метою ухвалення ефективних управлінських рішень. Вона орієнтована на підвищення конкурентоспроможності організацій, моніторинг ринку та мінімізацію ризиків. КР є важливим елементом стратегії управління підприємствами, оскільки дозволяє ефективно прогнозувати зміни на ринку, оцінювати тенденції та виявляти конкурентні переваги [1, с. 103].

Конкурентна розвідка відрізняється від промислового шпигунства тим, що ґрунтується на етичних принципах і законних методах збору інформації. Вона не порушує права на конфіденційність та не використовує підривні методи, характерні для шпигунства. Крім того, вона відрізняється від бізнес-розвідки, оскільки бізнес-розвідка фокусується на зборі внутрішньої інформації компанії, в той час як конкурентна розвідка вивчає зовнішнє середовище: ринок, конкурентів, технології та інші фактори, що можуть впливати на розвиток бізнесу.

Необхідність правового регулювання конкурентної розвідки обумовлена її близькістю до розвідувальної діяльності, зокрема через використання відкритих джерел і методи, які можуть бути схожі на методи спецслужб. В Україні наразі це питання не має достатнього законодавчого врегулювання, що створює прогалини та неясність у правовому полі. Законодавчі обмеження зазвичай стосуються таких аспектів, як захист комерційної таємниці, захист персональних даних та запобігання порушенням прав третіх осіб [1, с. 105].

Значення конкурентної розвідки для безпеки та управління важко переоцінити. Вона дозволяє виявляти нових конкурентів,

прогнозувати тенденції ринку, виявляти потенційні ризики та попереджати витоки інформації. Це також є важливим інструментом для забезпечення інформаційної безпеки бізнесу і покращення репутаційного менеджменту. Конкурентна розвідка допомагає компаніям не лише реагувати на зовнішні загрози, а й своєчасно отримувати інформацію для коригування стратегії розвитку.

Для здійснення конкурентної розвідки використовуються різноманітні інструменти та технології. Основними джерелами інформації є Інтернет, соціальні мережі, агрегатори даних, а також технології Big Data і штучний інтелект. Для збору інформації застосовуються методи OSINT (розвідка з відкритих джерел), що аналогічні тим, що використовуються в спецслужбах. Це дозволяє ефективно здійснювати аналіз і прогнозування, не порушуючи законодавства [6].

В умовах повномасштабної війни, значення конкурентної розвідки для національної безпеки України зросло. Важливими стали ініціативи в сфері освіти та підготовки кадрів, такі як OSINT Academy, Attack Index та курси з медіаграмотності. КР також є важливою для виявлення фейків, інформаційних атак і кібератак, які є значними загрозами для інформаційної безпеки держави [9].

Міжнародний досвід у сфері конкурентної розвідки показує, що у багатьох країнах існують чіткі стандарти та регламенти. Наприклад, в США розроблені стандарти для OSINT (ATP 2-22.9), а також існують спеціалізовані ради та асоціації, що займаються питаннями розвідки з відкритих джерел. У мирний час до 90% розвідінформації надходить саме з відкритих джерел, що підкреслює важливість легальних методів збору інформації [9].

З точки зору розвитку законодавства, важливо створити нормативну базу, яка чітко визначатиме межі між легітимною конкурентною розвідкою та незаконним шпигунством. Також необхідно забезпечити державну підтримку освітніх ініціатив і професійних спільнот у сфері КР, а також адаптувати міжнародний досвід правового регулювання OSINT до українських реалій.

Конкурентна розвідка повинна здійснюватися в рамках правових норм. Це означає, що аналіз інформації має проводитись без порушення правових чи етичних норм, а її основною метою є отримання відкритої інформації для поліпшення управлінських рішень, а не порушення законодавства чи прав третіх осіб.

Законодавче регулювання конкурентної розвідки в Україні здійснюється через низку нормативно-правових актів, таких як Конституція України [7], Цивільний [10] та Кримінальний кодекси [8], Закони “Про інформацію” [4], “Про захист персональних даних” [3] і “Про охоронну діяльність” [5]. Особливу увагу слід звернути на Закон «Про захист від недобросовісної конкуренції» [2], який регулює використання комерційної інформації.

Водночас є важливими питання щодо захисту комерційної таємниці, авторського права і прав на персональні дані, що мають важливе значення для законності конкурентної розвідки. Зібрана інформація не повинна порушувати права третіх осіб, зокрема на конфіденційність та приватність. Це також включає правові аспекти, пов’язані із захистом персональних даних, що становлять важливу частину конкурентної розвідки.

На основі міжнародного досвіду та національних реалій, для розвитку конкурентної розвідки в Україні важливо ухвалити додаткові нормативні акти, які будуть регламентувати специфіку цієї діяльності. Законодавство має чітко визначати правила збору, обробки та використання інформації, а також забезпечувати баланс між економічною конкуренцією і захистом особистих та комерційних даних [6].

Загалом, конкурентна розвідка є важливою складовою національної безпеки, оскільки забезпечує державу інформацією про економічні, технологічні та інші аспекти діяльності суб’єктів господарювання. В Україні законодавче регулювання цієї сфери потребує системного підходу, що базується на імплементації міжнародних стандартів і забезпеченні ефективної інформаційної безпеки для бізнесу та держави.

---

1. Андрощук Г. О. Законодавство України про захист від недобросовісної конкуренції: становлення, розвиток, проблеми регулювання. Часопис Київського університету права. 2024. № 2. С. 103–112. URL: https://doi.org/10.36695/2219-5521.2.2024.20 (дата звернення: 22.04.2025).

2. Про захист від недобросовісної конкуренції: Закон України від 07.06.1996 № 236/96-ВР. Відомості Верховної Ради України (ВВР). 1996. № 36. Ст. 164.

3. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. Відомості Верховної Ради України (ВВР). 2010. № 34. Ст. 481.

4. Про інформацію: Закон України від 02.10.1992 № 2657-XII. Відомості Верховної Ради України (ВВР). 1992. № 48. Ст. 650.

5. Про охоронну діяльність: Закон України від 22.03.2012 № 4616-VI. Відомості Верховної Ради України (ВВР). 2013. № 2. Ст. 8.

6. Кирій В. В., Солодкий В. С., Тімофєєв В. О. Конкурентна розвідка та контр-розвідка: навч. посібник. Харків: ХНУРЕ, 2015. 380 с.

7. Конституція України від 28.06.1996 № 254к/96-ВР. Відомості Верховної Ради України (ВВР). 1996. № 30. Ст. 141.

8. Кримінальний кодекс України: Закон від 05.04.2001 № 2341-III. Відомості Верховної Ради України (ВВР). 2001. № 25–26. Ст. 131.

9. Ланде Д. В. Правові питання конкурентної розвідки (с. 51–68) URL: https://ippi.org.ua/lande-dv-pravovi-pitannya-konkurentnoi-rozvidki-st-51-68 (дата звернення: 22.04.2025).

10. Цивільний кодекс України: Закон від 16.01.2003 № 435-IV. Відомості Верховної Ради України (ВВР). 2003. № 40–44. Ст. 356.

Лісов Олександр,
кандидат історичних наук,
доцент кафедри управління
та інформаційно-аналітичного забезпечення
оперативно-службової діяльності
Центру стратегічних комунікацій ННІ
інформаційної безпеки та стратегічних комунікацій
(Національна академія Служби безпеки України)

ОКРЕМІ АСПЕКТИ ВІДНЕСЕННЯ РЕЗУЛЬТАТІВ ОСІНТ-ДІЯЛЬНОСТІ ДО ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

У світі, де інформаційне поле стало одним із ключових театрів сучасного конфлікту, розвідка з відкритих джерел (ОСІНТ, англ. OSINT) набула виняткової ваги в структурах спецслужб і поступово трансформувалася з допоміжного інструменту у самостійну розвідувальну дисципліну. Водночас не втрачає своєї актуальності питання правового й організаційного статусу результатів ОСІНТ-діяльності. Вже не одне десятиліття серед науковців і практиків необхідність віднесення інформації, здобутої спецслужбами із загальнодоступних джерел, до інформації з обмеженим доступом є предметом дискусій. Одні доводять необхідність засекречувати певні дані, отримані в результаті ОСІНТ, для захисту національної безпеки або оперативних переваг, інші стверджують, що, оскільки ОСІНТ ґрунтується на загальнодоступній інформації, її результати повинні залишатися незасекреченими.

Це питання, серед іншого, стало предметом обговорення на конференції з ОСІНТ, що організував Офіс Директора Національної розвідки (США) ще у вересні 2008 року. Зокрема колишня співробітниця американської розвідки, директорка з розвідувальних досліджень в Джорджтаунському університеті доктор Дженніфер Сімс у своєму виступі підкреслювала, що факт використання в ОСІНТ загальнодоступних джерел не означає, що результати цієї діяльності можуть бути автоматично віднесені до категорії відкритої інформації. Розвідувальні дані, здобуті шляхом аналізу відкритих джерел, можуть мати високий рівень чутливості, особливо у випадках, коли вони забезпечують інформаційну перевагу у проце-

сі прийняття рішень у сфері національної безпеки. На думку доктора Сімс, якщо OCINT-результати створюють аналітичну перевагу, що впливає на формування безпекової політики або підтримує ухвалення критично важливих державних рішень, то така інформація має розглядатися як чутлива. Її охорона не повинна базуватися лише на характері джерел чи методів збору, а передусім – на цінності та впливовості самих висновків. Мірилом успіху розвідки, за твердженням фахівчині, завжди буде конкурентна перевага, яку вона забезпечує, а переваги зникають, якщо ви їх втрачаєте як шляхом розголошення, так і через вжиття недостатніх заходів для їх захисту. «Розвідувальна перевага – це результат, який потребує захисту незалежно від того, яким шляхом вона була здобута» – підсумовує Сімс [1].

З іншого боку, на окрему увагу заслуговує й аналіз проблеми завищення грифу секретності OCINT-результатів. Це питання ґрунтовно розглядає фахівець із понад 45-річним досвідом у сфері розвідки, колишній керівник найбільшої OCINT-структури Міністерства оборони США та чинний голова Комітету практиків Фонду OCINT Девід Різ. У своїй публікації [2] він звертає увагу на парадокс сучасної розвідки з відкритих джерел, результати якої часто без належних підстав отримують статус інформації з обмеженим доступом. У багатьох випадках доступ до інформації, яка зберігає свій відкритий характер, обмежується лише через те, що вона створена в межах розвідувальної структури.

Також системною проблемою автор вважає надмірне засекречення OCINT-продуктів. Це, на його думку, не лише суперечить природі розвідки з відкритих джерел, а й знижує потенціал її використання у системі національної безпеки, особливо у контексті міжвідомчої та міжнародної взаємодії: ускладнює інформаційний обмін, обмежує доступ навіть уповноважених осіб та підриває ефективність використання OCINT-результатів у режимі реального часу, що особливо критично в умовах кризових ситуацій.

Засекречення, на думку Д. Різа, має фокусуватися не на відкритій інформації, а на методах, технологіях або аналітичних моделях, які дійсно потребують захисту. При цьому, результати OCINT повинні залишатися максимально доступними, якщо це не створює безпекових ризиків [2].

Серед ОСІНТ-практиків часто зустрічається поміркована позиція щодо накладання грифу на ОСІНТ-результати – дотримання балансу між оперативними потребами та управлінням ризиками. Розповсюдження інформації повинно бути обмеженим та контрольованим, особливо в контексті чутливих досліджень, щоб уникнути витоків та попередження об'єктів розслідування.

У цьому аспекті важливою є й практика країн-членів Північноатлантичного альянсу щодо віднесення результатів ОСІНТ-діяльності до інформації з обмеженим доступом, закріплена в стандартах НАТО. Так, у межах виконання Цілей партнерства Україна-НАТО Департаментом інформаційно-аналітичного забезпечення Служби безпеки України проведено ґрунтовну роботу з опрацювання стандартів Альянсу, за результатами якої у 2023 році відомство запровадило два стандарти за напрямом розвідки з відкритих джерел: STANAG 6522 Ed. 1 / AJP-2.9 Ed. A Allied Joint Doctrine For Open-Source Intelligence; STANAG 6537 Ed. 1 / AIntP-22 Ed. A Open Source Intelligence (OSINT) Tactics, Techniques And Procedures. Зокрема, у другому стандарті окремий підрозділ присвячено питанню обмеження доступу до інформації в межах ОСІНТ-діяльності, що у загальних рисах розкриває політики НАТО у цій сфері.

Хоча зазначені стандарти не відносяться до нормативно-правових актів, вони передбачають використання в СБУ операційних процедур, сумісних з підходами НАТО, а також гармонізують термінологію у сфері розвідки з відкритих джерел з основними категоріями та поняттями, якими оперують структури Альянсу.

Відтак, основними підставами для надання ОСІНТ-результату грифу обмеження доступу можуть бути:

– Правові та політичні обмеження. Уряди та організації мають чітку політику, що регулює використання, зберігання та поширення розвідувальних даних, отриманих у межах ОСІНТ-діяльності.

– Результати ОСІНТ-діяльності, які включають інформацію від країн-партнерів або засекречених баз даних, можуть мати грифи секретності на основі угод, політик чи умов користування.

– Операційна безпека (OPSEC). Навіть якщо дані є загальнодоступними, їх використання спецслужбами може свідчити про зацікавленість в об'єкті, розкриваючи оперативні пріоритети.

– Ризики контр-ОСІНТ. Спецслужби противника, окремі організації, групи і особи можуть відстежувати ОСІНТ-активність суб'єктів розвідувального співтовариства України, щоб визначити, що саме досліджує або планує організація.

– Ризик агрегування (ефект мозаїки). Загальнодоступна інформація, яка на перший погляд здається нешкідливою, при узагальненні та аналізі може виявити інсайти, які не були очевидними в ізольованому вигляді.

– Ризик розкриття чутливих джерел і методів. Якщо методи збору інформації з відкритих джерел розкривають таємні прийоми, методи або інструменти, що використовуються розвідувальними службами, вони можуть потребувати захисту. Іноді розвідувальний продукт, заснований виключно на відкритій інформації, повинен бути засекречений, щоб захистити інтереси уряду від розголошення.

– Національна безпека. ОСІНТ-результати, що виявляють вразливості у військових операціях, критичній інфраструктурі або кіберзахисті, можуть бути засекречені. Тобто ОСІНТ-дослідження необхідно проводити для оцінки вразливості не тільки противника, але й власної держави чи організації.

ОСІНТ, попри відкрий характер на етапі збирання, може перетворюватися на чутливу інформацію в результаті аналізу, узагальнення та розкриття контексту. Така інформація здатна створити суттєву перевагу в ухваленні рішень у сфері національної безпеки, а отже – потребує належного захисту. У зв'язку з цим суб'єктам розвідувального співтовариства України доцільно впроваджувати політики, що дозволяють оцінювати чутливість інформації в межах ОСІНТ-діяльності та визначати обґрунтовану необхідність обмеження доступу до них. Водночас засекречування не повинно бути надмірним, адже це може суперечити принципам транспарентності, підзвітності та свободи інформації. Баланс між оперативними потребами та управлінням ризиками має досягатися через чітко прописані нормативні критерії й прозорі процедури віднесення ОСІНТ-результатів до інформації з обмеженим доступом.

---

1. Aftergood S. An Argument for Open Source Intelligence Secrecy. 17.09.2008. URL: https://fas.org/publication/osint_secrecy/ (дата звернення: 27.04.2025).
2. Reese D. Open-Source Intelligence and the Challenges of Overclassification. *Lawfare*. 2024. URL: https://www.lawfaremedia.org/article/open-source-intelligence-and -the-challenges-of-overclassification (дата звернення: 24.04.2025).

Лукащук Юрій,
доктор філософії,
асистент кафедри
автоматизованих систем управління
(Національний університет
«Львівська політехніка»)

ВИКОРИСТАННЯ ХМАРНИХ ТЕХНОЛОГІЙ ДЛЯ АВТОМАТИЗАЦІЇ ЗБОРУ ТА АНАЛІЗУ OSINT-ДАНИХ

У сучасному цифровому середовищі хмарні технології стали важливим інструментом у багатьох сферах, включаючи бізнес, державне управління, медицину та освіту. Вони надають зручний доступ до великих обсягів даних та обчислювальних ресурсів через Інтернет, дозволяючи здійснювати роботу з будь-якої точки світу [1].

Open Source Intelligence (OSINT), або розвідка з відкритих джерел, передбачає процес збору, обробки та аналізу інформації, що є публічно доступною в Інтернеті та інших відкритих платформах [2]. З огляду на швидкий розвиток цифрових технологій, більшість критично важливої інформації з'являється через пости в соціальних мережах, новини, блоги, форуми, а також супутникові зображення. Однак із зростанням обсягів цих даних ефективне їх опрацювання вручну стає складним і малоефективним.

Хмарні технології дозволяють значно спростити автоматизований збір та аналіз OSINT-даних, забезпечуючи масштабованість, гнучкість і інтеграцію з інструментами штучного інтелекту (ШІ) для більш точного аналізу. Це робить обробку великих масивів інформації більш ефективною, що є особливо важливим в умовах сучасних глобальних загроз, таких як гібридні війни, інформаційні атаки та швидко змінювана ситуація в реальному часі [3].

Серед основних переваг хмарних обчислень для OSINT варто відзначити можливість обробки великих даних у реальному часі, доступ до ресурсів з будь-якої точки світу, автоматизацію процесів збору та обробки даних, а також інтеграцію з технологіями машинного навчання для аналізу текстів, зображень і відео.

Архітектура типових систем OSINT, побудованих на основі хмарних технологій, включає кілька основних етапів. Спочатку

здійснюється збір даних із відкритих джерел, таких як веб-скрейпінг, API-запити або потоки даних з соціальних мереж. Це дає можливість отримати великі обсяги інформації в автоматизованому режимі, що значно скорочує час на збори.

Далі дані зберігаються у хмарних базах даних, наприклад, у BigQuery, DynamoDB чи Cloud Storage, що гарантує високу доступність та надійність зберігання інформації, а також масштабованість системи.

Для обробки даних використовуються серверлес-технології, зокрема AWS Lambda або Google Cloud Functions. Вони дозволяють динамічно масштабувати ресурси в залежності від обсягу даних. Також для роботи з потоковими даними активно застосовуються платформи, такі як Apache Kafka або Cloud Pub/Sub.

На етапі аналізу використовуються інструменти машинного навчання, серед яких Amazon SageMaker та Google Vertex AI, що дозволяють здійснювати класифікацію, прогнозування та виявлення аномалій у даних. Завершальний етап включає візуалізацію результатів за допомогою BI-платформ, таких як Google Data Studio чи Power BI, що забезпечує зручне та зрозуміле представлення аналітичної інформації.

Системи OSINT на основі хмарних технологій активно застосовуються для моніторингу соціальних мереж, де автоматизовано відстежуються ключові слова, географічні локації та зміни у публікаціях на платформах. Такі системи дозволяють оперативно виявляти важливі тенденції та події.

У сфері безпеки та конфліктології технології OSINT використовуються для створення карт конфліктів, де супутникові знімки комбінуються з відкритими даними, зокрема з інформацією із соціальних мереж, що дозволяє відслідковувати переміщення техніки та активність у зоні конфлікту. Подібні рішення допомагають оперативно реагувати на зміни ситуації на місцях [4].

Також варто зазначити важливість використання OSINT для боротьби з дезінформацією, де застосовуються методи виявлення повторюваних патернів, аналізу джерел поширення інформації та контент-аналізу для ідентифікації потенційно маніпулятивних повідомлень.

Незважаючи на численні переваги, застосування автоматизованих систем OSINT потребує дотримання етичних та правових

стандартів, зокрема забезпечення приватності користувачів, відповідності законодавству та захисту даних.

З розвитком технологій хмарні рішення для OSINT продовжують інтегруватися з новітніми досягненнями штучного інтелекту, що дозволяє підвищити ефективність фільтрації дезінформації та покращити візуалізацію результатів. У майбутньому очікується подальше вдосконалення таких систем, що відкриває нові можливості для їх застосування у різних сферах діяльності.

---

1. Pannu H. S., Tuli S. (2021). Cloud computing for scalable OSINT frameworks. Journal of Cloud Computing, 10(1), 1–14.

2. Bazzell M. (2021). Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information. 9-th ed. IntelTechniques.

3. Федоренко, І. М. (2023). Перспективи використання штучного інтелекту у сфері OSINT. Науковий вісник НТУУ «КПІ», № 4, с. 112–117.

4. ENISA. (2021). Cybersecurity and Digital Transformation: The Role of OSINT. European Union Agency for Cybersecurity.

Мага Андрій,
прокурор відділу нагляду
за додержанням законів регіональним органом безпеки
та процесуального керівництва і публічного обвинувачення
у кримінальних провадженнях щодо злочинів,
вчинених в умовах збройного конфлікту
(Прокуратура Автономної Республіки Крим
та міста Севастополя)

OSINT-ДОСЛІДЖЕННЯ ЯК ІНСТРУМЕНТ ВИЯВЛЕННЯ, ДОКУМЕНТУВАННЯ ТА РОЗСЛІДУВАНЯ ВОЄННИХ ЗЛОЧИНІВ

Загальне поняття OSINT (Open Source Intelligence) як методу збору, аналізу та перевірки інформації з відкритих доступних джерел.

Актуальність OSINT-дослідження у кримінальному процесі під час міжнародного збройного конфлікту а його критичне значення при здійсненні досудового розслідування за фактами вчинення воєнних злочинів, у тому числі при відсутності доступу до тимчасово окупованої території України.

Структура та вимоги до процесу проведення OSINT-дослідження у кримінальному провадженні, широке та вузьке розуміння і використання вказаного інструменту.

Нормативне регулювання у кримінальному процесуальному законодавстві України пошуку, здобуття та фіксації доказів шляхом проведення OSINT-дослідження.

Рекомендаційні вимоги Протоколу Берклі (Berkeley Protocol on Digital Open Source Investigations) – міжнародного стандарту ведення цифрових розслідувань, їх використання у кримінальному процесі.

Алгоритм та особливості складання протоколу огляду при проведенні OSINT-дослідження у кримінальному процесі.

Практичні аспекти OSINT-дослідження у кримінальному провадженні, участь спеціаліста у складанні протоколів огляду при здійсненні розслідування кримінальних проваджень, пошук, виявлення, фіксація та збереження здобутої інформації.

Можливі джерела отримання доказів при здійсненні OSINT-дослідження під час розслідування воєнних злочинів (інформації вебсайти, соціальні мережі, новинні ресурси тощо, реальні приклади).

Питання належності та допустимості доказів, здобутих під час проведення OSINT-дослідження у кримінальному провадженні.

Особливості дослідження судом під час судового розгляду доказів, здобутих при здійсненні OSINT-дослідження.

Основні виклики та проблеми використання OSINT-дослідження під час досудового розслідування кримінальних правопорушень за фактами вчинення воєнних злочинів.

Позитивні та негативні приклади з практичної діяльності документування, розслідування воєнних злочинів з використанням методів OSINT-дослідження, підтримання публічного обвинувачення у вказаній категорії кримінальних проваджень.

Особливості доказування за допомогою OSINT-дослідження фактів вчинення злочину, передбаченого ч.1 ст. 438 КК України – порушення законів та звичаїв війни, передбачених міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України, що виразилось у порушенні вимог ст. 147 Женевської Конвенції про захист цивільного населення під час війни від 12.08.1949 та полягало у примушуванні осіб, які перебувають під захистом, служити в збройних силах держави окупанта.

---

1. Кримінальний процесуальний кодекс України. https://zakon.rada.gov.ua/laws/ show/4651-17#Text
2. Протокол Берклі з веденням розслідувань з використанням відкритих цифрових даних. https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley- Protocol-Ukrainian.pdf
3. Вирок Дарницкого районного суду міста Києва від 24.04.2023, справа №753/14148/21. https://reyestr.court.gov.ua/Review/110409601
4. Вирок Дніпровського районного суду міста Києва від 06.04.2024, справа №755/11177/23. https://reyestr.court.gov.ua/Review/119559177

Манжай Олександр,
кандидат юридичних наук, професор,
завідувач кафедри протидії
кіберзлочинності навчально-наукового інституту № 4
(Харківський національний університет внутрішніх справ)

ПРО ОДИН СПОСІБ АНАЛІЗУ ДАНИХ СПІВТОВАРИСТВ У TELEGRAM

У мережі Telegram нерідко можна зустріти співтовариства, контент в середині яких містить ознаки кримінальної протиправності. Враховуючи викладене, під час вирішення оперативно-службових завдань може виникнути потреба в аналізі даних таких співтовариств. Простий логічний аналіз без використання спеціалізованого програмного забезпечення може не дати бажаних результатів з багатьох причин. Однією з головних причин у згаданому контексті є великий обсяг даних, з яким, зазвичай, доводиться працювати.

Враховуючи викладене, на основі наших попередніх напрацювань, а також матеріалу Стівена Лернера [1] можна запропонувати досить ефективний спосіб аналізу даних співтовариств Telegram, який може бути застосований і для других упорядкованих даних про соціальні зв'язки.

В основі наведеного способу використання зв'язки програм Telegram-Desktop+Excel+Gephi.

По-перше, потрібно в форматі JSON експортувати історію чату, який потрібно проаналізувати, в програмі Telegram-Desktop. Надалі JSON -файл імпортується до Excel, обробляється, а сформовані таблиці про вузли графу (користувачів) та ребра (повідомлення) передаються в програму Gephi.

Після проведення первинного укладання графу з великою кількістю вузлів можна побачити, що його візуальна інформативність не перебуває на належному рівні (рис. 1). Враховуючи викладене, потрібно виокремити частини графу, які становлять інтерес для дослідника.

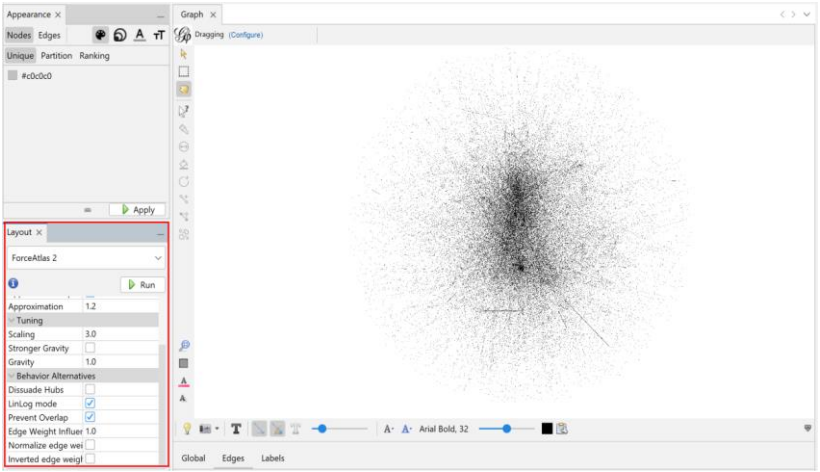


Рис. 1. Вигляд графу після укладання з використанням алгоритму ForceAtlas 2

У даному випадку проведемо аналіз таким чином (рис. 2):

1) розрахуємо модулярність, на підставі якої позначимо кольорами окремі співтовариства;

2) відобразимо на схемі вузли, які мають найбільшу потужність (кількість зв'язків) та приберемо з відображених вузлів саму групу, яка найчастіше створює повідомлення. Визначимо розмір вузлів пропорційним кількості зв'язків, тобто отриманих (надісланих) повідомлень;

3) сформуємо підсумкову читабельну схему.

Як наслідок на схемі будуть наявні найбільш активні учасники групи, однаковим кольором будуть позначені користувачі, які входять до одного співтовариства, розмір вузлів відображатиме інтенсивність написання повідомлень в групі, товщина стрілок та їх напрями відображатимуть кількість та напрям надсилання повідомлень. У даному випадку на схемі можна виводити або імена користувачів або відповідні ID, щоб довгі написи не заважали сприйняттю схеми. Перемикання відповідного способу відображення здійснюється через меню  (переключення між Id та Label).

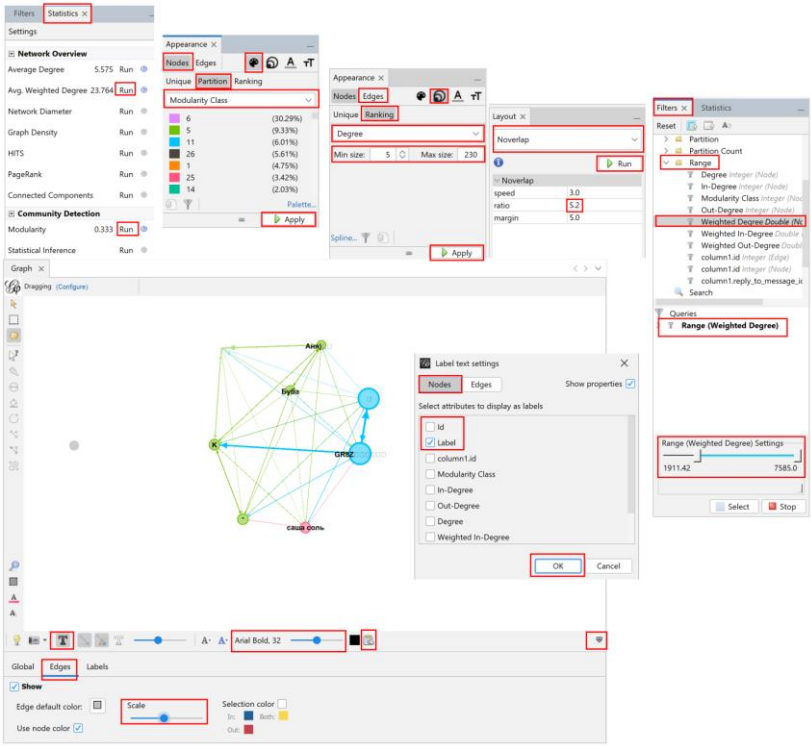


Рис. 2. Побудова графу з ключовими учасниками групи

Підсумкова схема будується за допомогою вкладки Preview та зберігається у потрібному розмірі.

Крім наведеного способу вельми перспективним виглядає застосування інструментів штучного інтелекту для аналізу великих структурованих даних про соціальні зв'язки [2]. Під час такого використання можна сформувати перелік користувачів, які мали найбільшу активність, та визначати стилістичні співпадіння між акаунтами. Для отриманого переліку користувачів можна створювати часову діаграму розміщення повідомлень з позначенням кількості постів по годинах різними кольорами по аналогії з тепловою мапою. На підставі аналізу часу розміщення постів можна розрахувати, в яких країнах можуть перебувати користувачі. Крім того, з використанням засобів штучного інтелекту можна швидко будува-

ти психологічні профілі користувачів, проводити кластерний аналіз з візуалізацією результатів тощо.

---

1. Lerner S. Telegram 101 to 401: SANS Cyber Defense. URL: https://www.youtube.com/watch?v=7lCd_fTa-Zo (дата звернення 28.04.2025).
2. McGraw J. W. How I turned ChatGPT into an intelligence analyst. URL: ttps://cybernews.com/editorial/chatgpt-analysis-hacktivist-pattern-recognition (дата звернення 28.04.2025).

Нагірна Оксана,
кандидат економічних наук, доцент,
доцент кафедри менеджменту та економічної безпеки
навчально-наукового інституту управління,
психології та безпеки
(Львівський державний університет
внутрішніх справ)

ТЕХНОЛОГІЇ OSINT: МОЖЛИВОСТІ ТА ПОТЕНЦІЙНІ ЗАГРОЗИ

OSINT (розвідка з відкритих джерел) - це процес легального отримання, вивчення та тлумачення даних, які вільно доступні для загального користування. Цей підхід активно застосовується в різних галузях - від IT-безпеки до медіа, від аналітики бізнесу до правоохоронної діяльності. Попит на знання в сфері OSINT стрімко зростає, адже вони дозволяють:

- виявляти потенційні загрози;
- ідентифікувати та аналізувати діяльність осіб;
- здійснювати перевірку фактичних даних;
- перевіряти достовірність інформаційних джерел;
- фіксувати ранні сигнали кібератак;
- аналізувати ринкових конкурентів;
- оцінювати репутацію або благонадійність конкретної особи [1].

Під час роботи з відкритими джерелами важливо дотримуватись певних принципів, які забезпечують ефективність і безпеку OSINT-діяльності. Ось ключові рекомендації:

1. Дотримання правових та етичних норм: уся діяльність повинна відповідати чинному законодавству та нормам етики. Варто поважати приватність людей і не використовувати зібрані дані на шкоду чи з порушенням закону.

2. Оцінка достовірності джерел: необхідно критично ставитися до джерел інформації, зокрема з інтернету. Перш ніж використовувати дані, переконайтесь у надійності та авторитетності джерела.

3. Комплексний аналіз даних: інформацію слід отримувати з кількох джерел і аналізувати з різних боків, щоб мати повну картину подій або явищ.

4. Захист і збереження даних: зібрану інформацію важливо надійно зберігати та оберігати від стороннього доступу - зокрема, за допомогою шифрування й інших засобів безпеки.

5. Постійне оновлення знань: Оскільки середовище відкритих джерел постійно змінюється, аналітик має регулярно підвищувати свою кваліфікацію.

6. Використання професійного інструментарію: спеціалізовані платформи та сервіси значно полегшують збір і обробку інформації, дозволяючи працювати швидше й точніше.

7. Забезпечення конфіденційності: у деяких випадках потрібно зберігати анонімність - для цього варто використовувати VPN, проксі та інші інструменти.

8. Актуалізація джерел: інформація з часом може втрачати актуальність, тому слід регулярно перевіряти, чи залишаються джерела релевантними.

9. Фіксація дій: Документування процесу допомагає відстежувати, як була зібрана та оброблена інформація, і вирішувати можливі помилки.

10. Спільне навчання та обмін досвідом: Співпраця з іншими фахівцями дозволяє збагачувати власний досвід і підвищувати ефективність роботи [2].

Дотримання цих рекомендацій гарантує результативне, безпечне й етичне застосування OSINT у будь-якій професійній сфері.

Для фахівців у сфері кібербезпеки застосування методів OSINT відкриває можливість виявляти публічно доступні дані про внутрішні процеси компаній, а також інформацію, що стосується зовнішнього середовища. Іноді до таких відомостей може належати чутлива інформація, яку організація мимоволі оприлюднила, наприклад, через метадані. Серед подібних вразливостей можна виділити: відкриті порти та незахищене обладнання, підключене до мережі; застаріле або невиправлене ПЗ; версії програм, назви пристроїв, параметри мереж і IP-адреси; випадкові витоки, як-от публікація власного коду на GitHub. Водночас, відкрита природа OSINT несе й потенційні загрози. Оскільки ці дані доступні кожному, ними можуть скористатися й кіберзлочинці. Найбільш поширені сценарії зловживання включають: використання соціальних платформ для збору особистої інформації про працівників, яка може стати підґрунтям для фішингових атак. LinkedIn, наприклад,

активно використовується для такого аналізу, хоча й інші мережі надають важливі відомості, як-от дні народження, імена дітей чи домашніх улюбленців - усе це часто використовується в паролях; завдяки розвитку хмарних технологій, сканування уразливого ПЗ, відкритих портів або неправильно сконфігурованих сервісів стало недорогим і легкодоступним. Крім того, ресурси на зразок GitHub часто стають джерелом чутливої інформації, зокрема облікових даних. Буває, що розробники несвідомо залишають у коді паролі або ключі доступу - саме такий випадок стався з Uber, коли через витік на GitHub було зламано внутрішню мережу компанії [3].

Отже, OSINT є цінним інструментом для збору інформації з різноманітних відкритих джерел. Вона надає можливість отримувати відповіді на численні запитання без необхідності звертатися до конфіденційних або засекречених матеріалів.

---

1. Що таке OSINT у 2025: Гайд від Molfar. URL: https://molfar.com/blog/shcho-take-osint-u-2024-gaid-vid-molfar.

2. Що таке OSINT (Open Source Intelligence, розвідка на основі відкритих джерел)? URL: https://thetransmitted.com/adlucem/shho-take-osint-open-source-intelligence-rozvidka-na-osnovi-vidkrytyh-dzherel/.

3. Дослідження на основі відкритих джерел або OSINT: де використовується та в чому небезпека. URL: https://www.eset.com/ua/about/ newsroom/blog/business-security/issledovaniye-na-osnove-otkrytykh-istochnikov-ili-osint-gde-ispolzuyetsya-i-v-chem-opasnost/?srsltid=AfmBOooDgwrx_gqYYxijkVt2v2vfjD_e.

Назаренко Роман,
старший викладач
*(Національна академія
Служби безпеки України)*

OSINT ЯК ІНСТРУМЕНТ ВЕРИФІКАЦІЇ РЕЛІГІЙНИХ НАРАТИВІВ ПІД ЧАС ВІЙНИ

У сучасному світі військові конфлікти дедалі частіше виходять за межі традиційного збройного протистояння. Вони охоплюють економічну, інформаційну, культурну та навіть релігійну площини, де на ключові ролі, поряд з військовим, - виходить семантичний компонент. Релігійні наративи мають здатність впливати на емоції, мобілізувати громади, підсилювати відчуття спільної ідентичності та приналежності. Проте, при їхній цілеспрямованій інструменталізації, вони можуть провокувати суспільні розколи, конфлікти, а у воєнний час – навіть загрожувати національній безпеці. Саме тому верифікація таких наративів є не лише справою інформаційної гігієни, а й складовою державної безпекової політики. Відтак, верифікація подібних наративів є не лише інформаційним, але й безпековим викликом. В умовах російсько-української війни особливої ваги набуває здатність вчасно розпізнавати і верифікувати інформаційні впливи, пов'язані з релігійною тематикою. Саме тому OSINT (Open Source Intelligence) – розвідка з відкритих джерел – стає важливим аналітичним інструментом у сфері національної безпеки. OSINT – це метод збору, аналізу та перевірки інформації з публічно доступних джерел. Його цінність полягає в тому, що він не потребує доступу до закритих даних, та дозволяє швидко реагувати на інформаційні пастки.

У сучасній війні росії проти України релігійна риторика стала частиною великої пропагандистської кампанії російської Церкви. Ми не раз ставали свідками маніпулятивних та неправдивих свідчень з боку російської пропаганди: «В Україні переслідують на релігійному ґрунті», або ж «УПЦ зазнає утисків від держави», «Мусульман переслідують в Україні» тощо. Ці матеріали розповсюджуються через соціальні мережі, проросійські ЗМІ, псевдорелігійні канали, а іноді – і через формально зареєстровані релігійні організації. Їхня мета – дискредитувати Україну в очах віруючих,

розпалити міжконфесійне напруження та мобілізувати міжнародну підтримку «постраждалих від гонінь». Дискредитація України на міжнародній арені є однією з ключових цілей російської федерації, адже заплямування іміджу та звинувачування у переслідуваннях на релігійному ґрунті може відобразитися на міжнародній економічній та військовій підтримці для нашої України з боку партнерів.

Розглянемо кілька прикладів застосування OSINT для релігійної тематики.

Кейс 1: «Захоплення храму УПЦ у Вінниці»

У 2023 році в проросійських медіа з'явилися повідомлення про «силове захоплення храму канонічної церкви» у Вінниці. OSINT-аналітики встановили, що запропоноване фото, що згадується у матеріалах, не відповідає дійсності, адже було зроблено ще у 2019 році та взяте зі стрічки новин про зовсім інший конфлікт. Ба більше, в соціальних мережах сторінка, що першою поширила фейк, була створена 2 тижні до безпосереднього інциденту та використовувала автоматичний переклад. В офіційних джерелах, до прикладу сайт міської ради, ніякої інформації про інцидент не було. Таким чином, маємо справу з цілеспрямованою інформаційною атакою, спрямованою на загострення релігійної напруги. Даний фейк був створений для мобілізації та актуалізації *протестного* релігійного середовища. Відтак, в країні, де традиційно високий рівень довіри до церковних структур, а більшість населення людей вважають себе релігійними, це може становити суттєву загрозу для національної безпеки України. До прикладу, за результатами дослідження які провів Центр Разумкова [1] близько 68% громадян України вважають себе релігійними. Ба більше, Церкві та релігійним організаціям як таким довіряє тотальна більшість жителів нашої країни.

Кейс 2: «Мусульман переслідують в Україні»

У арабомовному сегменті платформи X (Twitter) активно розповсюджувалися повідомлення про нібито «утиски кримських татар в Україні» з одного боку, та тотальну «заборону ісламу» – з іншого. Був проведений аналіз із використанням інструментів OSINT, що дозволив отримати наступні результати. Зокрема, виділяємо використання геотегів та часових міток, які свідчили, що запропоновані у численних матеріалах російських ЗМІ фото, були зроблені саме на території російської федерації, а не в Україні.

Переклад дописів показав, що мова ботів згенерована автоматично, та не є *живою* мовою. На додаток, повідомлення поширювалися через мережу акаунтів, пов'язаних із сирійськими пропагандистами, що підтримують російську федерацію.

Відтак, у час, коли релігія дедалі частіше стає полем інформаційного впливу, OSINT надає ефективний інструментарій для верифікації фактів, виявлення фейкових наративів та попередження міжконфесійних та міжрелігійних конфліктів. Релігійні наративи мають особливу силу – вони глибоко емоційні, і тому їх складніше деконструювати лише раціональним шляхом чи виключно в наслідок логічного умовиводу чи судження. Відповідно, вкрай необхідною є комплексна аналітична робота, в якій OSINT повинен поєднуватися з розумінням релігійного контексту. В межах даної траєкторії необхідно розвивати спеціалізовані OSINT-команди із залученням належного рівня експертизи фахівців. Важливо впроваджувати моніторинг релігійно забарвлених фейків у загальнонаціональні інформаційні системи безпеки та створювати т.з *інструменти контрнаративу та протидії* зокрема на релігійних платформах та в громадах. Зрештою, захист від релігійної дезінформації – це також захист морального ядра суспільства, яке у воєнний час має залишатися стійким, об'єднаним і свідомим.

---

1. Центр Разумкова. Рівень релігійності, довіра до Церкви, конфесійний розподіл та міжцерковні відносини в українському суспільстві (жовтень 2024р.) // https://razumkov.org.ua/images/2025/01/28/2024-Religiya-religion-FIN.pdf (24.03.2025).

Носов Віталій,
кандидат технічних наук, доцент,
професор кафедри протидії кіберзлочинності
Навчально-наукового інституту № 4
(Харківський національний університет внутрішніх справ)

АРХІТЕКТУРА АВТОМАТИЗОВАНОЇ СИСТЕМИ РОЗШУКУ ЛЮДЕЙ НА ОСНОВІ ВИКОРИСТАННЯ ДАНИХ З ВІДКРИТИХ ДЖЕРЕЛ

За час військової агресії рф на території України було вчинено велику кількість воєнних злочинів особами, які можуть перебувати як поза межами України, та і на окупованих територіях. Велика кількість людей, зокрема, дітей, було депортовано або примусово переміщено, зникло без вісти тощо. Для притягнення до відповідальності воєнних злочинців, знаходження та повернення примусово переміщених і зниклих осіб існує нагальна у розробці автоматизованої системи розшуку людей на основі використання даних з відкритих джерел (АСРЛ-OSINT).

Згідно стандарту інженерії систем і програмних засобів [1] архітектура системи має розглядатись контекстуально (рис. 1).

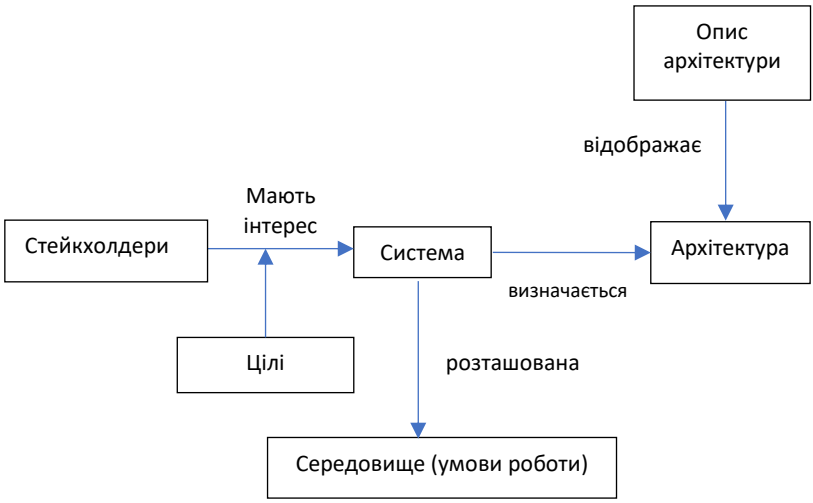


Рис. 1. Контекст опису архітектури системи

Стейкхолдерами АСРЛ-OSINT є:

– територіальні органи, заклади, установи і підприємства, що належать до сфери управління Міністерства внутрішніх справ України як головного органу у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сфері дотримання норм міжнародного гуманітарного права на всій території України (у частині повноважень з координації розшуку осіб, зниклих безвісти за особливих обставин, та вирішення інших пов'язаних з цим питань відповідно до Закону України «Про правовий статус осіб, зниклих безвісти за особливих обставин»);

– адвокатські об'єднання та інші організації, установи та підприємства, що займаються на договірних засадах розшуком зниклих осіб та злочинців.

Метою АСРЛ-OSINT є автоматизація збору та систематизація інформації із відкритих джерел (мережі Інтернет, соціальних мереж, відкритих реєстрів тощо), та отримання на її основі нової інформації з метою виконання завдань з розшуку людей (злочинців, осіб, депортованих або примусово переміщених, зниклих безвісти тощо), в тому числі в умовах протидії військовій агресії.

АСРЛ-OSINT є клієнт-серверною системою, в якій серверна частина фізично може бути розташована як в організації, так і у хмарного провайдера, а захищений клієнтський доступ здійснюється через Інтернет з персональних комп'ютерних пристроїв. Серверна частина має одночасно оброблювати до 100 задач. Механізми захисту забезпечують автентифікацію користувачів, розмежування і керування доступом, шифрування трафіку і критичних даних на сервері, резервне копіювання серверних даних, підтримання своєчасного оновлення системного і прикладного програмного забезпечення.

АСРЛ-OSINT забезпечує:

– пошук інформації у відкритих джерелах на основі запиту, складеного із персональних даних людини та її зображень;

– систематизацію інформації про осіб та події із контролем дублювання;

– контроль, налаштування пошуку та систематизацію даних користувачем.

АСРЛ-OSINT складається із трьох взаємопов'язаних модулів:

– модуль накопичення, аналізу та систематизації даних;

– модуль автоматичного пошуку інформації у відкритих джерелах за вихідними даними;

– модуль розпізнавання обличчя у фото- та відео-матеріалі.

Процес взаємодії модулів відбувається за наступними фазами: «отримання запиту - перевірка наявної в базі даних релятивної до запиту інформації – пошук нової інформації - формування звіту за запитом - коригування користувачем - додавання нової інформації до бази даних - встановлення зв'язків із наявною інформацією».

Логіка зв'язків модулів наступна:

– модуль пошуку використовує модуль розпізнавання для виявлення спільних ознак графічної інформації в запиті і в джерелі інформації;

– модуль систематизації використовує модуль розпізнавання для виявлення спільних ознак графічної інформації в запиті і в наявній в системі інформації;

– модуль систематизації отримує від модуля пошуку релятивну до запиту інформацію, перевіряє наявність схожої інформації в своїй базі даних і позначає потенційно дубльовані одиниці інформації.

Зазначений функціонал АСРЛ-OSINT забезпечується алгоритмами та технологіями штучного інтелекту зокрема:

– машинним навчанням для класифікації, прогнозування та побудови рекомендацій на основі відкритих даних;

– обробкою природної мови (NLP) для аналізу текстових повідомлень та публікацій в Інтернеті;

– комп'ютерним зором для аналізу фотографій та відео з відкритих джерел;

– геопросторовими технологіями для визначення місцезнаходження людини на основі GPS-даних або геотегованих зображень, тощо.

На знайдених фото- і відеоматеріалах за алгоритмами машинного навчання відбувається пошук і розпізнавання обличчя по власній базі розшуку. Штучна нейронна мережа фіксує ознаки, такі як розташування очей, носа, рота та інших ключових точок на обличчі. Ці ознаки допомагають визначити унікальні властивості обличчя і створити цифровий відбиток обличчя, який можна зберігати в базі даних і порівнювати з іншими цифровими відбитками.

Описана архітектура АСРЛ-OSINT може бути реалізована із використанням мови програмування Python, вебфреймворку, векторної бази даних для зберігання та пошуку обличчя, бібліотеки виявлення та розпізнавання обличчя, великої моделі мови (LLaMA).

---

1. ДСТУ ISO/IEC/IEEE 42010:2018 Інженерія систем і програмних засобів. Опис архітектури (ISO/IEC/IEEE 42010:2011, IDT). URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=77960 (дата звернення 28.04.2025).

Остапчук Дарія,
курсантка
(Львівський державний університет
внутрішніх справ)
Науковий керівник:
Ревак Ірина,
доктор економічних наук, професор,
завідувач науково-дослідної лабораторії
OSINT-досліджень та безпекової аналітики
навчально-наукового інституту управління,
психології та безпеки
(Львівський державний університет
внутрішніх справ)

МОНІТОРИНГ І ДОКУМЕНТУВАННЯ ДЕПОРТАЦІЇ УКРАЇНСЬКИХ ДІТЕЙ ДО РОСІЇ ЗА ДОПОМОГОЮ МЕТОДІВ OSINT

У ході збройного конфлікту діти становлять одну з найбільш вразливих категорій населення. Вони продовжують потерпати від численних форм насильства, зокрема вбивств, каліцтв, викрадень, сексуального насильства, вербування до збройних формувань окупантів, а також страждають від ракетних ударів по навчальних закладах та медичних установах як у районах активних бойових дій, так і на тимчасово окупованих територіях України.

Насправді зазначені дії становлять акт збройної агресії, що супроводжувався систематичними та грубими порушеннями норм міжнародного гуманітарного права, Статуту Організації Об'єднаних Націй, а також інших міжнародно-правових актів, включаючи вчинення воєнних злочинів і злочинів проти людяності [1]. У зв'язку із цим на міжнародній арені було порушене питання щодо визнання агресії росії проти України реальним актом геноциду українського народу.

Так, за повідомленням, оприлюдненим 21 квітня 2022 року на вебсайті медіаресурсу «Известия», понад 150 тисяч українських дітей із тимчасово окупованих територій так званих «ЛНР» і «ДНР» було переміщено до рф. У червні 2022 року онлайн-видання «Московский комсомолец» поширило інформацію про оздоровлення дітей з Донбасу в дитячих таборах на території росії. З метою

виявлення закономірностей у висвітленні тематики депортації українських дітей у російських медіа, а також для аналізу можливих взаємозв'язків між цими повідомленнями, було укладено аналітичну таблицю, що дозволяє класифікувати характер поданої інформації. При цьому медіа ресурси були згруповані відповідно до сфери їх діяльності – телебачення, радіомовлення та Інтернет-комунікації [2, с. 9]. Кожне медіа джерело було проаналізовано з урахуванням наявності у ньому інформаційних матеріалів, що:

– виправдовують незаконні дії рф у контексті депортації українських дітей;

– спрямовані на дискредитацію діяльності України та її політичного керівництва, пов'язаної із захистом прав українських дітей у контексті збройної агресії росії;

– мають на меті дискредитацію західних держав, міжнародних партнерів та союзників України, які здійснюють заходи із захисту українських дітей від наслідків воєнних дій.

Результати моніторингу показали, що 17 із 20 проаналізованих медіаресурсів поширювали повідомлення, що містили дискредитаційний характер щодо західних держав та організацій-партнерів України у вказаному контексті. Водночас 10 із 20 медіа демонстрували інформаційну активність за всіма зазначеними напрямами, тобто одночасно виправдовували дії рф, дискредитували Україну та її західних союзників [2].

У контексті збройного конфлікту, що триває, здійснюване рф перевиховання українських дітей слід розглядати не лише як тяжке порушення норм міжнародного права, а й як складову цілеспрямованої політики держави-агресора, спрямованої проти українського народу та його державності.

Депортація українських дітей до росії супроводжується численними грубими порушеннями норм міжнародного гуманітарного та правозахисного права, серед яких:

– відсутність добровільної згоди законних представників (батьків чи опікунів) на переміщення дітей за межі України;

– створення урядом рф умов для спрощеної процедури набуття українськими дітьми російського громадянства;

– ігнорування принципу врахування найкращих інтересів дитини при ухваленні рішень, що стосуються її долі;

– здійснення усиновлення або оформлення інших форм опіки, які забезпечують тривале перебування дітей на території рф;

– створення адміністративно-бюрократичних бар'єрів для українських батьків, що перешкоджають процесу возз'єднання з дітьми;

– застосування тиску, маніпуляцій та погроз із метою схилення батьків до передачі дітей для вивезення в росію;

– організація процесу перевиховання дітей із повним ігноруванням їхніх культурних, мовних та національних потреб, що спричиняє поступове стирання української ідентичності.

З огляду на вищевикладене, можна стверджувати про наявність чітко визначених та документально підтверджених ознак насильницької депортації та примусової асиміляції українських дітей. У цьому зв'язку правомірним і концептуально обґрунтованим є використання терміна «примусова депортація» для кваліфікації відповідних дій рф.

Представники російської владної вертикалі, зокрема чиновники та високопосадовці, виступають активними джерелами наративів і дезінформації, що стосується обставин незаконного переміщення українських дітей на територію рф. Вони здійснюють публічне озвучення відповідних заяв як на національному, так і на міжнародному рівнях – у межах діяльності міжнародних організацій та участі у міжнародних заходах. Така активність свідчить про системну, цілеспрямовану та координовану на найвищому державному рівні кампанію, спрямовану на легітимізацію та ідеологічне обґрунтування депортації українських дітей. До реалізації цієї інформаційної кампанії залучаються також державні та недержавні російські медіа, які стали об'єктом проведеного аналітичного дослідження.

Інформація, що поширюється російськими посадовими особами та засобами масової інформації, здебільшого має ознаки дезінформації, яка у всіх випадках або спрямована на дискредитацію України та її міжнародних партнерів, або слугує засобом виправдання дій рф в контексті депортації українських дітей, або ж поєднує обидва ці підходи. Така інформаційна стратегія формує в російському медійному дискурсі чітку дихотомію «ми–вони», в межах якої «ми» (росія) постає як сторона, що діє морально виправдано та «здійснює благо», тоді як «вони» (Україна та західні дер-

жави) подаються як джерело загрози, носії зла і противники. Застосування подібної опозиційної моделі є характерним для маніпулятивних технологій формування ворожнечі, легітимізації агресії та поширення воєнної пропаганди.

---

1. Радіо Свобода Weekly: Резолюція ООН вимагає від Росії негайно вивести війська з України. URL: https://www.radiosvoboda.org/a/podiyi-tyzhnya-viyna/32289019.html
2. Аналітичний звіт із висвітлення теми депортації українських дітей в російських медіа. URL: https://www.nrada.gov.ua/wp-content/uploads/2023/06/Analiz-deportatsija-ditej.pdf

Печенюк Святослав,
кандидат історичних наук,
головний науковий співробітник наукової лабораторії
(Національна академія Служби безпеки України)
Андрусишин Юлія,
кандидат психологічних наук,
головний науковий співробітник наукової лабораторії
(Національна академія Служби безпеки України)

ПЕРСПЕКТИВИ РОЗВИТКУ СЕРВІСІВ МОНІТОРИНГУ ІНФОРМАЦІЙНОГО ПРОСТОРУ В ІНТЕРЕСАХ ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ БЕЗПЕКИ

Сучасне інформаційне середовище характеризується перманентною генерацією й зростанням обсягів інформації у відкритих джерелах, насамперед в мережі Інтернет – від новинних публікацій та результатів досліджень до контенту у соціальних мережах. Серед останніх здебільшого аудіозаписи та відеоролики, повідомлення й коментарі до них тощо. Такий динамічний та невпинний потік різноманітних відомостей ускладнює процес моніторингу інформаційного поля, необхідного для ідентифікації та відстежування негативних соціальних явищ, протиправної діяльності тощо в інтересах протидії безпековим викликам й загрозам [1].

Моніторинг інформаційного простору може здійснюватися як вручну (з використанням пошукових систем Google, Bing тощо), так і за допомогою спеціалізованого програмного забезпечення. Хоча функціонал пошуковиків дозволяє налаштовувати запит доволі детально і отримувати релевантні результати, такий спосіб пошуку інформації краще підходить для разових завдань, ніж для регулярного OCINT-моніторингу. Для здійснення останнього найбільш оптимальним є використання спеціальних сервісів, що дають змогу автоматизувати частину рутинних процесів.

Нині на ринку представлено безліч різноманітних комерційних моніторингових сервісів [2], що активно використовуються PR-спеціалістами публічних осіб, маркетологами та SMM-фахівцями компаній для відстеження ділової репутації, впізнаваності бренду та взаємодії з аудиторією й клієнтами. Часто до функціоналу таких сервісів крім збирання, сортування і групування повідомлень, входить аналіз тональності тексту, оскільки для бізнесу критично важ-

ливою є робота з негативними відгуками [3]. Групування подібних повідомлень дозволяє знизити час на їх обробку аналітиком, розподіляти за пріоритетом, виявляти тенденції та прогнозувати варіанти розвитку ситуації.

Наявні комерційні моніторингові сервіси пропонують досить широкий набір функцій. Разом з тим, у контексті виконання завдань із забезпечення державної безпеки такий функціонал часто задовільняє не усі умови і потреби щодо відстеження інформаційного простору. Зокрема, наразі дискусійною є результативність семантичного аналізу повідомлення [4], адже визначення її відтінку (позитивний або негативний) має суб'єктивний характер, потребує розуміння контексту та стилю вираження (іронія, сатира, сарказм тощо). Відтак наразі зазначений вид аналізу здійснюється фахівцем-аналітиком. Також не завжди коректними і повними є обсяги охоплення аудиторії. Адже у той час як комерційні моніторингові сервіси фокусуються здебільшого на великих інформаційних майданчиках (загальнонаціональні та регіональні медіа) і рейтингових дописувачах у соцмережах (інфлюенсерах), для протидії та попередження безпекових загроз не менш важливим є відстеження активності у нечисельних локальних й тематичних спільнотах (групах, чатах тощо), які, до того ж, часто можуть бути закритими.

Загалом, функціонал моніторингової системи для задоволення потреб складових сектору безпеки і оборони держави, на відміну від бізнес-орієнтованих продуктів, має забезпечувати можливість виконання таких основних завдань:

здійснювати пошук за ключовими словами та фразами не лише у тексті, а й в аудіо- та відеоматеріалах;

збирати інформацію з груп і каналів у соціальних мережах та месенджерах;

коректно визначати тональність (семантичне забарвлення) повідомлення;

видавати статистичні дані за частотою згадування певних ключових слів чи словосполучень (фраз);

зберігати та архівувати зібрану інформацію.

Пошук інформації в аудіо- та відеоматеріалах сьогодні здійснюється за ключовими словами подібно тому, як і в тексті – після транскрибації мовлення у текст або розпізнавання написів та лого-

типів на розкадрованому відео. Тому поліпшення потребують алгоритми транскрибації аудіо, розпізнавання зображення та перекладу для пошуку різними мовами.

Моніторинг значної кількості малих публічних місцевих груп та тематичних каналів передбачає наявність розвиненої технічної інфраструктури. Доступ до закритих і приватних спільнот, що потенційно можуть становити інтерес у контексті протидії безпековим загрозам, обмежується умовами надання послуг самих соцмереж і месенджерів та правом особи на приватність.

Показники семантичного забарвлення публікацій, що здійснюється за допомогою слів-маркерів із заздалегідь заданих словників, часто є нерелевантними. Відтак, впровадження досконаліших технологій, зокрема на основі штучного інтелекту, могло б покращити результативність визначення тональності повідомлення з урахуванням контексту та художніх прийомів вираження думки автора.

Статистичний аналіз контенту дозволяє вивчати розвиток ситуації в динаміці. Аналіз тональності тексту (як основи мови ворожнечі) разом з визначенням частоти, у тому числі піків, згадувань ключових слів і фраз або публікації повідомлень дає змогу виявляти та відстежувати рівень загроз певним державним установам, об'єктам критичної інфраструктури, окремим особам тощо.

Питання зберігання та архівування зібраного контенту потребує додаткового законодавчого врегулювання, насамперед у контексті дотримання норм авторського права [5]. Водночас його важливість важко переоцінити, адже наявність архіву зібраної інформації, окрім можливості ретроспективного аналізу розвитку ситуації, дасть змогу також достовірно виявляти першоджерела навіть за умови видалення оригінальних публікацій. До того ж, збереження копій повідомлень з дотриманням вимог документування цифрових доказів дозволить використовувати їх як електронні докази в суді згідно із законодавством [6; 7].

Підсумовуючи вищевикладене, слід зазначити, що наявні на сьогодні сервіси моніторингу інформаційного простору дозволяють виконувати широкий спектр завдань – від виявлення окремих фактів протиправної діяльності до прогнозування розвитку важливих соціальних явищ та процесів. Разом з тим, використання таких сервісів у діяльності структур сектору безпеки і оборони

держави потребує вдосконалення окремих їх функцій. Це, насамперед, збільшення обсягу відстежуваних джерел, поліпшення алгоритмів аналізу повідомлень, зокрема їхнього семантичного забарвлення, збереження зібраних матеріалів з метою їхнього подальшого аналізу та забезпечення можливості використання у судовому провадженні. Зазначеному може сприяти імплементація технологій на основі штучного інтелекту з їх подальшим аналізом фахівцем-аналітиком для вироблення конструктивних рекомендацій та прийняття обґрунтованих рішень у контексті протидії безпековим викликам і загрозам.

---

1. Стратегія забезпечення державної безпеки, затверджена і введена в дію Указом Президента України від 16.02.2022 № 56/2022. URL: https://www.president.gov.ua/documents/562022-41377 (дата звернення: 29.04.2025).
2. 10 найкращих сервісів моніторингу згадок у 2022 році. URL: https://prposting.com/uk/blog/23-social-media-monitoring-tools (дата звернення: 30.04.2025).
3. Як соцмережі можуть зіпсувати ваш бізнес. URL: https://www.bbc.com/ukrainian/features-48927222 (дата звернення: 29.04.2025).
4. ШІ в медіамоніторингу: як застосовуємо на практиці. URL: https://cases.media/en/article/shi-v-mediamonitoringu-yak-zastosovuyemo-na-praktici (дата звер-нення: 29.04.2025).
5. Законослухняний контент та авторські права. URL: https://weblana.com.ua/blog-ua/kontent-ta-avtorski-prava (дата звернення: 29.04.2025).
6. Електронно-цифрові докази під час виконання вимог ст. 290 КПК України. URL: https://yur-gazeta.com/dumka-eksperta/elektronnocifrovi-dokazi-pid- chas-vikonannya-vimog-st-290-kpk-ukrayini.html (дата звернення: 30.04.2025).
7. Фіксація змісту веб-сторінки для суду. Електронні докази в суді. URL: https://jurliga.ligazakon.net/analitycs/189715_fksatsya-zmstu-veb-stornki-dlya-sudu-elektronn-dokazi-v-sud (дата звернення: 30.04.2025).

Підхомний Олег,
доктор економічних наук, професор,
професор кафедри фінансів, грошового обігу і кредиту
(Львівський національний університет
імені Івана Франка)

МОЖЛИВОСТІ ВІДКРИТИХ ДЖЕРЕЛ У ДОСЛІДЖЕННІ ВЗАЄМОЗВ'ЯЗКІВ ТОВАРНИХ І ФІНАНСОВИХ ПОТОКІВ

Актуальність дослідження можливостей відкритих джерел у вивченні взаємозв'язків товарних і фінансових потоків обумовлена зростанням масштабів транснаціональних економічних зловживань, зокрема схем ухилення від митного та валютного контролю, обходу санкцій, відмивання коштів через міжнародну торгівлю та криптовалютні інструменти. В умовах глобалізації та цифровізації відкриті джерела інформації – такі як митні бази даних, реєстри компаній, аналітика блокчейн-транзакцій, судові документи та журналістські витоки – надають дослідникам, фінансовим аналітикам і правоохоронцям унікальні інструменти для ідентифікації нетипових або прихованих зв'язків між учасниками товарно-грошових операцій. Це відкриває нові можливості для оцінки ризиків, викриття тіньових схем і зміцнення фінансової безпеки як на національному, так і на міжнародному рівнях.

Для дослідження взаємозв'язків товарних і фінансових потоків за допомогою відкритих джерел необхідна системна робота з різними типами інформаційних ресурсів, що охоплюють як торговельну, так і фінансову складову. Важливу роль відіграють митно-статистичні платформи на кшталт Panjiva, ImportGenius, TradeAtlas, Volza, Seair та UN Comtrade, які дають змогу аналізувати імпортно-експортні операції, ідентифікувати невідповідності у дзеркальній статистиці, виявляти підозрілі контракти та країни-посередники. Доповнюють ці можливості корпоративні реєстри, зокрема OpenCorporates, Offshore Leaks Database, OCCRP Aleph і Sayari Graph, що дають змогу простежити структури власності, зв'язки між компаніями та фіктивними посередниками, виявити бенефіціарів і пов'язаних осіб. Окрему аналітичну вагу мають ресурси фінансового моніторингу, санкційних списків і ризик-індикаторів,

зокрема World-Check, Orbis, OpenSanctions та Dow Jones Risk & Compliance, які допомагають зіставити компанії й осіб зі статусом політично значущих осіб, санкційними обмеженнями чи судовими провадженнями. Для ідентифікації платежів у криптовалютах застосовуються блокчейн-сканери (Etherscan, Blockchair, BTCscan), графові аналітичні платформи (Breadcrumbs) та комерційні сервіси на кшталт Chainalysis або TRM Labs, які дають змогу розкрити ланцюги фінансування товарних схем, обхід санкцій і підозрілі криптотранзакції. Значну роль у верифікації інформації відіграють судові бази (CourtListener, PacerMonitor), журналістські розслідування (OCCRP, ICIJ, Bellingcat), а також архіви витоків (DDoSe-?rets, WikiLeaks). Надзвичайно корисними для географічної візуалізації товарних маршрутів є сервіси відстеження суден (Marin-?Traffic, VesselFinder) та літаків (FlightRadar24, ADS-B Exchange), які дають змогу ідентифікувати фактичне переміщення вантажів, виявляти порти перевантаження, приховані ланки маршрутів і фізичну логістику товарно-фінансових схем. У комплексі ці ресурси створюють потужне інформаційне середовище для викриття непрозорих економічних зв'язків, тіньових фінансових операцій та незаконного переміщення товарів у міжнародному масштабі.

Експортно-імпортні бази даних є ключовим джерелом відкритої інформації для аналізу міжнародних товарних потоків, ідентифікації торгових партнерів, виявлення аномалій у митній статистиці та побудови ланцюгів постачання. Такі платформи, як Panjiva, ImportGenius, ExportGenius, Volza, Zauba та TradeAtlas, надають доступ до вантажних декларацій, описів партій товару, імен експортерів та імпортерів, країн походження, маршрутів суден і обсягів торгівлі. Вони дозволяють зіставляти дані між країнами (наприклад, імпорт однієї країни проти експорту іншої), ідентифікувати схеми подвійного інвойсування, заниження митної вартості, обхід санкцій через країни-посередники та використання офшорних компаній. Завдяки структурованості, відкритому доступу або платній підписці ці бази є важливим інструментом у дослідженнях, що поєднують фінансову аналітику, митний контроль і розслідувальну журналістику.

HS-коди (гармонізована система опису та кодування товарів) є основою для класифікації товарів у міжнародній торгівлі, визначення митних платежів, застосування експортного контролю та

санкцій. Водночас маніпуляції з HS-кодами є поширеним інструментом у схемах обходу митного нагляду, ухилення від сплати податків, маскування санкційних товарів або продукції подвійного призначення. Зміна коду, навмисне застосування неконкретних категорій або перекваліфікація товару у менш контрольовану категорію дає змогу приховати реальну природу поставки. Такі зловживання створюють суттєві ризики для національної безпеки, ускладнюють виявлення санкційних порушень, а також спотворюють статистику зовнішньої торгівлі. Відстеження аномалій стосовно HS-кодів у експортно-імпортних базах та зіставлення їх з відомими характеристиками продукції є одним із ефективних методів виявлення прихованих схем у товарно-фінансових потоках.

Санкційні списки є надзвичайно цінним джерелом структурованих даних, які дають змогу встановлювати зв'язки між фізичними особами, підприємствами, адресами реєстрації, транспортними засобами та криптовалютними гаманцями. Органи, що їх формують – такі як OFAC (США), ЄС, ООН, Канада чи Велика Британія – дедалі частіше включають до переліків не лише імена й назви компаній, а й блокчейн-гаманці (наприклад, Bitcoin, Ethereum). Це відкриває нові можливості для OSINT-досліджень, зокрема для виявлення обхідних схем, непрямих бенефіціарів або гаманців, що використовуються в заборонених транзакціях. Завдяки інтеграції таких даних з відкритими реєстрами, митною статистикою та блокчейн-аналітикою можна повноцінно виявляти мережі взаємозв'язків, що допомагає не лише у виявленні порушень законодавства та санкційних режимів, а й у превентивному моніторингу відповідних ризиків.

Пригунов Павло,
кандидат психологічних наук, професор,
директор Департаменту з питань безпеки, оборони,
діяльності органів юстиції та запобігання корупції
(Секретаріат Кабінету Міністрів)
Франчук Василь,
доктор економічних наук, професор,
старший науковий співробітник
науково-дослідної лабораторії OSINT-досліджень
та безпекової аналітики
навчально-наукового інституту управління,
психології та безпеки
(Львівський державний університет
внутрішніх справ)
Мельник Степан,
доктор економічних наук, професор,
заступник декана факультету № 2
з освітньої та науково-дослідної діяльності
(Львівський державний університет
внутрішніх справ)
Гобела Володимир,
кандидат економічних наук, доцент,
доцент кафедри менеджменту
та економічної безпеки
навчально-наукового інституту управління,
психології та безпеки
(Львівський державний університет
внутрішніх справ)

OSINT В СИСТЕМІ ПРИЙНЯТТЯ БЕЗПЕКОВОГО РІШЕННЯ

Життєдіяльність людини та соціально-економічної системи відбувається в умовах дії тих чи інших загроз, які завдають їм певних збитків (шкоду) у різній формі. Для протидії загрозам людина та інституції приймають безпекові рішення. Прийняття безпекових рішень, це інтелектуальний, психологічний, до певної міри технологічний і водночас складний процес.

Питанням прийняття рішень, особливо управлінських, у наукових дослідженнях приділяється багато уваги, пропонуються різні підходи, етапи, моделі тощо. Центральним у цих дослідженнях є

термін «рішення», яке трактується як «дія», зокрема: «обрання шляху дій після обмірковування, обговорення якогось питання» [1].

Отже прийняття рішення – це «дія», яка має два пов'язаних між собою етапи: етап підготовки варіантів дій (обмірковування, обговорення питання) та етап вибору кінцевого варіанту (обрання шляху дій). Приймати безпекові рішення доцільно на основі суджень, або раціонально, тобто шляхом логічного мислення, а не інтуїтивно, бо шансів на вірний вибір альтернативи невисокі.

У даному дослідженні «прийняття безпекового рішення» розглядається як – діяльність, яка має два пов'язаних між собою етапи: етап підготовки дій та етап вибору кінцевого варіанту дій, спрямованих на створення відповідних можливостей й механізмів, а також безпосереднє попередження, ліквідацію потенційних чи реальних загроз, або відновлення (якщо загроза реалізувалася). Безперечно, що прийняття безпекового рішення супроводжується комунікаційним процесом, де визначальним є цільова інформація про загрози, яка й дозволяє їх виявляти. Способів і технологій збору такої інформації є чимало, серед яких є й OSINT.

Структурну схему прийняття безпекового рішення подано на рис 1.

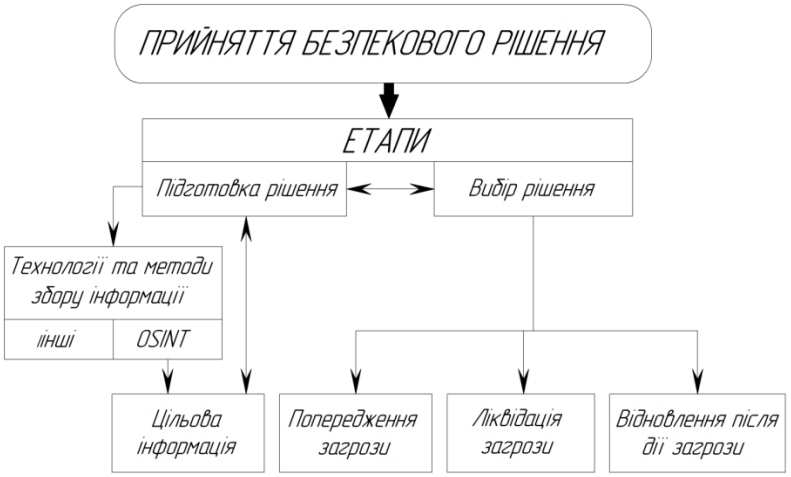


Рис. 1. Структурна схема прийняття безпекового рішення

Джерело: авторська розробка

Безпекове рішення в інституціях приймається відповідними суб'єктами, яким делеговані такі функції та повноваження на підставі інформації, отриманої, зокрема й за результатами використання OSINT.

OSINT дозволяє збирати і аналізувати інформацію про загрози та документувати протиправні дій у відповідному часі та просторі. На підставі цієї інформації приймаються рішення щодо ліквідації чи пом'якшення впливу загроз, а відтак уникнення втрат чи зведення їх до мінімуму.

Використання OSINT-технологій збільшує можливості суб'єктів прийняття безпекових рішень щодо отримання відповідної інформації з відкритих джерел. Проте вичерпного й однозначного визначення поняття «OSINT» також немає, зокрема OSINT це:

- розвідувальна діяльність, яка послуговується інформацією загальнодоступних джерел, яка збирається, використовується та своєчасно надається аудиторії з метою задоволення потреб аналітичної служби [2];

- концепція, методологія і технологічний принцип добування і агрегації військової, політичної, економічної та іншої інформації з відкритих джерел, без порушення законів [3].

У даному дослідженні OSINT розглядається як технологія, оскільки для збору й аналізу інформації використовуються компетенції фахівця, комп'ютери, програми, методи, інструменти тощо, інтегровані в цілісний процес. Тобто OSINT – це технологія, яка інтегративно поєднує інфраструктуру, компетентності, методи та інструментарій, необхідні для здійснення бажаних перетворень в інформації з відкритих джерел для отримання цільової інформації.

OSINT-технології для отримання інформації можна використовувати для протидії різним загрозам. Зокрема, незаконному відмиванню та легалізації грошей отриманих злочинним шляхом, розповсюдженню наркотичних речовин, зброї тощо. Така інформація може використовуватися й використовується для розслідування інтернет-злочинів та переслідування злочинців; для пошуку у соціальних мережах потенційно небезпечних груп та індивідуумів [4]. OSINT-технології використовуються для прийняття безпекових рішень й у сфері безпеки бізнесу, наприклад: для аналізу інформації про компанію; перевірки працівників на дотримання службової

таємниці у соціальних-мережах; індивідуальні перевірки власних співробітників, контрагентів тощо.

Отже використання OSINT як технології для виявлення загроз та прийняття безпекових рішень на державному, регіональному, місцевому рівнях та рівні окремого суб'єкта господарювання дозволяє посилити їх спроможності щодо їх попередження чи ліквідації (припинення). З розвитком цифровізації та діджиталізації OSINT як технологія об'єктивно є одним із основних елементів комунікаційного процесу в системі прийняття безпекового рішення.

---

1. Ачкасова Л. М. Оцінювання ефективності управлінських рішень. *Економіка транспортного комплексу* : збірник наукових праць. Харків : ХНАДУ, 2018. Вип. 23. С. 50–59.
2. U. S. National Intelligence: An Overview 2011. – 54 с. [Електронний ресурс]. – Режим доступу до ресурсу: https://www.hsdl.org/?view&did=697740.
3. Richard A. Best «Open Source Intelligence (OSINT): Issues for Congress, Congressional Research Service» // 2005. – 9 с. [Електронний ресурс]. – Режим доступу до ресурсу: https://fas.org/sgp/crs/intel/RL34270.pdf
4. CYBER INTELLIGENCE by Europol [Електронний ресурс]. – Режим доступу до ресурсу: https://www.europol.europa.eu/activities- 31 services/services-support/intelligence-analysis/cyber-intelligence.

Радейко Роман,
кандидат юридичних наук, доцент,
CEO OnlineLawSchool

ТИПОВІ ПОМИЛКИ OSINT-АНАЛІТИКІВ: АНАЛІЗ ПРОБЛЕМНИХ АСПЕКТІВ МЕТОДОЛОГІЇ ВІДКРИТОГО РОЗВІДУВАННЯ

Сучасний інформаційний простір характеризується експоненційним зростанням обсягів даних, що вимагає від OSINT-аналітиків високого рівня професійної підготовки та методологічної дисципліни. Аналіз практичного досвіду дозволяє виявити десять найбільш критичних помилок, які систематично повторюються у роботі фахівців з відкритого розвідування.

1. Проблема стратегічного планування в OSINT-дослідженнях. Фундаментальною помилкою OSINT-аналітиків є робота без чіткої методологічної стратегії. В умовах інформаційного перевантаження фахівці часто потрапляють у «кролячі нори» – безкінечні потоки інформації, втрачаючи фокус на початковій меті. Ефективна OSINT-стратегія повинна включати чітке визначення цілей дослідження, таксономію релевантних джерел інформації, критерії оцінки достовірності даних, методику документування процесу та процедури верифікації отриманих результатів.

2. Методологічний консерватизм як перешкода ефективності. Закон «золотого молотка» проявляється у схильності аналітиків надмірно покладатися на обмежений набір інструментів, що призводить до неповного охоплення для аналізу доступних даних. Подолання цієї проблеми потребує постійного оновлення арсеналу технологічних інструментів, регулярної практики з новими OSINT-платформами та інструментами, участі у професійних заходах для обміну досвідом та експериментування з нестандартними підходами до збору даних.

3. Проблематика верифікації даних з відкритих джерел. Критичною помилкою є використання інформації без належної перевірки її достовірності. Публічні дані можуть містити неточності, застарілі дані або навмисну дезінформацію. Процес верифікації повинен включати перехресну перевірку інформації як мінімум з двох незалежних джерел, аналіз метаданих для визначення автен-

тичності контенту, оцінку репутації джерел та порівняння з офіційними даними.

4. Контекстуалізація інформації як невід'ємний елемент аналізу. Фрагментарне сприйняття інформації без розуміння її контексту призводить до хибних висновків. Контекстуальний аналіз повинен враховувати культурні та лінгвістичні особливості джерела, часовий контекст публікації, специфіку платформи та можливі мотивації авторів контенту для забезпечення повноцінної інтерпретації даних.

5. Операційна безпека у процесі OSINT-досліджень. Неналежне управління цифровою присутністю аналітика компрометує дослідження. Компоненти ефективної OPSEC включають використання віртуальних машин для ізоляції активностей, ретельне управління IP-адресами та геолокацією, мінімізацію персональної інформації в цифровій діяльності та шифрування чутливих комунікацій для захисту як самого дослідження, так і дослідника.

6. Диверсифікація джерел інформації. Зосередження виключно на популярних соціальних мережах (Facebook, Instagram, TikTok) обмежує глибину аналізу. Важлива інформація часто міститься на спеціалізованих форумах DarkNet, у корпоративних спільнотах та таких платформах як Reddit і Discord. Диверсифікація джерел повинна включати галузеві форуми, архівні веб-ресурси, спеціалізовані пошукові системи та мультилінгвальні джерела для забезпечення глобальної перспективи.

7. Когнітивні упередження в аналітичній діяльності. Людський фактор привносить систематичні помилки у процес аналізу. Найпоширеніші упередження включають: пошук інформації, що підтверджує попередні припущення), упередження доступності (надмірний вплив легкодоступної інформації) та селективний підбір (фокусування на обмеженому підмножині даних).

8. Документування процесу дослідження як запорука відтворюваності результатів. Опущення етапу документації даних призводить до втрати критичної інформації та неможливості відтворити результати. Ефективна документація включає детальне логування всіх дій та пошукових запитів, збереження вихідних джерел з тимчасовими мітками, фіксацію ланцюгів логічних висновків та архівацію веб-сторінок для забезпечення повноцінної відтворюваності дослідження.

9. Управління інформаційним перевантаженням. Експоненційний ріст доступної інформації створює виклик фокусування на релевантних даних. «Параліч аналізу» виникає, коли обсяг інформації перешкоджає прийняттю рішень. Стратегії управління інформацією включають використання таксономій для категоризації даних, впровадження систем пріоритизації, автоматизацію первинної фільтрації та розробку чітких критеріїв релевантності.

10. Технічні обмеження та їх вплив на результати аналізу. Технологічні обмеження платформ, API та інструментів створюють систематичні прогалини у зборі даних. Ключові технічні виклики включають обмеження швидкості API та блокування за IP, часткову індексацію контенту пошуковими системами, зникнення контенту та технічні бар'єри доступу до певних джерел, що потребує комплексних стратегій подолання.

Підвищення якості OSINT-аналізу потребує розробки стандартизованих протоколів для кожного етапу процесу, інвестування в навчання та сертифікацію фахівців, побудови професійних мереж для обміну досвідом, впровадження автоматизації для первинної обробки даних та розвитку критичного мислення для подолання когнітивних упереджень. Ефективність OSINT-аналізу безпосередньо залежить від систематичного підходу до уникнення типових помилок. Розуміння цих помилок та їх системних причин дозволяє аналітикам розвивати більш надійні методології, підвищувати якість розвідувальної інформації та знаходити оптимальний баланс між глибиною аналізу та оперативністю отримання результатів в умовах сучасного інформаційного середовища.

Ревак Ірина,
доктор економічних наук, професор,
завідувач науково-дослідної лабораторії
OSINT-досліджень та безпекової аналітики
навчально-наукового інституту управління,
психології та безпеки
(Львівський державний університет
внутрішніх справ)

КРИТЕРІЇ ПОРІВНЯННЯ РЕЛЕВАНТНОСТІ ТЕМАТИЧНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

В умовах гібридних загроз та інформаційної перенасиченості сучасного інформаційного простору особливої актуальності набуває проблема оцінювання релевантності тематичних інформаційних ресурсів, зокрема в межах OSINT-досліджень. Під час війни, коли оперативність і точність інформації є критично важливими для забезпечення безпеки, виникає об'єктивна потреба у формуванні чітких критеріїв для порівняльного аналізу джерел за їхньою достовірністю, практичною цінністю та швидкістю реагування.

Наукова дискусія щодо релевантності у сфері OSINT стикається з низкою викликів: по-перше, релевантність тут має не лише тематичний, а й функціональний вимір (наскільки джерело придатне для аналітичної розвідки); по-друге, темп змін у цифровому середовищі зумовлює потребу в динамічній переоцінці ресурсів; по-третє, інформаційні ресурси часто мають політичну або пропагандистську забарвленість, що ускладнює оцінювання їхньої об'єктивності.

У процесі аналізу інформаційних джерел важливо забезпечувати збалансований підхід до оцінювання таких потенційно суперечливих характеристик, як актуальність і повнота, відкритість і правова допустимість, структурованість і глибина аналітичного змісту. Особливо це актуально в рамках OSINT-досліджень, коли необхідно порівнювати джерела різної природи – від офіційних державних реєстрів до агрегаторів витоків даних і неформалізованих інформаційних платформ. У такому випадку чітко сформульовані критерії релевантності стають фільтром, що відсіює слабкі або сумнівні джерела і фокусує увагу на тих, які мають найбільшу інформаційну цінність відповідно до поставлених завдань.

Релевантність інформаційного ресурсу може оцінюватися за низкою її видів, що відображають як відповідність змісту запиту, так і значущість інформації для користувача. Інформаційна релевантність визначає, наскільки документ відповідає запиту за фактичним змістом і ключовими термінами, тоді як когнітивна релевантність враховує індивідуальні очікування, досвід і знання користувача. Формальна (логічна) релевантність зосереджується на точному збігові термінів і структур між запитом і документом, що важливо для автоматизованих пошукових систем. Змістовна релевантність базується на експертній оцінці сторінки чи ресурсу і враховує якість контенту у відповідь на конкретний запит. Пертинентна релевантність виходить за межі текстової відповідності, орієнтуючись на відповідність інформації реальним потребам користувача. Додатково важливими є тематична релевантність (відповідність предмету дослідження), часова (актуальність даних), географічна (відповідність локації чи юрисдикції), функціональна (придатність формату чи типу інформації для завдання), а також структурна, правова релевантність та релевантність доступу, які відображають технічну придатність, законність використання та легкість отримання інформації відповідно. Такий системний підхід дає змогу багатовимірно оцінити інформаційне джерело залежно від контексту використання.

Серед критеріїв релевантності варто окреслити такі як відповідність темі дослідження, актуальність, доступність, достовірність, повнота, географічне та часове охоплення, правомірність використання, структурованість тощо.

Так, *відповідність темі дослідження* передбачає оцінку того, наскільки зміст ресурсу безпосередньо стосується предмета аналізу. Такий критерій враховує наявність термінів, понять, фактів і даних, які співвідносяться з основними гіпотезами, цілями або завданнями дослідження. Інформаційний ресурс вважається релевантним тоді, коли він містить змістовні відомості, що безпосередньо сприяють поглибленню розуміння або дослідженню конкретної теми, а не лише частково з нею пов’язані.

Актуальність інформаційного ресурсу прямо залежить від наближеності дати його створення або оновлення до моменту проведення аналізу. Цей показник є особливо чутливим до динаміки предметної сфери: у контексті швидкозмінних тем – таких

як санкційна політика, воєнні конфлікти чи фінансові ринки – інформація стрімко втрачає свою цінність, тоді як у відносно стабільних галузях релевантними можуть залишатися навіть джерела, створені раніше.

Доступність характеризує ступінь зручності та можливості отримання інформації користувачем. Ресурс вважається більш релевантним, якщо він відкритий, не потребує платної підписки, складної авторизації або спеціального програмного забезпечення. Доступність також враховує мовну підтримку, наявність пошуку, стабільність роботи ресурсу та географічні обмеження на доступ.

Достовірність визначає якість джерела з огляду на перевіреність, надійність і можливість верифікації поданої інформації. Найвищу довіру зазвичай викликають офіційні, незалежні або авторитетні ресурси, які надають дані з чітким зазначенням джерела, спираються на первинні документи, експертні оцінки або супроводжуються відповідними посиланнями. У межах дослідницької діяльності особливо важливо уникати використання непідтверджених, анонімних чи потенційно маніпулятивних матеріалів.

Повнота, географічне та часове охоплення описує масштабність і репрезентативність наданої інформації. Повноцінний інформаційний ресурс характеризується охопленням значного часово-просторового спектра: він включає дані, що охоплюють тривалий період (кілька років або десятиліть), а також інформацію з різних регіонів чи юрисдикцій, не обмежуючись локальними або вузько спрямованими вибірками. Такий підхід забезпечує можливість формування цілісного уявлення про досліджуване явище, дозволяє аналізувати його динаміку в часі та здійснювати міжрегіональні порівняння.

Правомірність використання визначає, наскільки законно і етично можна застосовувати дані з ресурсу у публічному аналізі чи дослідженні. Йдеться про дотримання авторського права, регламентів щодо обробки персональних даних, умов публічного доступу та відповідності юрисдикції користувача. Навіть високоякісний ресурс може бути нерелевантним у формальному сенсі, якщо його використання не допускається в аналітичній чи юридичній практиці.

Структурованість вказує на те, наскільки ресурс організований і технічно придатний для аналітичної обробки. Це охоплює наявність чітких полів (дата, об'єкт, країна, сума), можливість експорту даних, доступ до API, візуалізацію зв'язків та фільтрацію. Структуровані джерела значно підвищують ефективність роботи з великими масивами інформації, дозволяють проводити порівняння, крос-аналіз та інтегрувати дані в автоматизовані системи.

Наприклад, у контексті дослідження руху товарів подвійного призначення між країнами такі ресурси як OpenCorporates і Aleph різняться за низкою ключових критеріїв релевантності.

Відповідність темі. Обидві платформи придатні для ідентифікації компаній-учасників ланцюгів постачання, однак Aleph має вищу релевантність завдяки інтеграції з витоками, санкційними списками та журналістськими розслідуваннями.

Актуальність. OpenCorporates частіше оновлюється, зокрема щодо активного статусу компаній у державних реєстрах; Aleph містить статичні документи, але може охоплювати історичні дані й «мережеву пам'ять».

Достовірність. OpenCorporates базується на офіційних реєстрах, тому має формально вищу достовірність; Aleph включає неформальні джерела, що підвищує глибину, але потребує критичної перевірки.

Повнота й охоплення. Aleph ширше покриває офшори, географічну варіативність, зокрема в «сірій зоні» торгівлі; OpenCorporates обмежується зареєстрованими компаніями з понад 140 юрисдикцій.

Правомірність використання. Обидві платформи орієнтовані на легальне використання, але OpenCorporates має чіткіші публічні ліцензії.

Структурованість. OpenCorporates має зрозуміліші API, уніфіковані поля й краще підходить для автоматизованого оброблення; Aleph забезпечує складніші графи зв'язків, але менш стандартизовані дані.

Ще однією важливою відмінністю між OpenCorporates і Aleph є їх інтегрованість з аналітичними інструментами, зокрема Maltego – популярною платформою для побудови графів зв'язків. Aleph має офіційно підтримувану інтеграцію з Maltego через

трансформ-джерело OCCRP Aleph, що дозволяє прямо в середовищі Maltego візуалізувати зв'язки між компаніями, особами, адресами, санкційними об'єктами та витоками даних. Це робить Aleph надзвичайно зручним для мережевого OSINT-аналізу, зокрема при виявленні прихованих постачальників або офшорних структур у ланцюгах постачання товарів подвійного призначення. OpenCorporates також може бути підключений до Maltego через окремі плагіни або API-запити, проте така інтеграція менш глибока й не має стільки типів сутностей і метаданих, як у випадку з Aleph. Таким чином, у питанні структурованої візуалізації ризиків і виявлення складних міждержавних схем, особливо пов'язаних із чутливими або контрольованими товарами, Aleph має перевагу саме через свою розширену інтегрованість з Maltego.

Отже, OpenCorporates ідеально підходить для систематичної фільтрації компаній, тоді як Aleph – для глибокого виявлення нетипових зв'язків, схем прокладок і потенційних ризиків, зокрема у сфері обігу товарів подвійного призначення. Оптимальним є комбіноване використання обох платформ.

Ключовими фактори підвищення ефективності визначення релевантності інформаційних ресурсів, на нашу думку, є:

– спеціалізація на певному виді досліджень;

– готовність періодично проводити пошуково-аналітичні експерименти;

– практика прогнозування певних подій та облік точності цього прогнозування;

– практика прогнозування результатів певних пошукових дій та облік точності цього прогнозування;

– періодичний ретроспективний аналіз власної пошуково-аналітичної діяльності;

– дискусії з носіями альтернативних поглядів на проблематику.

Рибка Дмитро,
доктор філософії,
старший викладач
(Національна академія Служби безпеки України)

БРАУЗЕР DUCKDUCKGO ЯК СКЛАДОВА БЕЗПЕКИ OSINT-ДІЯЛЬНОСТІ

Розвідка з відкритих джерел (OSINT) – це збір інформації з публічно доступних джерел для подальшого використання у різних сферах, таких як правоохоронна діяльність, приватні та медійні розслідування, аналітичні дослідження для маркетингу тощо. OSINT включає в себе аналіз даних з медіа, офіційних документів, публічних записів, Інтернету та інших відкритих платформ.

Під час OSINT досліджень ми повинні, в першу чергу, потурбуватись про власну безпеку. Ця теза стала критично актуальною під час агресії росії проти нашої держави, у тому числі і на полях кіберпростору.

Яким же чином можливо досягти достатнього рівня анонімності і безпеки під час роботи в Інтернеті у т.ч. і під час проведення OSINT-досліджень? Безпека і анонімність забезпечується такими інструментами як Virtual Privat Network (VPN), надійним браузером та віртуальним комп'ютером всередині реального комп'ютера (VM).

Вибір надійного браузера стає перед будь-яким дослідником. З чого ж вибрати? Так, є досить поширені браузери типу CHROME, EDGE, MOZILA. Доля користувачів даних продуктів складає до 90% в залежності від географічних і маркетингових особливостей країни. Однак, на нашу думку, ці браузери гарні лише для повсякденної діяльності типу перегляду новин або пошуку товарів для домашніх улюбленців.

Як інструмент захисту (анонімності і безпеки) ці браузери не підходять або при їх використанні необхідно задіювати певний масив інших допоміжних програмних продуктів.

Добре підходить для OSINT досліджень як елемент безпеки браузер TOR. Однак він має кілька недоліків. Це блокування користувачів в певних країнах і швидкість роботи.

В 2022 році компанія DuckDuckGo, яка раніше була відома своєю пошуковою системою, випустила орієнтований на конфіден-

ційність веб-браузер DuckDuckGo для систем на базі macOS. З 22 червня 2023 року, користувачі Windows, які прагнуть більшої конфіденційності під час перегляду веб-сторінок, можуть застосовувати новий браузер DuckDuckGo у вигляді бета-версії.

Від інших браузерів DuckDuckGo відрізняється тим, що за замовчуванням не збирає і не передає дані користувача третім особам. Розробник повідомляє, що браузер використовує приблизно на 60% менше трафіку порівняно з тим же Google Chrome. Під час входу на будь-який сайт DuckDuckGo заблокує відстеження геолокації, зашифрує більшу частину трафіку, вимкне всі сервіси відстеження і приховає нав'язливу рекламу, а також порожні простори сторінки сайтів, де раніше були рекламні банери. У ньому також є вбудований менеджер паролів. [1]

Браузер має вбудований плеєр Duck Player, який дає змогу дивитися YouTube без реклами. Перед початком перегляду він «вирізає» ролик з сайту і вмонтує його у свою сторінку без трекерів і реклами. Серед інших функцій також є можливість видалення історії натисканням однієї кнопки. Крім того, користувач може приховати свою реальну адресу електронної пошти за допомогою замінника @duck.com.[2]

Для ілюстрації можливостей анонімізації DuckDuckGo проведем діагностичне порівняння браузера Microsoft Edge без застосування Virtual Privat Network та з затосуванням VPN, браузера DuckDuckGo без застосування VPN. У якості Virtual Privat Network використовуємо Proton VPN, а у якості засобу тестування вебсайт https://coveryourtracks.eff.org. [3]

Щодо результатів:

1. Браузер Microsoft Edge без використання будь-яких заходів анонімізації не блокує рекламу, не блокує трекери, передає унікальний цифровий відбиток.
2. У разі застосування спільно з браузером Microsoft Edge віртуальної мережі Proton VPN, останній блокує рекламу та трекери, однак браузер все одно надсилає унікальний цифровий відбиток.
3. У третьому варіанті – а саме використання DuckDuckGo навіть без VPN, були блоковані реклама та трекери, однак унікальний цифровий відбиток був зафіксований засобом тестування.

Які недоліки саме цього браузера?

Цей продукт на ринку досить недовго і говорить поки про його недоліки рано. Деякі інтернет-користувачі сумніваються в його анонімності, оскільки мобільна версія не блокувала деякі трекери компанії Microsoft. Однак, як не дивно, всі негативні відгуки і сумніви звучать лише з російських сайтів. Складається враження, що це піаркомпанія направлена на те, щоб користувачі на теренах рф не використовували цей браузер у зв'язку з неможливістю відстеження "компетентними органами".

Висновок: Коли ви обираєте той чи інший програмний продукт поставте перед собою питання, яку конкретну ціль ви переслідуєте у зв'язку з його використанням. Не існує універсальних засобів від усіх загроз. Певним апаратнимими і програмними продуктами можна досягнути відносної безпеки і анонімності при роботі в мережі, в тому числі і під час OSINT досліджень. Будь-який застосунок, утиліта чи налаштування не зроблять перебування користувача в мережі захищеним і анонімним на 100%. Такі інструменти як надійний браузер мінімізують вашу уразливість. Тому, під час проведення серйозних розслідувань за допомогою методів OSINT радимо використовувати всі доступні нам засоби, а саме: Virtual Privat Network (VPN), надійний браузер та віртуальний комп'ютер всередині реального комп'ютера (VM).

---

1. DuckDuckGo-Вікіпедія веб-сайт. URL: https://uk.wikipedia.org/wiki/DuckDuckGo#cite_note-31 (дата звернення 29.04.2025)
2. Браузер DuckDuckGo із захистом від стеження і реклами вже доступний на Windows веб-сайт. URL: https://root-nation.com/ua/news-ua/it-news-ua/ua-duckduckgo-windows (дата звернення 29.04.2025)
3. A Project of the Electronic Frontier Foundation: веб-сайт. URL: https://coveryourtracks.eff.org (дата звернення 29.04.2025).

Рижков Едуард,
кандидат юридичних наук, професор,
професор кафедри інформаційних технологій
(Дніпровський державний університет внутрішніх справ)

МЕТОДИКА «OSINT+»: СИНЕРГІЯ ВІДКРИТИХ ТА ВІДОМЧИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ У ДІЯЛЬНОСТІ ОПЕРАТИВНИХ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Сучасна правоохоронна діяльність зазнає фундаментальних трансформацій під впливом цифрової революції та експоненційного зростання обсягів загальнодоступної інформації. Глобально спостерігається тенденція до все ширшого використання розвідки на основі відкритих джерел (Open Source Intelligence, OSINT) як невід'ємного інструменту в поліцейській роботі. OSINT дозволяє правоохоронцям ефективніше виявляти, аналізувати та реагувати на злочинні прояви, використовуючи величезний масив даних, що генеруються в Інтернеті, соціальних мережах, публічних реєстрах та інших відкритих платформах.

Водночас Національна поліція України (НПУ) функціонує в унікальному контексті, позначеному викликами пост-реформаційного періоду, адаптацією до нових форм злочинності (включаючи кіберзлочинність та гібридні загрози), а також необхідністю діяти в межах специфічних правових та суспільних очікувань. Це вимагає від НПУ не лише засвоєння передових світових практик, але й розробки власних, адаптованих методик розвідувальної діяльності, що максимально використовують наявні ресурси та

Аналіз практики оперативних підрозділів НПУ свідчить про формування та застосування особливої методики інформаційно-пошукової роботи, яка виходить за межі класичного OSINT. Ця методика характеризується системною інтеграцією даних, отриманих з відкритих джерел, із санкціонованим доступом до спеціалізованих відомчих баз даних обмеженого доступу, зокрема ресурсів Інформаційного порталу Національної поліції та інформаційно-пошукової системи «Філін». Такий підхід дозволяє оперативним працівникам не лише збирати загальнодоступну інформацію, але й оперативно верифікувати її, збагачувати контекстом та поглиблю-

вати аналіз за рахунок використання службових інформаційних масивів.

Для позначення цієї гібридної, синергетичної методики пропонується ввести термін «OSINT+». Важливо підкреслити, що йдеться не про просте паралельне використання різних джерел, а про цілеспрямований процес їх інтеграції та взаємного доповнення в рамках єдиного розвідувального циклу. Запропонована концептуалізація «OSINT+» є, по суті, спробою формалізувати та науково обґрунтувати вже існуючу, хоча, можливо, не завжди чітко артикульовану, оперативно-розшукову практику. Така формалізація є необхідною умовою для її стандартизації, впровадження в навчальний процес, забезпечення належного контролю та правової відповідальності. Розвиток цієї методики, ймовірно, є не лише технологічною еволюцією, а й цілеспрямованою адаптацією до специфічного інформаційного середовища, правових можливостей НПУ та характеру злочинності в Україні, що дозволяє долати обмеження традиційного OSINT та ефективно використовувати унікальні державні повноваження.

Ключовими характеристиками OSINT є легальність доступу до джерел інформації та відкритий (негласний) характер її збору. До основних принципів OSINT належать: чітке визначення інформаційної потреби, планування пошуку, законний збір даних, їх критична обробка та аналіз (включаючи верифікацію), та цільове розповсюдження отриманих розвідувальних продуктів.

У правоохоронній діяльності застосовується широкий спектр методик OSINT, адаптованих до специфіки розслідування злочинів. До них належать: аналіз соціальних мереж (SOCMINT), дослідження веб-сайтів та форумів, пошук у публічних реєстрах та базах даних, аналіз геолокаційних даних, моніторинг подій та новинних потоків, а також, за наявності законних підстав та відповідних повноважень, дослідження ресурсів «темної мережі» (Dark Web). Інструментарій OSINT включає як загальнодоступні пошукові системи та онлайн-сервіси, так і спеціалізоване програмне забезпечення для моніторингу, збору та аналізу даних. Однак вирішальне значення має не стільки володіння конкретними інструментами, скільки аналітичні навички осінтера, його здатність критично оцінювати інформацію та виявляти значущі зв’язки.

OSINT надає правоохоронцям цінні можливості для: ідентифікації підозрюваних, свідків або потерпілих; встановлення місцезнаходження розшукуваних осіб або осіб, зниклих безвісти; виявлення та картування злочинних мереж та зв'язків; збору попередньої або допоміжної доказової інформації; вивчення способу вчинення злочинів (modus operandi); моніторингу суспільно значущих подій та потенційних загроз.

Водночас, використання OSINT у правоохоронній діяльності має суттєві обмеження. До них належать: інформаційне перевантаження та складність обробки великих масивів даних; поширеність дезінформації, фейків та маніпуляцій у відкритих джерелах; минливість цифрової інформації (можливість видалення або зміни); складність визначення достовірності інформації відносно конкретної особи.

Саме ці обмеження підкреслюють важливий аспект: хоча OSINT використовує публічно доступні дані, сам процес та мета їх збору правоохоронними органами регулюються спеціальним законодавством (наприклад, Законом України «Про Національну поліцію», Кримінальним процесуальним кодексом України), що накладає значно суворіші правові рамки порівняно з використанням OSINT журналістами чи іншими осінтерами. Систематичний збір навіть відкритої інформації з метою розслідування може вимагати дотримання принципів необхідності та пропорційності, що не завжди є релевантним для інших суб'єктів. Ця специфіка вказує на потенційну цінність інтеграції OSINT із законним доступом до непублічних, але більш надійних відомчих даних, як це передбачає концепція «OSINT+».

Крім того, у поліцейській практиці OSINT рідко виступає як самодостатній інструмент. Значно частіше він слугує або відправною точкою для генерування первинних оперативно-розшукових версій та пошукових ознак, які потребують подальшої перевірки іншими засобами (включаючи запити до відомчих баз даних), або ж як допоміжний засіб для підтвердження чи спростування інформації, отриманої з традиційних джерел (наприклад, показів свідків, результатів негласних слідчих (розшукових) дій). Ця подвійна роль OSINT – як ініціатора та як верифікатора – логічно зумовлює потребу в його тісній інтеграції з іншими інформаційними ресурсами поліції, що й реалізується в рамках методики «OSINT+».

Оперативні підрозділи кримінальної поліції НПУ виконують ключові завдання, пов'язані з попередженням, виявленням, припиненням та розкриттям кримінальних правопорушень, розшуком осіб, які переховуються від органів досудового розслідування, суду або ухиляються від відбування кримінального покарання, та осіб, зниклих безвісти, а також здійсненням оперативного супроводу кримінального провадження. Ефективне виконання цих функцій неможливе без своєчасного доступу до повної, достовірної та релевантної інформації про осіб, події, об'єкти та зв'язки, що становлять оперативний інтерес.

Інформаційний портал НПУ є інтегрованою інформаційно-комунікаційною системою, що забезпечує авторизованим користувачам доступ до різноманітних відомчих баз даних та обліків.

На відміну від Інформаційного порталу, система «Філін» має більш спеціалізоване призначення та вищий рівень обмеження доступу («обмеженим грифом користування»). Вона адмініструється Департаментом кримінального аналізу НПУ та його територіальними підрозділами і використовується переважно в інтересах оперативно-розшукової діяльності (ОРД) та кримінального аналізу. Ця система є потужним інструментом для поглибленого аналізу кримінальних зв'язків, виявлення латентних злочинів та підтримки складних оперативно-розшукових заходів.

Існування двох рівнів доступу до інформаційних ресурсів – загальнодоступного в межах поліцейських повноважень (Інформаційний портал) та спеціалізованого, пов'язаного з ОРД («Філін») – свідчить про свідоме структурування інформаційних потоків залежно від чутливості даних та правового режиму їх використання. Це означає, що методика «OSINT+» повинна враховувати ці рівні, і перехід від використання відкритих джерел до запитів у Портал чи, тим більше, до системи «Філін» має відбуватися за наявності відповідних правових підстав та з дотриманням встановлених процедур.

Ключова перевага внутрішніх баз даних порівняно з OSINT полягає в тому, що вони надають офіційну, структуровану та історично накопичену інформацію, яка часто відсутня або є недостовірною у відкритих джерелах. Можливість перевірити дані, отримані з OSINT (наприклад, ймовірне ім'я особи, пов'язаної з певним нікнеймом), за офіційними поліцейськими обліками (наявність судимостей, статус розшуку, реєстрація транспортних засобів тощо)

дозволяє швидко верифікувати інформацію, надати їй необхідний контекст та значно підвищити її надійність та операційну цінність. Саме ця можливість валідації та збагачення даних є одним з головних рушіїв синергії в рамках «OSINT+».

Враховуючи вищезазначене, пропонується наступне формальне визначення: **«OSINT+» – це інтегрована інформаційно-аналітична методика, що застосовується уповноваженими працівниками Національної поліції (правоохоронних органів) України та характеризується системним, цілеспрямованим та юридично обґрунтованим поєднанням розвідувальної інформації, отриманої з відкритих джерел (OSINT), з даними, доступ до яких надається через спеціалізовані відомчі інформаційні системи обмеженого доступу (зокрема, Інформаційний портал НПУ та систему «Філін») з метою виконання оперативно-службових завдань.**

Ключовим у цьому визначенні є поняття «інтеграція» або «фузія» (fusion). «OSINT+» – це не просто послідовне звернення до різних типів джерел, а ітеративний процес, де результати аналізу даних з одного типу джерела (наприклад, OSINT) стають підставою для цільового пошуку в іншому (наприклад, відомчій базі даних), а отримані там відомості, у свою чергу, можуть спрямовувати подальший пошук у відкритих джерелах.

Робочий процес в рамках «OSINT+» на рівні тактики може розвиватися у двох основних напрямках:

1. **Від OSINT до внутрішніх баз даних.** У цьому випадку інформація, виявлена у відкритих джерелах (наприклад, нікнейм користувача в соціальній мережі, номер телефону з онлайн-оголошення, фотографія з місця події), стає підставою для перевірки за Інформаційним порталом або системою «Філін» з метою ідентифікації особи, встановлення її зв’язків, перевірки на причетність до правопорушень тощо.

2. **Від внутрішніх баз даних до OSINT.** Такий підхід реалізується коли відомості, отримані з відомчих систем (наприклад, встановлене коло спілкування розшукуваної особи з даних «Філін», відомості про транспортний засіб, що використовувався під час вчинення злочину, з Порталу), використовуються для цілеспрямованого пошуку додаткової інформації у відкритих джерелах (пошук

профілів у соцмережах, аналіз онлайн-активності, геолокаційний пошук тощо).

Цей процес вимагає від оперативного працівника не лише технічних навичок роботи з різними джерелами, але й аналітичного мислення, здатності критично оцінювати достовірність та релевантність даних, зіставляти фрагментарну інформацію та формулювати обґрунтовані гіпотези для подальшої перевірки.

Інтеграція OSINT та відомчих баз даних у рамках методики «OSINT+» забезпечує низку суттєвих переваг:

- можливість швидкої верифікації даних з відкритих джерел за офіційними обліками значно економить час та ресурси;
- поєднання даних дозволяє точніше встановлювати особи підозрюваних, свідків, потерпілих, а також виявляти їхні приховані зв'язки;
- інтегрований аналіз допомагає виявляти структуру та учасників організованих злочинних груп;
- комплексний підхід дозволяє отримати більш повне уявлення про події, осіб та обставини, що становлять оперативний інтерес;
- відомчі бази даних допомагають заповнити прогалини та подолати обмеження OSINT (анонімність, недостовірність), тоді як OSINT може надати актуальну інформацію, яка ще не потрапила до офіційних обліків;
- інформація з OSINT, підтверджена даними з офіційних джерел, може набути більшої ваги в процесі доказування (за умови дотримання процесуальних норм).

Ефективне застосування «OSINT+» вимагає від осінтерів (оперативників, аналітиків) не лише технічних навичок роботи з OSINT-інструментами та відомчими базами даних, але й специфічних компетенцій у сфері інформаційної інтеграції. Це включає здатність критично оцінювати надійність джерел, виявляти потенційні упередження, корелювати розрізнені фрагменти інформації, синтезувати дані з різних джерел (з урахуванням їх правового статусу та рівня чутливості) та формулювати обґрунтовані висновки. Це окремий набір аналітичних навичок, який виходить за межі простого володіння інструментами.

За умови неухильного дотримання правових рамок, принципів та процедур, методика «OSINT+» може розглядатися як науково обґрунтований та легітимний інструмент підвищення ефектив-

ності оперативно-службової діяльності Національної поліції України. Вона дозволяє максимально використовувати потенціал як відкритих, так і відомчих інформаційних ресурсів для виконання завдань правоохоронної діяльності.

Складність методики «OSINT+», її міждисциплінарний характер (поєднання технічних, аналітичних та правових знань), високий рівень правової чутливості та потенційні ризики зловживань зумовлюють нагальну потребу у впровадженні спеціалізованого, формалізованого навчання для працівників НПУ. Існуючі навчальні програми можуть містити окремі модулі з основ OSINT або правил роботи з відомчими базами даних, однак вони, як правило, не розглядають ці компоненти в їх інтегрованому взаємозв'язку та не фокусуються на специфічних викликах та методології їхньої інтеграції.

Ефективне навчання «OSINT+» має виходити за межі передачі технічних знань про інструменти та процедури доступу. Його ключовим завданням є культивування професійного судження – здатності оперативного працівника в кожній конкретній ситуації оцінити необхідність, пропорційність та законність переходу від відкритих джерел до закритих баз даних, критично інтерпретувати отриману інтегровану інформацію та приймати обґрунтовані рішення. Це вимагає використання інтерактивних методів навчання, таких як аналіз ситуаційних завдань, рольові ігри та обговорення нестандартних проблемних ситуацій, що сприяють розвитку аналітичного мислення та креативності.

Навчання методиці «OSINT+» є актуальним як для курсантів закладів вищої освіти МВС, так і для діючих оперативних працівників НПУ. Курсанти потребують отримання фундаментальних знань та навичок з «OSINT+» як невід'ємної частини сучасної професійної підготовки ще до початку служби в практичних підрозділах. Це дозволить їм з перших днів роботи ефективно та законно використовувати інтегровані методи збору інформації. Діючі працівники потребують періодичного підвищення кваліфікації для оновлення знань про нові інструменти та методики, адаптації до змін у законодавстві та технологіях, а також для корекції можливих неформальних практик, що могли сформуватися раніше та не відповідають сучасним вимогам законності та ефективності.

Впровадження формалізованого навчання «OSINT+» сприятиме не лише підвищенню індивідуальної майстерності працівни-

ків, але й інституціоналізації цієї методики в рамках оперативно-розшукової доктрини НПУ та інших правохоронних органів. Чітко визначений навчальний курс накшталт існуючого “Пошук інформації з відкритих джерел (OSINT) працівниками кримінальної поліції” з доопрацьованим змістом може сигналізувати про офіційне визнання та стандартизацію «OSINT+», переводячи її зі сфери неформальних знань та навичок окремих працівників у розряд базових компетенцій, необхідних для ефективної роботи в сучасних умовах. Це, у свою чергу, створює підґрунтя для подальшого вдосконалення методики на основі аналізу практики та зворотного зв’язку з навчального процесу.

На підставі викладеного можимо зробити наступні висновки.

Фактично існує та активно застосовується в практиці оперативних підрозділів Національної поліції України специфічна методика інформаційно-пошукової роботи, яку запропоновано позначати терміном «OSINT+». Ця методика характеризується системною інтеграцією розвідки на основі відкритих джерел (OSINT) із санкціонованим використанням інформації зі спеціалізованих відомчих баз даних обмеженого доступу (Інформаційний портал НПУ, система «Філін»).

Проведений аналіз показав, що «OSINT+» має значні синергетичні переваги, дозволяючи прискорити процес розкриття та розслідування злочинів, підвищити ефективність ідентифікації осіб та виявлення зв’язків, покращити ситуаційну обізнаність та частково подолати обмеження, властиві «чистому» OSINT.

Методика «OSINT+» є не просто технічним чи технологічним нововведенням, а важливою адаптацією правоохоронної діяльності до реалій цифрової епохи. Вона являє собою критично важливу спроможність НПУ ефективно та законно протидіяти сучасним формам злочинності, які все частіше залишають сліди як у відкритому кіберпросторі, так і у відомчих інформаційних системах. Визнання, формалізація та подальше вдосконалення цієї методики є необхідною умовою для підтримання операційної ефективності Національної поліції.

Свиридюк Наталія,
доктор юридичних наук, професор
(Одеський державний університет
внутрішніх справ)

OSINT В УМОВАХ ВОЄННОГО СТАНУ

Упродовж останніх десятиліть розвиток цифрових технологій суттєво трансформував як характер міжнародних конфліктів, так і форми впливу на безпеку держав. Зростання відкритості суспільств, розширення доступу до інформаційних ресурсів, а також глобалізація обміну даними призвели до формування нової аналітичної парадигми, в якій відкриті джерела інформації набули ключового значення. У цьому контексті особливого значення набуває OSINT (*Open Source Intelligence*) – розвідка з відкритих джерел, що набула не лише військового та стратегічного, але й політичного, соціального й правового виміру.

OSINT – це метод отримання, аналізу й інтерпретації інформації з відкритих джерел, що доступні без спеціального дозволу або засобів технічного збору. Йдеться про такі джерела, як вебсайти, соціальні мережі, форуми, відеоплатформи, бази даних, наукові публікації, державні реєстри, супутникові знімки тощо. На відміну від традиційних форм розвідки (наприклад, HUMINT – агентурної або SIGINT – технічної), OSINT базується на публічно доступній інформації, що дозволяє використовувати її не лише державним органам, а й громадському сектору, журналістам, дослідникам, правоохоронним структурам, військовим, волонтерам і навіть приватним особам.

У контексті воєнного стану роль OSINT (відкритої розвідки) стрімко зростає. Завдяки відкритим джерелам вдається оперативно отримувати інформацію про переміщення військових сил, логістичні процеси, морально-психологічний стан як цивільного населення, так і військових, масштаби руйнувань інфраструктури, гуманітарні потреби та інші важливі аспекти. При цьому вона не вимагає значних фінансових витрат чи складних технічних засобів, а спирається на аналітичні здібності, критичне мислення та системний підхід. Під час війни в Україні OSINT став джерелом численних виявлень воєнних злочинів, верифікації атак, встановлення маршрутів колон, виявлення дезінформаційних кампаній тощо.

Разом з тим, активне використання відкритих джерел в умовах війни несе серйозні виклики для інформаційної безпеки. Дані, що здаються невинними (наприклад, фото з геолокацією чи дописи у соцмережах), можуть розкривати стратегічно важливу інформацію: точне розташування військових підрозділів, маршрути постачання, стан об'єктів критичної інфраструктури. Більше того, ворог також активно використовує OSINT для ведення гібридної війни – зокрема, для виявлення вразливостей, підготовки інформаційно-психологічних операцій, поширення фейків і розпалювання паніки серед населення.

Особливість OSINT полягає у його двоспрямованості: з одного боку, це потужний інструмент забезпечення відкритості, контролю та ефективності, а з іншого – можливе джерело витоку конфіденційної інформації. У цьому сенсі особливу роль відіграє держава, яка відповідає як за формування нормативно-правової бази, так і за координацію міжвідомчої взаємодії, формування культури інформаційної безпеки серед населення та підтримку технічної спроможності аналітичних структур.

Окрему увагу слід приділяти юридичному та етичному вимірам OSINT. В умовах війни виникає конфлікт між правом на доступ до інформації та необхідністю забезпечення безпеки. У багатьох випадках журналісти, волонтери або активісти, маючи добрі наміри, можуть публікувати матеріали, які можуть стати інструментом у руках ворога. Так само, правові межі використання даних з відкритих джерел не завжди чітко визначені, особливо в умовах надзвичайного стану. Питання конфіденційності, приватності, авторських прав і захисту персональних даних залишаються в центрі уваги і потребують правового осмислення.

Водночас OSINT відкриває унікальні можливості для громадського контролю, правозахисної діяльності та документування правопорушень. Під час війни в Україні активісти, дослідники та правозахисні організації використовують відкриті джерела для документування знищення цивільної інфраструктури, верифікації ударів по мирному населенню, виявлення воєнних злочинців. Такі докази визнаються судами, у тому числі міжнародними, і можуть відігравати критичну роль у майбутніх процесах притягнення до відповідальності.

Окремо варто відзначити роль громадян у створенні OSINT-контенту. У сучасному світі практично кожен користувач мобільного пристрою стає потенційним джерелом інформації (відео з місця подій, фото пошкодженої техніки, коментар у Telegram-каналі можуть мати стратегічне значення). Це підкреслює потребу в масовому навчанні інформаційній гігієні та відповідальності, особливо у прифронтових регіонах.

Не менш важливою є інтеграція OSINT у систему національної безпеки та кіберзахисту. Розвідка з відкритих джерел не повинна існувати ізольовано. Вона має бути частиною загальної системи ситуаційного аналізу, оперативного реагування, інформаційного прогнозування. Для цього необхідна міжвідомча координація, розвиток аналітичних центрів, залучення фахівців з IT, соціології, лінгвістики, криміналістики та права. Успішні приклади вже існують, зокрема в ЗСУ, СБУ, кіберполіції, а також у міжнародних партнерів України.

Таким чином, об'єктивна потреба аналізу OSINT в умовах воєнного стану випливає з поєднання трьох чинників:

1. Стратегічна цінність відкритої інформації для державного та громадського секторів.
2. Зростаючі загрози, які пов'язані з неконтрольованим поширенням чутливих даних.
3. Необхідність розробки збалансованої політики, яка забезпечить ефективність і безпеку.

У контексті гібридної війни, коли інформаційний фронт стає не менш важливим за фізичний, OSINT потребує системного осмислення не лише як технічного засобу, а як багатовимірного соціально-політичного феномену.

Водночас OSINT є об'єктивно необхідним інструментом для оперативного реагування на загрози, стратегічного планування та підтримки інформаційної безпеки. Висока динаміка бойових дій, значна кількість цифрового контенту з місць подій, а також потреба у верифікації великого обсягу інформації в режимі реального часу вимагають системного збору, перевірки та інтерпретації даних з відкритих джерел. Без такого аналізу втрачається можливість ефективно орієнтуватися в інформаційному середовищі, що напряму впливає на безпеку держави, армії та цивільного населення.

Тож, у сучасних умовах OSINT виступає не лише важливим інструментом для посилення відкритості, контролю та ефективності управлінських процесів, а й водночас створює виклики, пов'язані з безпекою інформації. Саме тому держава відіграє ключову роль у врегулюванні цього балансу: шляхом нормативного регулювання, міжвідомчої координації, формування культури обережного поводження з інформацією серед громадян та забезпечення технічної спроможності аналітичних структур. Ефективне поєднання цих елементів є необхідною умовою для повноцінного використання потенціалу відкритої розвідки.

З огляду на це, OSINT в умовах воєнного стану є обґрунтованою та нагальною потребою, що випливає з його стратегічної цінності, зростаючих інформаційних загроз і необхідності державного регулювання. Як багатовимірний феномен, OSINT потребує системного осмислення, міждисциплінарного підходу та інституційного забезпечення для ефективного використання його потенціалу в інтересах національної безпеки.

Сівак Андрій,
аспірант кафедри міжнародного права
та галузевих правових дисциплін
Національної академії наук України
(Київський університет права НАН України)

ПУБЛІЧНІ ІНФОРМАЦІЙНІ ДЖЕРЕЛА ЯК ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ: РОЛЬ OSINT У СУЧАСНОМУ ДЕРЖАВНОМУ УПРАВЛІННІ

У сучасному інформаційному суспільстві інформація перетворюється на стратегічний ресурс, здатний впливати на безпекові, політичні та економічні процеси як на національному, так і на глобальному рівнях. Своєчасний і точний аналіз публічно доступної інформації – один із ключових інструментів реагування держави на актуальні загрози. Розвідка на основі відкритих джерел (OSINT) набуває дедалі більшої ваги як в аналітичному, так і в оперативному забезпеченні державної безпеки.

Open Source Intelligence (OSINT) – це процес систематичного збору, аналізу та інтерпретації інформації, яка є публічно доступною та законною для використання. Джерела OSINT охоплюють широкий спектр платформ і форматів, включаючи:

- цифрові ресурси (веб-сайти, форуми, блоги, соціальні мережі, відеоплатформи);
- класичні ЗМІ (газети, телебачення, радіо);
- державні та міжнародні документи (законодавчі акти, звіти, публічні реєстри);
- наукові й аналітичні матеріали (дослідження, конференції, наукові журнали) [1].

На українському інтелектуальному та аналітичному полі термін «OSINT» почав активно використовуватись із початком збройної агресії Росії проти України. Завдяки доступності цифрових інструментів, волонтерські ініціативи, журналісти-розслідувачі та неурядові організації змогли ефективно використовувати відкриті дані для виявлення ворожої активності, фіксації воєнних злочинів та протидії дезінформаційним кампаніям [2].

Ефективне використання OSINT залежить від наявності та правильного застосування відповідних технологій. Серед них:

- Пошукові системи: Google, Bing, DuckDuckGo дозволяють здійснювати глибокий контекстуальний пошук.
- Соціальні мережі: Facebook, X (Twitter), Telegram, TikTok є джерелами значного обсягу неструктурованої, але надзвичайно цінної інформації.
- Геоінформаційні системи (GIS): Google Maps, OpenStreetMap сприяють просторовому аналізу та геолокації подій.
- Бази даних: відкриті реєстри, зокрема ЄДРПОУ, можуть надавати важливу інформацію про юридичні особи та їх зв'язки.
- Архіви веб-сайтів: Wayback Machine дає можливість відстежити зміни в інтернет-контенті з часом.
- Інструменти аналізу OSINT: Maltego, SpiderFoot, Shodan, TheHarvester дозволяють автоматизувати обробку великих обсягів даних [3][4].

Особливої уваги заслуговує гібридний підхід, за якого OSINT інтегрується з методами HUMINT (розвідка через особисті контакти) чи SIGINT (перехоплення електронних сигналів) у межах комплексного аналізу безпекових ризиків.

Низка зарубіжних держав вже впровадила підрозділи OSINT в структури своїх правоохоронних і розвідувальних органів. Зокрема, таку практику мають Scotland Yard OSINT Unit, Royal Canadian Mounted Police OSINT Division, а також OSINT-підрозділи в структурах поліції Нью-Йорка і Лос-Анджелеса. До аналогічної діяльності залучені аналітичні служби, такі як BBC Monitoring у Великій Британії, ізраїльський Хатсав та австралійське Національне управління оцінки [5].

В Україні аналіз відкритих джерел уже має певну законодавчу базу. Конституція України (ст. 34) гарантує свободу збирання і поширення інформації. У кримінальному процесі відповідні механізми передбачені главою 21 КПК України, зокрема під час зняття інформації з електронних джерел у межах негласних слідчих дій [5].

У сучасних умовах стрімкої цифровізації та інформаційних загроз розвідка на основі відкритих джерел (OSINT) відіграє критично важливу роль у системі забезпечення національної безпеки. Вона поєднує гнучкість, доступність та ефективність у зборі релевантної інформації з публічних джерел, що дозволяє використовувати її як у стратегічному плануванні, так і в оперативній діяльності.

OSINT охоплює широкий спектр технологічних інструментів, джерел і методів, які можна застосовувати як державними структурами, так і недержавними суб'єктами – журналістами, громадськими організаціями, дослідницькими центрами. Зокрема, на тлі російсько-української війни, OSINT довів свою ефективність у документуванні воєнних злочинів, протидії дезінформації, виявленні ворожих позицій та ідентифікації загроз.

Разом з тим, використання OSINT супроводжується низкою викликів – від складності роботи з великими обсягами даних і проблеми достовірності джерел до юридичних обмежень і ризиків втручання в приватне життя. Застосування цих інструментів потребує високої кваліфікації, дотримання правових норм та етичної обережності.

Подальше впровадження OSINT у державну безпекову політику доцільно здійснювати через інституційне оформлення відповідних підрозділів, вдосконалення нормативної бази, розвиток технічної інфраструктури й освітніх програм для аналітиків. Лише за умов поєднання технологічної підготовки, правової грамотності та етичної відповідальності OSINT може стати справжнім інструментом підвищення безпекового потенціалу держави.

Таким чином, розвідка з відкритих джерел є не лише функціональним інструментом у сфері безпеки, а й важливим елементом демократичного суспільства, який дозволяє забезпечити прозорість, відповідальність і стійкість у протистоянні сучасним загрозам.

---

1. Курс «OSINT – розвідка з відкритих джерел та інформаційна безпека» на платформі Prometheus: https://prometheus.org.ua/prometheus-free/osint-open-source-intelligence/

2. Технології OSINT: як відкриті джерела допомагають медійникам https://pressassociation.org.ua/ua/tehnologiї-osint-yak-vidkriti-dzherela-dopomagayut-medijnikam/

3. Стаття «Онлайн-безпека: як використати OSINT на користь Україні» на сайті IT Arena: https://itarena.ua/ua/onlajn-bezpeka-yak-vykorystaty-osint-na-koryst-ukrayini/

4. Стаття «ДОСЛІДЖЕННЯ ТЕХНОЛОГІЇ ВИКОРИСТАННЯ OSINT ЯК НОВОЇ ЗАГРОЗИ З ДЕАНОНІМІЗАЦІЇ ОСОБИ В ІНТЕРНЕТ ПРОСТОРІ» у збірнику наукових праць «Кібербезпека: освіта, наука, практика»: https://csecurity.kubg.edu.ua/index.php/journal/article/view/647

5. Жарков Я.М., Васильєва А.О. Наукові підходи щодо визначення суті розвідки з відкритих джерел. // Вісник Київського національного університету імені Тараса Шевченка. 2013. Вип.30, с.38-41.

Сорочинський Олександр,
здобувач вищої освіти
(Національна академія Служби безпеки України)

ВИКОРИСТАННЯ OSINT У ПРОТИДІЇ ОКРЕМИМ ЗАГРОЗАМ З БОКУ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ

В умовах повномасштабного вторгнення рф в Україну питання інформаційної безпеки має стратегічну важливість. росія веде масштабну гібридну війну, поєднуючи традиційні воєнні дії з кібер та інформаційними атаками. У цьому контексті розвідка відкритих джерел (далі – OSINT) набуває надзвичайно важливого значення, тому що абсолютна більшість сучасних розвідданих надходить саме з відкритих джерел. Технологія OSINT «прорвала інформаційний туман війни» та допомогла виявити «кричущі факти» злочинів, скоєних росією проти України. Тому є дійсно важливим показати, як OSINT застосовується для протидії різним видам загроз з боку рф: інформаційний операціям, виявленню воєнних і кримінальних злочинів.

росія проводить цілеспрямовані інформаційні кампанії, спрямовані на дискредитацію України та деморалізацію українського суспільства. За даними Meta, російські спецслужби організували «розгалужену мережу дезінформації» з сотнями фейкових акаунтів та десятками підробних новинних сайтів, які поширюють кремлівські наративи про війну. Зокрема, було імітовано понад 60 сайтів під виглядом BBC, Guardian чи Der Spiegel, а через фейкові акаунти та ботоферми в Facebook/Instagram рф одночасно транслювала вигадані «новини» наприклад, фейкові матеріали про «Бучу» як постановку України. Більше 1 600 таких акаунтів виявили аналітики Meta – саме вони розповсюджували проросійські пости і ролики серед аудиторії Європи та України [1].

OSINT-спільнота активно протидіє цим операціям. Завдяки OSINT-розслідуванням спростовуються міфи Кремля – наративи про «український геноцид», «американські біолабораторії» тощо – та формуються об’єктивні висновки. Наприклад, українські аналітики як Центр протидії дезінформації, StopFake, InformNapalm системно моніторять месенджери й соцмережі, ідентифікуючи

ботів, які розповсюджують кремлівські фейки. Таким чином OSINT-дослідники знаходять і публікують докази того, що звинувачення на адресу України є сфабрикованими, а також фіксують прямі порушення з боку рф. Активне використання відкритих даних і платформи медіакомунікацій дозволило Україні значно посилити власну позицію: наприклад, масштабні мережі російської пропаганди були виявлені й локалізовані завдяки OSINT-аналізу активності в Telegram, Facebook, Twitter тощо [2].

OSINT є надважливим у військовій сфері: як у розумінні втрат ворога, так і у фіксації воєнних злочинів. Прикладом є проєкт Eyes on Russia, який зі зрозумілих відкритих даних як супутникові знімки, фото, відео та повідомлення в соцмережах задокументував понад 23 000 випадків руйнувань цивільної інфраструктури, загибелі мирних жителів та інших порушень прав людини. Аналітики цієї групи використовують техніки геолокації і хронометрації, щоби верифікувати фото та відеодокази, та поєднують їх з офіційними звітами. Аналогічно працюють незалежні розслідувачі з Bellingcat і Amnesty: вони складають докази причетності рф до військових злочинів, використовуючи виключно відкриту інформацію.

OSINT-інструменти також активно допомагають у виявленні конкретних військових злочинців й їх підрозділів. Наприклад, українська приватна компанія Molfar використовує аналіз публічних постів і фотографій у Telegram, Viber та інших мережах, щоб геолокувати позиції ворожих підрозділів і навіть визначати військові російські кадри [3]. Так, аналіз відео з ювілею російської «П'ятнашки» дозволив з'ясувати точне розташування бригади рф та її керівництва. Аналогічні OSINT-розслідування допомагали ідентифікувати причетних до катувань чи згвалтувань мирних жителів. Усе це нарощує доказову базу для українських та міжнародних судів. Крім того, існує OSINT-проєкт Oryx, який щоденно фіксує втрати російської техніки на війні – цей «рахунок техніки» також будується на публічних знімках і відео, опублікованих у відкритих джерелах [4]. Підводячи підсумки проведеного дослідження, слід зазначити, що OSINT як інструмент відкритої розвідки відіграє ключову роль у виявленні загроз з боку рф, дозволяючи оперативно фіксувати факти дезінформації, воєнних злочинів та кіберзагроз, що в комплексі підсилює національну безпеку України.

1. Klepper D. https://apnews.com/. URL: https://apnews.com/article/russia-ukraine-technology-social-media-misinformation-05d147b128c48bfa23705409448b7bbc (дата звернення: 30.04.2025).

2. Freear, M. (2022). OSINT in an Age of Disinformation Warfare. RUSI. URL: https://www.rusi.org/explore-our-research/publications/commentary/osint-age-disinformation-warfare (дата звернення 30.04.2025);

3. InformNapalm. Використання OSINT-методів у боротьбі з російською агресією. URL: https://informnapalm.org (дата звернення 30.04.2025);

4. Bellingcat. OSINT Tools and Resources Handbook. URL: https://www.bellingcat.com/resources/ (дата звернення 30.04.2025);

Темрієнко Валерій,
старший викладач кафедри ОРД та РЗ ННІ № 2
(Харківський національний університет
внутрішніх справ)

OSINT-ДОСЛІДЖЕННЯ ЯК ІНСТРУМЕНТ ВИЯВЛЕННЯ, ДОКУМЕНТУВАННЯ ТА РОЗСЛІДУВАННЯ ВОЄННИХ ЗЛОЧИНІВ

Теперішні технології суттєво змінили способи ведення війни, а також методи її дослідження й документування. Одним з ефективних методів став OSINT – розвідка з відкритих джерел (Open Source Intelligence). Термін «відкритий» вказує на загальнодоступність джерела (на відміну від секретних джерел і джерел з обмеженим використанням). Підчас повномасштабної війни росії проти України ця методологія набула особливої актуальності, дозволяючи точно і швидко фіксувати факти, що потенційно можуть бути кваліфіковані як воєнні злочини.

Воєнні злочини визначаються як серйозні порушення міжнародного гуманітарного права, зокрема положень Женевських конвенцій 1949 року та Додаткових протоколів до них. Згідно з Римським статутом Міжнародного кримінального суду (ст. 8), до воєнних злочинів належать умисне вбивство цивільного населення, тортури, насильство, депортація, руйнування цивільної інфраструктури тощо.

OSINT охоплює аналіз інформації, яка є у відкритому доступі: публікації в соціальних мережах, відеозаписи, супутникові знімки, публічні реєстри, медіа. На відміну від закритої розвідки, OSINT є доступним і легальним інструментом, який активно використовують журналісти, правозахисники та аналітичні центри.

Основні методи OSINT, які використовуються підчас документування та розслідування військових злочинів:

- Геолокація: встановлення місця події за ландшафтними та архітектурними орієнтирами;
- Хронолокація: визначення часу події через аналіз тіней, погодних умов, метаданих;
- Верифікація даних через порівняння з іншими джерелами.

Одним із найвідоміших досліджень в Україні підчас військової агресії росії стали масові вбивства цивільних у Бучі, де супут-

никові знімки компанії Maxar дозволили встановити, що тіла мирних жителів лежали на вулицях ще до відступу російських військ. Було спростовано заяви російської сторони про «постановку».

Інший приклад – аналіз авіаудару по Драмтеатру в Маріуполі у березні 2022 року. За допомогою OSINT-аналітики було ідентифіковано дату та тип авіаудару, а також кількість жертв.

До найпоширеніших інструментів належать:

- Google Earth Pro, Sentinel Hub – для супутникової аналітики.
- InVID, Metadata2Go – для аналізу відео та фото.
- TinEye, Google Reverse Image Search – зворотній пошук зображень.
- Paliscope, Maltego – для побудови зв'язків між об'єктами розслідування.

Хоча OSINT поки що не має універсального статусу допустимого доказу у міжнародному праві, практика його використання зростає. Міжнародний кримінальний суд визнає такі докази у разі їхньої належної автентифікації.

Показовим став судовий процес щодо збиття літака Boeing 777 рейс MH17 із Нідерландів до Малайзії, де саме OSINT-докази (супутникові дані, відео, повідомлення у соцмережах) лягли в основу обвинувачень.

OSINT-дослідження пов'язані з низкою викликів:

- ризик маніпуляцій і дезінформації;
- загроза приватності жертв;
- небезпека для дослідників;
- труднощі з юридичною валідністю зібраної інформації.

Для зниження цих ризиків потрібне дотримання аналітичних стандартів, прозора методологія та міждисциплінарна співпраця з юристами і правозахисниками.

OSINT-дослідження довели свою ефективність як інструмент виявлення та фіксації воєнних злочинів. Вони дозволяють оперативно реагувати на події, зберігати докази для подальших судових процесів та інформувати міжнародну спільноту. Водночас необхідно удосконалювати правову базу, яка б дозволила ефективно інтегрувати OSINT у систему міжнародного правосуддя.

---

1. Римський статут Міжнародного кримінального суду. – ООН, 1998.
2. Женевські конвенції 1949 року та Додаткові протоколи до них.

3. Розслідування Bellingcat – https://www.bellingcat.com
4. Криміналістична архітектура – https://forensic-architecture.org
5. Технології Maxar – https://www.maxar.com
6. Центр інформаційної стійкості – https://www.info-res.org
7. Техніки OSINT: ресурси для розкриття інформації в Інтернеті (M. Bazzell, 2023).
8. Звіти Human Rights Watch, Amnesty International щодо України (2022–2023 рр.).
9. Zwitter A., Boisse-Despiaux M. «Етичні виклики OSINT в епоху AI» Розвідка та національна безпека, 2022.
10. Ініціатива правосуддя з відкритим вихідним кодом (OSJI) – https://www.justiceinitiative.org
11. Федчак І. А. Основи кримінального аналізу : навчальний посібник. Львів : Львівський державний університет внутрішніх справ, 2021. 288 с.
12. Щурат Т. Г., Смук А. О. Деякі аспекти розвідки з відкритих джерел інформації (OSINT). Оперативно-розшукова діяльність Національної поліції: проблеми теорії та практики : матеріали Всеукраїнської науково-практичної конференції. Дніпро, 2017. 132 с.

Тимошенко Віра,
доктор юридичних наук, професор,
провідний науковий співробітник
(Національна академія внутрішніх справ)

КРИМІНАЛІСТИЧНА ІДЕНТИФІКАЦІЯ З ВИКОРИСТАННЯМ СИСТЕМ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ У ВИМІРІ ЗАХИСТУ ПРАВ ЛЮДИНИ

Захист прав людини в сучасному світі є одним із пріоритетних завдань держави та суспільства. Права людини, як невід'ємне надбання всіх людей, включають право на життя, свободу та особисту недоторканність, право на повагу до гідності, свободу пересування, право на невтручання в особисте та сімейне життя й багато інших. Процес реалізації прав зазнає впливу політичного, економічного, соціального, психологічного, релігійного та інших факторів, які можуть створювати певні загрози та виклики цьому процесу. До подібних наслідків може призводити й використання спеціальної техніки в процесі запобігання злочинам, зокрема систем відеоспостереження з функцією розпізнавання обличчя.

Як відомо, серед завдань, що стоять перед криміналістикою, на особливу увагу заслуговує ідентифікація особи злочинця. Розслідування злочинів, вчинених в умовах неочевидності, зазвичай пов'язане зі складністю встановлення особи правопорушника. Якщо злочин вчинила особа, яка раніше не порушувала закон і не потрапляла в поле зору правоохоронних органів, доцільно звернутись до новітніх розробок у сфері криміналістичної ідентифікації, серед яких і технологія розпізнавання обличчя, що охоплює аналіз створеного комп'ютером шаблону, отриманого із зображення людини, та порівняння комп'ютерного аналізу з уже зібраними зображеннями [1]. Користування цією технологією дає можливість проводити перевірку, ідентифікацію та категоризацію шляхом аналізу зображення обличчя людини, допомагає фіксувати переміщення підозрюваних, встановлювати час та виявляти потенційних спільників, свідків, постраждалих і невідомі жертви, а значить може використовуватися для виявлення, розслідування та запобігання злочинам і шкоді, а також для протидії різним загрозам, тим самим сприяючи суспільним інтересам у сфері безпеки та правопорядку

[2]. Використання технології розпізнавання обличчя сприяє попередженню злочинності за рахунок покращення поліцейського нагляду та можливостей слідства. Правоохоронні органи отримують можливість швидкої ідентифікації та визначення місця знаходження підозрюваних, тим самим прискорюючи арешти [3].

До переваг біометричної ідентифікації особи за зображенням обличчя слід віднести оперативність розпізнавання об'єкта та високу ефективність. Оскільки системи розпізнавання обличчя часто пов'язані з базами даних за кримінальними справами, вони дозволяють поліції ефективно перевіряти та контролювати відомих порушників і втікачів. Серед мінусів виділяють ресурсозатратність впровадження окремих технічних рішень, необхідність створення різних баз даних, додаткового захисту інформації, що обробляється, проведення подальшого контролю, можливість помилки та поширення на людей, які не причетні до вчинення правопорушень. Сучасні алгоритми розпізнавання обличчя демонструють високий рівень точності завдяки використанню нейронних мереж. Однак ризик помилок, пов'язаних з ідентифікацією, існує завжди, а наслідком може бути порушення прав людини. Так, неточності в алгоритмах можуть призвести до помилкових спрацювань, що створює додаткові ризики для невинних громадян. Крім того, технологія розпізнавання обличчя стикається з проблемою расової та ґендерної упередженості, що може призвести до дискримінації. Спостереження за масами людей без належного законодавчого контролю за цим процесом здатне призвести до порушення конфіденційності та неправомірного втручання в особисте життя, контролю над особистою інформацією. Порушення вимог кібербезпеки призводить до витоку даних та використання інформації зі злочинною метою.

Технології розпізнавання обличчя в ряді країн світу знайшли застосування в багатьох областях, включаючи безпеку та правоохоронну діяльність. В Україні у Верховній Раді зареєстровано законопроект № 11031 «Про єдину систему відеомоніторингу стану публічної безпеки», який передбачає встановлення камер для постійного спостереження. Однак впровадження такої системи вимагатиме великих фінансових інвестицій, оскільки камери повинні бути встановлені в людних місцях, а їх багато. Нова система може спростити пошук злочинців, але також загрожує можливим тотальним стеженням за населенням [4]. До того ж у законопроекті відсутня

заборона на використання штучного інтелекту (ШІ) для збору та обробки персональних даних. Ця заборона передбачена Artificial Intelligence Act – законом про регулювання ШІ, що спрямований на мінімізацію ризиків, пов'язаних з його використанням (прийнятий Європейським парламентом 13 березня 2024 року та схвалений Радою ЄС 21 травня 2024 року) [5]. Отже, прийняття законопроекту № 11031 загрожує появою ряду законодавчих колізій та невідповідністю технологічним і правовим стандартам Євросоюзу.

Ще в 2021 р. Рада Європи рекомендувала суворі правила з метою уникнути значних ризиків для недоторканності приватного життя та захисту персональних даних, пов'язаних із зростаючим використанням технологій розпізнавання обличчя. Рада Європи наголошує, що для уникнення дискримінації деякі програми для розпізнавання обличчя повинні бути повністю заборонені. Зокрема, заборона повинна поширюватися на так звані технології розпізнавання емоцій, що дозволяють за виразом обличчя визначати особисті якості, внутрішні відчуття, психічний стан або рівень залучення співробітників до роботи, оскільки ці технології пов'язані з серйозними ризиками в таких галузях, як працевлаштування, доступ до страхування та освіти [6]. Отже, вони можуть загрожувати правам людини.

Таким чином, використання технологій розпізнавання обличчя дозволяє правоохоронним органам діяти більш ефективно, запобігати загрозам та швидко розкривати злочини, тим самим сприятиме попередженню злочинності. Однак, незважаючи на численні переваги, ці технології вимагають ретельного підходу до їх впровадження та експлуатації. Захист даних, запобігання помилкам, правове регулювання та врахування етичних аспектів – ключові питання, які необхідно вирішувати в процесі використання технологій розпізнавання обличчя. У процесі попередження злочинності та запобігання злочинам слід уникати обмеження прав і свобод людини. Процедура та межі такого використання мають бути чітко визначені у законодавстві.

---

1. Akbari A. Facial Recognition Technologies 101: Technical Insights. In *The Cambridge Handbook of Facial Recognition in the Modern State*. Edited by Rita Matulionyte and Monika Zalnieriute. Cambridge Law Handbooks. Cambridge: Cambridge University Press, 2024. P. 29–43. DOI: https:// doi.org/ 10.1017/9781009321211.004

2. Lynch N. Facial Recognition Technology in Policing and Security–Case Studies in Regulation. *Laws*. 2024. Vol. *13*(3). P. 35. https://doi.org/ 10.3390 /laws13030035

3. Guo Z., Kennedy L. Policing based on automatic facial recognition. *Artificial Intelligence and Law*. 2023. Vol. 31 (2). P. 397-443. DOI:10.1007/s10506-022-09330-x

4. Мельник О. В Україні готуються до запровадження системи тотального розпізнавання обличчя – коли запрацює. 2024, 11 вересня. URL.: https://isef.in.ua/nauka-ta-innovatsii/v-ukraini-hotuiutsia-do-zaprovadzhennia-systemy-totalnoho-rozpiznavannia-oblych-koly-zapratsiuie-575/

5. The EU Artificial Intelligence Act. URL.: https://artificialintelligenceact.eu/

6. Facial recognition: strict regulation is needed to prevent human rights violations. Council of Europe. Strasbourg. 2021, 28 January. URL.: https://www.coe.int/en/web/portal/-/facial-recognition-strict-regulation-is-needed-to-prevent-human-rights-violations-

Торбас Олександр,
доктор юридичних наук, професор,
завідувач кафедри кримінального процесу
(Національний університет
«Одеська юридична академія»)

ОСОБЛИВОСТІ ВИКОРИСТАННЯ OSINT У КРИМІНАЛЬНОМУ ПРОЦЕСУАЛЬНОМУ ДОКАЗУВАННІ

На даний момент складно переоцінити роль OSINT в майже будь-яких сферах життєдіяльності, адже будь-хто в даний момент, сам цього не розуміючи, залишає свій цифровий слід в мережі Інтернет. «OSINT є концепцією, методологією та технологією для отримання та використання військової, політичної, економічної та іншої інформації з відкритих джерел без порушення закону» [1]. «Він використовується для прийняття рішень у сфері національної оборони та безпеки, у розслідуваннях та інших сферах. OSINT включає збір інформації, її реєстрацію, облік та аналіз, аналітичну та синтетичну обробку первинної інформації, зберігання та поширення даних, забезпечення інформаційної безпеки та представлення результатів досліджень» [2].

Відповідно, особи, які обізнані зі специфікою збирання відомостей з відкритих джерел, можуть досить швидко отримати потрібну інформацію про фізичних або юридичних осіб, яка в подальшому може бути використана в тому числі у незаконних цілях. Однак на противагу цьому працівники правоохоронних органів також можуть використовувати відомості, отримані з відкритих джерел, при розслідуванні різних кримінальних правопорушень. Хоча, напевно, найяскравіше це проявляється саме при розслідуванні воєнних кримінальних правопорушень.

Хоча з технічної точки зору було розроблено безліч механізмів для виявлення, оцінки, аналізу та фіксації відомостей, отриманих з відкритих джерел, на практиці досі виникають проблеми з процесуальним закріпленням такої інформації та її подальшим використанням для доведення фактів вчинення воєнних кримінальних правопорушень. Незважаючи на величезний обсяг інформації, яку можна отримати за допомогою OSINT, уповноважені учасники

кримінального провадження з певною настороженістю ставляться до таких відомостей та найчастіше використовують такі відомості як додаткову доказову інформацію, яка обов'язково має встановлюватися «традиційними» доказами. Власне це ж стає причиною відсутності єдності у розумінні форм фіксації відомостей, отриманих з відкритих джерел.

Як зазначають вчені, найчастіше відомості з відкритих джерел оформлюються у формі протоколу [3, с. 773]. Такий висновок можна зробити як оцінивши положення кримінального процесуального законодавства, так і стандартів фіксації відомостей з відкритих джерел, які містяться в протоколі Берклі. Судова практика також підтверджує правильність такого підходу. Наприклад, популярними є наступні формулювання «… а саме: протоколом огляду від 18.02.2025 в ході якого оглянуто Інтернет сторінку сайту «Мариупольского многопрофильного техникума». На вказаному сайті розміщена стаття про «щотижневу церемонію винесення прапору та виконання гімну рф» на якому взяла участь ОСОБА_5 , як ведуча заходу «OSINT аналіз»; протокол огляду від 12.02.2025 в ході якого оглянуто публікацію в соціально орієнтованій мережі «Контакт» з назвою «Моя видео-визитка учасника республиканского конкурса «Педагог года Донецкой Народной Республики» в номинации «Советник года» яка розміщена 28.02.2024 в цьому відео ОСОБА_5 зазначає, що з 01.09.2023 року зайняла посаду «советника директора по воспитанию и взаимодействию с детскими общественными обьединениями» «OSINT аналіз» [4].

Більше того, навіть з аналізу практики ВС можна зробити висновок, що такий спосіб збору даних з відкритих джерел є найбільш вдалим, адже не може порушувати права та законні інтереси учасників кримінального провадження: «З метою з`ясування обставин, які підлягають доказуванню, інспектор Управління протидії кіберзлочинам в Одеській області провів огляд публікацій в засобах масової інформації через мережу Інтернет і задля збереження доступності інформації у відкритих джерелах, здійснив її цифрове зберігання - архівацію, яка надає змогу захистити та зберігати інформацію з плином часу, включаючи її справжність, доступність, ідентичність, постійність, рендеринг (візуалізацію) та зрозумілість, що корелюється зі стандартами, викладеними у Протоколах Берклі, визнаних Управлінням ООН (т. 2, а. п. 135 - 159)» [5]. В даному

випадку можна зробити висновок, що ВС визначає дещо нижчий стандарт допустимості доказів, отриманих з відкритих джерел, саме через технічну легкість фіксації такої інформації та простоту у її подальшій перевірці самим судом.

В той же час наявні і інші прикладі використання OSINT у кримінальному провадженні. Так, в одному з судових рішень обґрунтованість підозри, крім іншого, також доводиться «довідкою за результатами OSINT-дослідження до № 4/1/1-15543 від 12.12.2024щодо діяльності ООО «АЛАБУГА МАШИНЕРИ» (основний вид діяльності: виробництво обладнання спеціального призначення, не включеного до інших угрупувань), в якій зазначено, що вказане підприємство може бути одним із головних підрядників розробленого між рф та Іраном проекту «Лодка» по виробництву ударних безпілотників» [6]. Очевидна проблема в даному випадку полягає в тому, що чинне кримінальне процесуальне законодавство не містить такого окремного процесуального документу як довідки, а тому не зовсім зрозуміло, чи було в даному випадку докази отримано в порядку, передбаченому КПК України, та, відповідно, чи можуть такі докази визнаватися допустимими.

В межах даної доповіді дуже складно оцінити правову природу такої довідки, проте можна зробити припущення, що протокол огляду веб сайту та довідка за результатами OSINT дослідження вказують на різні ступені залучення інформації з відкритих джерел. Протокол огляду доцільно складати тоді, коли необхідно зафіксувати інформацію з одного конкретного джерела. Довідку ж доцільно складати тоді, коли доказове значення має не окреме джерело інформації, а ціла сукупність джерел. Крім того в такого роду довідках також можна пояснювати специфіку збору, оцінки, аналізу та фіксації такої інформації, що також може мати значення для кримінального провадження. Очевидною проблемою є те, що, як було зазначено вище, кримінальний процесуальний статус таких довідок не визначений чинним законодавством, що ускладнює їх застосування на практиці.

---

1. Жарков Я.М., Васильєв А.О. Наукові підходи щодо визначення суті розвідки з відкритих джерел. Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки. 2013. Вип. 30. С. 38-41.

2. Калугін В.Ю., Сіфоров О.І. Використання OSINT у встановлені фактів воєнних злочинів та особи воєнних злочинців. ВОЄННИЙ СТАН: ТЕОРЕТИКО-ПРАКСЕОЛОГІЧНІ ПРОБЛЕМИ ЮРИСПРУДЕНЦІЇ. 2024. С. 202-225.

3. Тетерятник Г.К., Виходець Ю.О. Теоретичні та праксеологічні аспекти фіксування та використання у кримінальному процесуальному доказуванні інформації з Інтернет-джерел. Юридичний науковий електронний журнал. 2022. № 10. С. 772-776.

4. Ухвала слідчого судді Жовтневого районного суду м. Дніпропетровська від 16.04.2025, справа № 201/4267/25. URL: https://reyestr.court.gov.ua/Review/126668932

5. Постанова ВС від 27.01.2025, справа № 947/22776/22. URL: https://reyestr.court.gov.ua/Review/124866093

6. Ухвала слідчого судді Шевченківського районного суду м. Києва від 21.03.2025, справа № 761/10611/25. URL: https://reyestr.court.gov.ua/ Review/126035663

Шаповаленко Євген,
кандидат юридичних наук, доцент,
професор кафедри оперативно-розшукової діяльності
та національної безпеки
(Національна академія внутрішніх справ)

ПРАВОВІ ТА ОРГАНІЗАЦІЙНІ АСПЕКТИ РОЗШУКУ БЕЗВІСТІ ЗНИКЛИХ НА ДЕОКУПОВАНИХ ТЕРИТОРІЯХ

Деокупація тимчасово окупованих територій України становить ключовий напрям стратегічного розвитку української держави та суспільства в умовах збройного конфлікту. Основними завданнями цього процесу є: припинення збройної агресії з боку рф, виведення її військових формувань та ліквідація незаконних збройних угруповань на території України, а також відновлення конституційного ладу й правопорядку в межах міжнародно визнаних кордонів України. При цьому особлива увага приділяється гарантуванню безпеки громадян та превенції кримінальних правопорушень у перехідний період [1].

Після деокупації частини територій України, що тривалий час перебували під контролем збройних формувань рф, виявлено значну кількість фактів зникнення людей, масових поховань та ознак насильницьких злочинів. пошук безвісти зниклих у цих регіонах є складним, багатокомпонентним процесом, який потребує чіткої координації дій слідчих органів, судово-медичних експертів, пошукових груп і правозахисників. Встановлення долі зниклої особи має не лише кримінально-правове, а й глибоке моральне та соціальне значення – для рідних, для суспільства, для історичної справедливості. За час повномасштабної війни в Україні безвісти зникли десятки тисяч людей. У реєстрі зниклих безвісти за особливих обставин міститься понад 71 тис. записів про військових і цивільних українців. З них 40 тис. людей отримали такий статус з початку 2025 року. У розшуку перебувають 59 тис. українців. Лише 7,5 тисяч із них офіційно визнані Міжнародним Комітетом Червоного Хреста полоненими. Станом на 1 січня 2025 року припинено пошук 9255 людей: 3923 особи були знайдені живими й ідентифіковано 5332 тіла. Також у реєстрі накопичується інформація про неіденти-

фіковані тіла. Наразі йдеться про понад 3,2 тис. таких записів [2].

Однак, відповідно до норм міжнародного гуманітарного права сім'ї мають право знати про долю членів їхньої родини, а також можуть звернутися до держави за наданням інформації. Положеннями міжнародного гуманітарного (звичаєвого) права передбачено, що у випадку збройних конфліктів міжнародного та неміжнародного характеру сторони конфлікту «повинні вживати всіх можливих заходів для з'ясування долі осіб, оголошених зниклими безвісти» [3]. Таке положення міжнародного гуманітарного права спрямовано на забезпечення порядку виконання відповідними суб'єктами, правоохоронними органами та організаціями, які мають правоохоронні функції обов'язку щодо диференціації причин зникнення осіб під час тимчасової окупації територій та визначення способів їх розшуку та репатріації [4].

Особливості правового регулювання суспільних відносин, пов'язаних із набуттям правового статусу осіб, зниклих безвісти за особливих обставин, з обліком, розшуком та соціальним захистом таких осіб і членів їхніх сімей визначаються:

Женевською конвенцією [5] та Римським статутом Міжнародного кримінального суду [6] – у частині захисту цивільного населення та відповідальності за насильницьке зникнення;

Законом України від 12.07.2018 № 2505-VIII «Про правовий статус осіб, зниклих безвісти за особливих обставин» [7]. Закон є основним нормативно-правовим актом, в якому окреслена державна політика щодо осіб, зниклих безвісти за особливих обставин: визначення окремого правового статусу, прав та гарантій, що передбачені для зниклих безвісти осіб, а також для їхніх родин; системи органів та інститутів державної влади, що відповідальні за втілення державної політики з цього питання, тощо. Інші законодавчі та підзаконні акти лише доповнюють та деталізують положення даного Закону [8];

Порядком забезпечення вилучення тіл (останків) осіб, загиблих (померлих) у зв'язку із збройною агресією проти України, затвердженому постановою Кабінету Міністрів України від 17 червня 2022 р. № 698 [9];

Кримінальним процесуальним кодексом (КПК) України (ст. ст. 214, 242) щодо підстав для розслідування та проведення експертиз [10] та ін.

На деокупованих територіях причинами зникнення стали:

насильницьке утримання у підвалах, катівнях або під час «фільтраційних» процедур; депортація до рф або примусове переміщення в окуповані регіони; вбивство та поховання у «братських» або «прихованих» могилах; знищення документів та перешкоджання ідентифікації; руйнування соціальної інфраструктури, що призвело до втрати зв'язку між людьми. Загалом, розшук зниклих безвісти на деокупованих територіях є глибоко гуманітарною місією, спрямованою на захист прав людини, відновлення соціальної справедливості та історичної пам'яті. Саме тому аналіз особливостей цього процесу є вкрай актуальним у сучасних умовах.

Координацією пошукових дій займається Комісія з питань осіб, зниклих безвісти, яка веде облік зниклих та організовує міжвідомчу співпрацю. У свою чергу, Національна поліція України є одним із перших органів, до яких звертаються родини осіб, зниклих безвісти за особливих обставин, адже саме до територіальних органів поліції подається заява про розшук особи, за якою й відкривається відповідне провадження. І, хоча з початком повномасштабного вторгнення виникали проблеми щодо відкриття провадження відносно осіб, зниклих безвісти за особливих обставин (попередня відмова у відкритті провадження щодо цивільної особи через нерозуміння підслідності справи та некоректна кваліфікація), на даний момент на цьому етапі процесу з проблемами вони переважно не стикаються. Однак труднощі виникають на інших етапах. Зокрема, як родичі, так і представники громадських організацій відзначають, що ускладненою є комунікація зі слідчими, яким передається провадження за територіальною підслідністю, – відповідно, справа переходить до представників Національної поліції в територіальних підрозділах Донецької, Луганської, Херсонської, Запорізької областей. Враховуючи навантаження на слідчих частково окупованих та прифронтових областей, суттєво сповільнюється проведення слідчих (розшукових) дій, а родини тривалий час не можуть дізнатися про статус провадження. Крім того, сповільнює процес і часта зміна слідчих, відповідальних за провадження, у зв'язку з їхнім навантаженням [8].

Надалі, слідчий або прокурор зобов'язані невідкладно, але не пізніше 24 годин після отримання відповідної заяви або повідомлення про кримінальне правопорушення, або після самостійного виявлення обставин, що можуть свідчити про таке правопорушення, внести відповідні відомості до ЄРДР та розпочати розслідуван-

ня (ч. 1 ст. 214 КПК України). Слідчий, невідкладно в письмовій формі повідомляє керівника органу прокуратури про початок досудового розслідування, підставу початку досудового розслідування та інші відомості, передбачені ч. 5 ст. 214 КПК України (ч. 6 ст. 214 КПК України) [10].

Першочергові оперативно-розшукові заходи й процесуальні дії спрямовані на огляд місцевості з використанням дронів, супутникових знімків; виявлення катівень, масових поховань; залучення свідків – місцевих мешканців, військових, волонтерів; фіксація обстановки та вилучення предметів, що можуть містити ДНК-матеріал; аналіз списків депортованих, утримуваних, переміщених; зіставлення з базами зниклих. Також, оперативно-розшукові заходи спрямовані на встановлення анкетних даних зниклої особи, дати й місця народження, номери мобільних телефонів; встановлення близьких родичів зниклої особи, їх номерів мобільних телефонів; анкетних даних, номерів мобільних телефонів тощо; встановлення точної дати, часу й останнього місця перебування зниклої особи; встановлення конкретних обставин, за яких особа зникла безвісти; проведення аналізу за номером мобільного телефона; здійснення моніторингу місця знаходження мобільного телефону, передусім щодо останніх 3–5 днів до зникнення його з мережі; перевірка особи за наявними автоматизованими базами даних (для перевірки інформації, чи не знаходиться розшукувана особа на території України); з метою перевірки можливого знаходження особи на території Євросоюзу надати відповідний запит (використання можливостей Європолу) [4].

Відзначимо, що розслідування масових поховань можуть бути невід'ємною частиною масштабнішого розслідування щодо потенційно незаконного заподіяння смерті. Інформація про масові поховання, надана свідками, членами громади та вцілілими особами, може містити важливу інформацію. Відповідно до Закону України «Про державну реєстрацію геномної інформації людини», обов'язковій державній реєстрації підлягає геномна інформація встановлена з раніше відібраних біологічних зразків осіб, зниклих безвісти, або біологічного матеріалу з особистих речей осіб, зниклих безвісти, відомості щодо яких внесено до ЄРДР або відображено в постанові про початок досудового розслідування, винесеній у порядку, передбаченому ст. 615 КПК України [11].

Варто наголосити, що установлення безвісти зниклих під час воєнних дій – аналітичне дослідження, що є одним з найскладніших для відпрацювання як класичними методами, так і за допомогою аналітики. Дослідження такого змісту нагадують роботу з неструктурованим масивом інформації значного обсягу. Повідомлення про зникнення обчислюють тисячами і варіюються від повідомлень родичів, які втратили зв'язок з рідними, до зникнення осіб у процесі окупації певних територій. Інколи злочинці намагаються скористатися воєнним часом для приховання та інсценування вбивств чи грабежів. Тому правоохоронці зосереджують максимальну увагу на кожному провадженні про зникнення і одразу приступають до комплексу розшукових й аналітичних заходів. Така робота безпосередньо пов'язана з накопиченням та узагальненням величезного обсягу даних про зниклих осіб. Кожна зникла людина відпрацьовується на предмет зв'язків і контактів, через які можна встановити її місцеперебування. Проводять відповідний моніторинг медіа. Кожний випадок індивідуальний, проте за кожним повідомленням стоїть доля людини.

Підсумовуючи констатуємо, що проблематика розшуку безвісти зниклих на деокупованих територіях України є складним комплексом взаємопов'язаних юридичних, криміналістичних, гуманітарних та морально-етичних завдань. Масові порушення прав людини, зафіксовані після звільнення тимчасово окупованих територій, підтверджують системний характер злочинів, пов'язаних із насильницькими зникненнями, позасудовими вбивствами, депортацією та катуванням цивільного населення.

Успішне встановлення долі зниклих осіб потребує: ефективної міжвідомчої координації між правоохоронними органами, судово-медичними експертами, представниками місцевої влади, волонтерськими організаціями та міжнародними партнерами; створення єдиної інтегрованої бази даних із можливістю обміну інформацією; широкого застосування сучасних технологій, включно з ДНК-ідентифікацією, аналізом супутникових знімків, 3D-моделюванням місцевості тощо; належного нормативного регулювання процедур ексгумації, ідентифікації та поховання загиблих з дотриманням принципів гуманного поводження та міжнародного гуманітарного права.

У довгостроковій перспективі розшук зниклих безвісти осіб має розглядатися не лише як процесуальне завдання кримінального

провадження, а як невід'ємна частина постконфліктного правосуддя, національної пам'яті та забезпечення прав людини. Лише за умови повного документування кожного факту насильницького зникнення й відновлення істини щодо обставин зникнення можна досягти справжньої справедливості та зміцнити довіру суспільства до державних інституцій.

---

1. Луценко Б. Г. Кримінологічне забезпечення та супроводження деокупації тимчасово окупованої території України: дис… докт. філос. : 081 – Право. Х., 2024. 263 с.
2. Майже 30 тисяч українців отримали статус зниклих безвісти з 2024 року. *Національне інформаційне бюро*. URL: https://nib.gov.ua/news/maizhe-30-tysiach-ukraintsiv-otrymaly-status-znyklykh-bezvisty-z-2024-roku/
3. Борнмутський протокол про захист і розслідування масових поховань. URL: https://www.icmp.int/wp-content/uploads/2022/02/11489-FMC-Mass-Graves-Project-UKRAINE-V3.0-HI-RES.pdf
4. Назимко Є. С., Пономарьова Т. І., Лосич С. В. Особливості здійснення правоохоронної діяльності на деокупованих територіях: навч. посіб. Кропивницький: ДонДУВС, 2024. 199 с.
5. Женевська конвенція про поводження з військовополоненими: Конвенція ООН від 12.08.1949 р. URL: https://zakon.rada.gov.ua/laws/ show/ 995_153#Text
6. Римський Статут Міжнародного Кримінального Суду від 17.07.1998 р. URL: https://zakon.rada.gov.ua/laws/show/995_588/sp:max50:nav7:font2#Text
7. Про правовий статус осіб, зниклих безвісти за особливих обставин: Закон України від 12.07.2018 р. № 2505-VIII. URL: https://zakon.rada.gov.ua /laws/show/2505-19#Text
8. Як Україна розшукує зниклих безвісти внаслідок агресії росії та підтримує членів їхніх сімей. *Аналітичний звіт*. 2024. URL: https://zmina.ua/wp-content/uploads/sites/2/2024/07/znykli_bezvisty_a4_ua-preview.pdf
9. Деякі питання забезпечення вилучення, передачі та репатріації тіл (останків) осіб, загиблих (померлих) у зв'язку із збройною агресією проти України: постанова Кабінету Міністрів України від 17.06.2022 р. № 698. URL: https://zakon.rada.gov.ua/laws/show/698-2022-%D0%BF#Text
10. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text
11. Про державну реєстрацію геномної інформації людини: Закон України від 09.07.2022 р. № 2391-IX. URL: https://zakon.rada.gov.ua/laws/show/2391-20#Text

Швидкий Олексій,
аспірант
(Державна навчально-наукова установа
«Академія фінансового управління»)

OSINT 4.0: ЦИФРОВІ ТЕХНОЛОГІЇ ДЛЯ ЗМІЦНЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

У сучасну цифрову епоху та в умовах повномасштабної війни Росії проти України, розвідка з відкритих джерел (OSINT) перетворилася з допоміжного інструменту на критично важливий компонент системи національної безпеки. Термін «OSINT» набув поширення наприкінці 1990-х років, зокрема у статті колишнього офіцера ЦРУ Роберта Девіда Стіла, однак завдяки швидкому розповсюдженню використання цифрових інформаційних технологій спостерігається трансформація суспільних відносин у сфері збору та аналізу інформації, що призвело до появи нової парадигми розвідувальної діяльності, де межа між професійними розвідниками та пересічними громадянами стає все більш розмитою, а цифрові інструменти відкривають безпрецедентні можливості для забезпечення національної безпеки [1; 2].

Військова агресія російської федерації проти суверенної територіальної цілісності та державності України стала унікальним контекстом, що демонструє як потенціал, так і виклики використання цифрових інструментів OSINT-технологій. Російсько-українську війну часто називають «першою цифровою війною», де широке застосування смартфонів, соціальних мереж, супутникових знімків та дронів створює безпрецедентний обсяг даних у режимі реального часу [3; 4].

На основі аналізу масштабної цифрової трансформації та її впливу на систему національної безпеки варто розглянути еволюцію OSINT-підходів від її історичних витоків до сучасного цифрового втілення: 1) ранні початки OSINT (OSINT 1.0) сягають початку XIX століття – від використання газет країн-противників для прийняття рішень у секторі оборони; 2) кінець XIX століття – початок XX століття (OSINT 2.0) – поява систематичної практики збору інформації з відкритих джерел стали більш систематичними з поя-

вою генеральних штабів та державних (національних) розвідувальних управлінь; 3) кінець XX століття (OSINT 3.0) – поява інформаційно-комунікаційних технологій сприяла розширенню сфери охоплення та формуванню ширшої розвідувальної діяльності; 4) сучасна ера (OSINT 4.0) – моніторинг інформації у соціальних мережах, поява нових рівнів інформації шляхом використання супутників, відбулось розмиття меж між традиційним збором розвідданих та обміном публічною інформацією.

У цифрову епоху та в умовах сучасної війни OSINT перетворилася з допоміжного джерела розвідки на критично важливий компонент зусиль у сфері національної безпеки. Демократизація інформації через соціальні мережі та доступність комерційних технологій зробили OSINT потужним інструментом як для державних, так і недержавних суб'єктів, кардинально змінивши спосіб збору та використання розвідданих у конфліктах. Широке використання смартфонів та соціальних мереж як комбатантами, так і цивільними, створило безпрецедентний обсяг інформації, доступної в режимі реального часу, яка безпосередньо стосується збройних конфліктів. Комерційні супутникові знімки та інші технології з відкритим кодом надають додаткові рівні інформації, які раніше були недоступні для більшості суб'єктів. В контексті сучасної війни ці еволюційні процеси набули особливого значення, оскільки цифрові технології стали каталізатором фундаментальних змін у підходах до національної безпеки.

Війна росії проти України слугує ключовим тематичним дослідженням, що демонструє як потенціал, так і виклики використання OSINT для національної безпеки у високоризикованому геополітичному середовищі, підкреслюючи динамічну взаємодію між традиційними методами розвідки та новою сферою OSINT, що має значні наслідки для майбутніх військових та розвідувальних практик. Інтенсивність військових дій та активна участь як державних, так і недержавних суб'єктів в інформаційній сфері роблять його ідеальною призмою для аналізу ефективності та обмежень OSINT. Війна також спричинила появу інновацій в методологіях та інструментах розвідки, а досвід України, ймовірно, визначатиме майбутнє OSINT у контекстах національної безпеки в усьому світі.

Органи у сфері національної безпеки та оборони (Міністерство оборони, Служба безпеки України, Рада національної безпеки і

оборони), активно залучаються до використання OSINT, публікуючи заяви та звіти щодо важливості та застосування OSINT для забезпечення національної безпеки [5; 6]. Зокрема, розроблено інструменти та платформи, такі як додаток «Дія», для збору інформації від громадян, визнаючи OSINT як критично важливого інструменту для національної безпеки. В умовах війни використання всіх доступних джерел інформації, включаючи ті, що надаються громадськістю, стає важливим для ситуаційної обізнаності та оборони.

Хоча OSINT є надзвичайно цінною, вона не позбавлена обмежень і створює значні виклики, пов'язані з цілісністю даних, етичними міркуваннями та потенціалом для маніпуляцій. Відкрита природа Інтернету та соціальних мереж, хоча й полегшує збір інформації, також створює середовище, де легко поширюється неправдива або оманлива інформація, що вимагає ретельної перевірки та критичного аналізу.

Таблиця 1. Переваги та обмеження використання цифрових технологій OSINT у сфері національної безпеки

Ефективність	**Обмеження**
Можливості раннього попередження	Інформаційне перевантаження
Відстеження пересування військ	Складність верифікації
Викриття воєнних злочинів	Етичні та юридичні питання (конфіденційність, зловживання інформацією)
Протидія дезінформації	Ризик дезінформації та маніпуляції
Формування громадської думки	Потенціал для упередженості та необхідність критичної оцінки джерел
Забезпечення ситуаційної обізнаності	Залежність від доступності та якості відкритих джерел, які можуть бути обмежені або маніпульовані противником
Доповнення традиційних методів розвідки	Необхідність спеціалізованих навичок та інструментів для ефективного аналізу
Демократизація розвідки та залучення громадськості	Потенційні витрати на створення та підтримку інфраструктури для зберігання та обробки великих обсягів даних

Джерело: систематизовано автором на основі [7-9].

OSINT 4.0 представляє собою революційну трансформацію підходів до національної безпеки України. Цифрові технології не просто вдосконалили традиційні методи розвідки – вони створили нову парадигму, де швидкість, масштаб та демократизація збору інформації фундаментально змінюють спосіб протидії загрозам. Ключові фактори успіху: стратегічна інтеграція цифрових технологій у систему національної безпеки; розвиток спеціалізованих навичок та компетенцій; міжнародна співпраця та обмін досвідом; баланс між ефективністю та етичними нормами. Для подальшого розвитку можливостей України у сфері OSINT необхідно вдосконалювати методології, інструменти та навчальні програми. Важливим є сприяння співпраці між українськими та міжнародними експертами, а також створення етичних норм та правових рамок.

Цифрові технології залишатимуться критично важливим інструментом для забезпечення національної безпеки України в умовах динамічного геополітичного ландшафту. Успішна адаптація до викликів цифрової епохи визначатиме спроможність країни ефективно протистояти загрозам та захищати національні інтереси.

---

1. Oerlemans J. J., Langenhuijzen S. Balancing National Security and Privacy: Examining the Use of Commercially Available Information in OSINT Practices. *International Journal of Intelligence and CounterIntelligence*. 2024. No. *38*(2). P. 579-597. URL: https://doi.org/10.1080/08850607.2024.2387850

2. Van Puyvelde D., Tabárez Rienzi F. (2025). The rise of open-source intellig.-nce. *European Journal of International Security*. 2025. P. 1-15. URL: https://doi.org/10.1017/eis.2024.61

3. Open-Source intelligence and the war in Ukraine / INSS. 2023. URL: https://www.inss.org.il/publication/russia-ukraine-intelligence/

4. How open-source intelligence has shaped the Russia-Ukraine war / Ministry of Defence. 2022. URL: https://www.gov.uk/government/speeches/how-open-source-intelligence-has-shaped-the-russia-ukraine-war

5. Malyasov D. OSINT takes center stage in Russia's war in Ukraine. *Defence Blog.* 2023. URL: https://defence-blog.com/osint-modern-warfare-ukraine-defense/

6. НКЦК проводить дводенний онлайн-тренінг «Використання засобів OSINT та ОТ для забезпечення кібербезпеки та протидії дезінформації» / Рада національної безпеки і оборони України. 2021. URL: https://www.rnbo.gov.ua/ua/Diialnist/5188.html

7. Gale A. E. The role of Open-Source Intelligence in the war in Ukraine / Modern Diplomacy. 2023. URL: https://moderndiplomacy.eu/2023/05/17/the-role-of-open-source-intelligence-in-the-war-in-ukraine/

8. Puzzling pieces: OSINT and war crime accountability in Ukraine / Royal United Services Institute. 2024. URL: https://www.rusi.org/explore-our-research/publications/commentary/puzzling-pieces-osint-and-war-crime-accountability-ukraine

9. Open-Source data documents war atrocities in Ukraine / ESRI. 2022. https://www.esri.com/about/newsroom/blog/ukraine-open-source-intelligence

Шевельова Таїсія,
здобувач вищої освіти другого (магістерського) рівня
(Національна академія Служби безпеки України)
Науковий керівник:
Жевелєва Ірина,
кандидат юридичних наук, доцент
(Національна академія Служби безпеки України)

МІЖНАРОДНИЙ ДОСВІД ЗАКОНОДАВЧОГО ВРЕГУЛЮВАННЯ СФЕРИ ШТУЧНОГО ІНТЕЛЕКТУ

Для розуміння сутності поняття штучний інтелект розглянемо підходи науковців до його визначення. Так однією з універсальних є запропонована Барановим О. А. дефініція поняття: штучний інтелект (далі – ШІ) – це певна сукупність методів, способів, засобів та технологій, насамперед, комп'ютерних, що імітує (моделює) когнітивні функції, які мають критерії, характеристики та показники еквівалентні критеріям, характеристикам та показникам відповідних когнітивних функцій людини [1].

Експертною групою високого рівня європейської комісії зі штучного інтелекту було запропоновано таке означення: штучний інтелект – це системи, розроблені людьми, які, отримавши комплексну мету, діють у фізичному чи цифровому світі, сприймаючи навколишнє середовище, інтерпретуючи зібрані структуровані або неструктуровані дані, на основі знань, отриманих з цих даних, приймають найкращі рішення (відповідно до попередньо визначених параметрів) для досягнення заданої мети [2].

Європейським парламентом ШІ визначено, як будь-який інструмент, що використовується програмою для відтворення поведінки, пов'язаної з людиною, такої як міркування, планування та творчість. це поняття може бути розширено, оскільки ші вже може виходити за межі людських можливостей [3].

13 березня 2024 року переважною більшістю голосів Європейським парламентом ухвалено Artificial Intelligence Act (далі – Закон про ШІ). Це перший у світі всеосяжний нормативний акт, який регулює відносини, пов'язані із штучним інтелектом. Як зазначено у пресрелізі, він спрямований на захист фундаментальних прав, демократії, верховенства права та стійкості навколишнього середовища від штуч-

ного інтелекту з високим ризиком, одночасно стимулюючи інновації та утверджуючи Європу як лідера в цій галузі [4].

Закон про ШІ має на меті класифікувати та регулювати програми штучного інтелекту на основі їхнього ризику завдання шкоди. Ця класифікація включає чотири категорії ризику («неприйнятний», «високий», «обмежений» і «мінімальний»), а також одну додаткову категорію для ші загального призначення. Особливу увагу приділено забороні деяких застосунків ШІ, які загрожують правам громадян, таких як системи біометричної категоризації та розпізнавання емоцій. Це відображає тенденцію до захисту приватності та особистих даних, яка стає все більш актуальною в сучасному світі [5].

Нові правила забороняють використання біометричних систем ідентифікації (CIP) правоохоронними органами, за винятком конкретно визначених ситуацій. Система RBI «в реальному часі» може бути впроваджена лише при суворому дотриманні заходів безпеки, наприклад, обмеженням її використання за часом і географією, а також попередньою отриманою судовою або адміністративною згодою. Такий застосунок може містити, наприклад, пошук зниклої особи або запобігання терористичному акту. Використання таких систем після включення дії вважається вкрай ризиковим і потребує судового дозволу, пов'язаного з кримінальною справою.

Також передбачені чіткі зобов'язання для інших систем штучного інтелекту з високим рівнем ризику через їхню значну потенційну шкоду здоров'ю, безпеці, основним правам, навколишньому середовищу, демократії та верховенству права. Приклади використання ШІ з високим ризиком містять критичну інфраструктуру, освіту та професійну підготовку, працевлаштування, основні приватні та державні послуги (наприклад, охорона здоров'я, банки), певні системи правоохоронних органів, управління міграцією та кордонами, правосуддя та демократичні процеси (наприклад, вплив на вибори). Такі системи повинні оцінювати та зменшувати ризики, вести журнали використання, бути прозорими і точними та забезпечувати нагляд з боку людини. Громадяни матимуть право подавати скарги на системи штучного інтелекту та отримувати пояснення щодо рішень, заснованих на системах високого ризику ШІ, які впливають на їхні права [6].

Системи штучного інтелекту загального призначення (GPAI) та відповідні моделі, на яких вони базуються, мають відповідати конкретним вимогам з прозорості, зокрема дотримання законодав-

ства ЄС про авторське право. Більш потужні моделі GPAI, які можуть створювати системні ризики, підпадають під додаткові вимоги, зокрема проведення оцінки моделі та зменшення системних ризиків, а також обов'язкове звітування про інциденти. Крім цього, штучні або підроблені зображення, аудіо- чи відеоконтент («дипфейки»), повинні бути чітко позначені як такі.

Після технічних уточнень Закон має бути остаточно погоджений. Він набуде чинності через двадцять днів після його публікації в «Офіційному журналі» Євросоюзу і буде повністю застосовний через 24 місяці після набрання чинності, за винятком окремих положень.

Закон про ШІ став важливим кроком у забезпеченні технологічного розвитку, який відповідає вимогам суспільства та захищає права і безпеку громадян. Такий розвиток сприяє створенню ефективних і етичних регуляторних рамок, які сприятимуть сталому розвитку та інноваціям у цьому важливому секторі.

У статті 3 Закону наведене визначення «системи штучного інтелекту», що означає програмне забезпечення, яке розроблено з використанням одного або кількох методів і підходів, перелічених у додатку і до Закону, і може, для заданого набору визначених людиною цілей, генерувати результати, такі як контент, прогнози, рекомендації, або рішення, що впливають на середовище, з яким вони взаємодіють.

Ще у лютому 2020 року Європейська комісія опублікувала Білу книгу зі штучного інтелекту: європейський підхід до досконалості і довірі (White Paper On Artificial Intelligence – A European approach to excellence and trust), в якій пропонуються численні заходи і варіанти політики для майбутньої нормативної бази ЄС для штучного інтелекту. Комісія також підготувала звіт про наслідки для безпеки і відповідальності штучного інтелекту, Інтернету, речей та робототехніки.

Однак очікується, що Закон про ШІ набуде чинності не раніше від 2026 року, і буде діяти пільговий період, протягом якого зацікавлені сторони зможуть адаптувати свою діяльність для дотримання норм акта.

Для ефективного використання штучного інтелекту значний вплив здійснив Європейський парламент, створивши самостійний орган Європейської ради з питань штучного інтелекту (European Artificial Intelligence Board).

Сполучене Королівство Великої Британії та Північної Ірландії є одним з лідерів у встановленні міжнародних стандартів у галузі штучного інтелекту, визначенні як внутрішніх, так і глобальних засад розвитку технологій майбутнього.

Стратегічні напрями правового регулювання процесами, пов'язаними з впровадженням технологій штучного інтелекту, окреслено в Національній Стратегії штучного інтелекту, який підготував уряд Великої Британії (від 22 вересня 2021 року). Ця стратегія спрямована на максимальне використання досвіду та наявних ресурсів, що дозволить швидко адаптуватися до нових технологічних змін. Адаптивний підхід ґрунтується на реалізації фундаментальних принципів (безпека, прозорість, справедливість, підзвітність) як основи для розвитку штучного інтелекту та водночас підтримки безпеки й етики використання штучного інтелекту, забезпечення захисту прав людини [7].

Таким чином, можна зазначити, що ЄС та Великобританія є першими державами, які реалізують і запроваджують на законодавчому рівні особливості застосування ШІ у власному законодавстві. Однак потрібно відзначити, що відсутність визначення ШІ не обмежує інші держави у його використанні.

---

1. Баранов О.А. Визначення терміну «штучний інтелект». Інформація і право. 1(44)/2023. с. 32–49. https://doi.org/10.37750/16-6798.2023.1(44).287537.
2. European commission. 2018. a definition of artificial intelligence: main capabilities and scientific disciplines. report high-level expert group on artificial intelligence. Url: https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines.
3. Intelligence artificielle: définition et utilisation. Url: https://www. europarl.europa.eu/news/fr/headlines/society/20200827sto85804/intelligence-artificielle-definition-et-utilisation.
4. Artificial intelligence act. a9-0188/2023. Url: https://www.europarl. europa.eu/ doceo/document/ta-9-2024-0138_en.html.
5. artificial intelligence act: mePs adopt landmark law. news. european Parliament. Url: https://www.europarl.europa.eu/news/en/press-room/2023 1206iPr 15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai
6. EU AI Act: first regulation on artificial intelligence. Abgerufen am 24. Mai 2024. URL: https://www.consilium.europa.eu/en/press/pressreleases/2024/05/21/
7. National AI Strategy. URL: https://www.gov.uk/government/ /national-ai-strategy/national-aistrategy-html-version

Шевченко Наталія,
кандидат економічних наук, доцент,
доцент кафедри менеджменту та економічної безпеки
навчально-наукового інституту
управління, психології та безпеки
(Львівський державний університет
внутрішніх справ)

РОЛЬ OSTIN-ДОСЛІДЖЕНЬ У РЕАГУВАННІ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ ТА СТІЙКІСТЬ УКРАЇНСЬКОЇ ЕКОНОМІКИ В СУЧАСНИХ УМОВАХ

В умовах сучасної війни, в тому числі гібридної, яку веде російська федерація проти України, питання інформаційної безпеки та економічної стійкості набувають стратегічного значення. Одним із ключових інструментів формування ефективної політики у цій сфері є результати OSTIN-досліджень – аналітичних ініціатив, спрямованих на виявлення загроз, прогнозування ризиків та розробку рішень, що сприяють захисту національних інтересів.

OSTIN (розвідка на основі відкритих джерел; англ. Open source intelligence, OSINT) працює як аналітичний центр, який акумулює науково-дослідний потенціал задля зміцнення безпеки України. У фокусі досліджень перебувають інформаційна гігієна, вплив дезінформаційних кампаній на суспільну свідомість, кібербезпека, а також взаємозв'язок між інформаційними атаками та економічною дестабілізацією [1].

Згідно з результатами OSTIN-досліджень, основними векторами інформаційних загроз для України, які мають безпосередній вплив на економічну стабільність, є такі:

1. Поширення фейкових економічних прогнозів. Російські та прокремлівські медіа регулярно публікують неправдиві аналітичні звіти про нібито неминучий дефолт України, занепад банківської системи чи втрату макрофінансової підтримки з боку Заходу. Метою є дестабілізація фінансових ринків та підрив довіри до національної валюти.

2. Маніпуляції щодо курсу гривні та валютного ринку. Через телеграм-канали, боти й псевдоекспертні думки розганяються чутки про стрімке падіння гривні, що спричиняє штучну паніку серед

населення та бізнесу, провокує купівлю валюти й створює навантаження на банківську систему.

3. Дискредитація урядових економічних ініціатив. Інформаційні атаки часто спрямовані на підрив довіри до податкових, соціальних чи антикорупційних реформ. Використовується мова ворожнечі, підміна понять, розповсюдження «викриттів» нібито корумпованих чиновників, що дискредитує державну політику загалом.

4. Атаки на банківську систему. У періоди загострення ситуації на фронті поширюються повідомлення про нібито банкрутство великих банків, недоступність рахунків, блокування платіжних систем тощо. Це викликає недовіру до фінансової системи та загрожує її стабільності.

5. Знецінення міжнародної підтримки. Ворожі наративи часто зосереджені на тому, щоб переконати українців, що міжнародна допомога є неефективною або корумпованою, а також що донори втомилися від війни. Це підриває соціальний оптимізм і інвестиційну довіру.

6. Економічна деморалізація через соцмережі. Поширення негативних сценаріїв («усе марно», «економіка не витримає», «Захід зрадить») формує тривожні настрої в суспільстві, демотивує підприємців, інвесторів і сприяє емоційній нестабільності.

Особливу увагу в дослідженнях OSTIN приділено аналізу методів протидії деструктивним інформаційним впливам, зокрема через застосування технологій штучного інтелекту для моніторингу інформаційного простору, розпізнавання фейків та швидкого реагування на ворожі вкиди. Це забезпечує ефективне інструментальне підґрунтя для державних структур. У сфері економічної безпеки OSTIN-дослідження також пропонують моделі підвищення стійкості до інформаційних шоків через створення комунікаційних стратегій для бізнесу, фінансових інституцій та органів влади. Одним із підходів є розвиток стратегічних наративів, здатних нейтралізувати паніку та поширення деструктивних наративів.

Крім цього, OSTIN-дослідження відіграють важливу роль у формуванні державної політики в умовах війни, надаючи урядовим структурам і силовим відомствам науково обґрунтовані рекомендації щодо підвищення інформаційної стійкості суспільства та економіки. На основі цих рекомендацій розробляються як оперативні заходи, так і довгострокові стратегії.

Отже, можемо зробити висновок, що OSTIN-дослідження є не лише джерелом глибокої аналітики, а й потужним інструментом формування відповідей на інформаційно-економічні виклики сучасності. Їх роль у забезпеченні національної безпеки України постійно зростає, що вимагає подальшого розвитку наукової бази та залучення експертного середовища до процесу ухвалення стратегічних рішень.

---

1. Розвідка на основі відкритих джерел – OSTIN. Вікіпеція. URL: https://uk.wikipedia.org/wiki

2. Економічна аналітика в бізнесі: навчальний посібник / [О.С. Гринькевич, С.О. Матковський, А.В. Сидорова та ін.] ; за ред. О.С. Гринькевич, С.О. Матковського, А.В. Сидорової, Н.С. Струк. Львів : ЛНУ ім. Івана Франка, 2022. – 480 с.

3. Минько О. В. Використання технологій OSINT для отримання розвідувальної інформації / О. В. Минько, О. Ю. Іохов, В. Т. Оленченко, К. В. Власов. Системи управління, навігації та зв'язку. 2016. Вип. 4. С. 81-84.

Шевчук Віктор,
доктор юридичних наук, професор,
заслужений юрист України,
завідувач кафедри криміналістики
(Національний юридичний університет
імені Ярослава Мудрого),
головний науковий співробітник
(НДІ вивчення проблем злочинності
імені академіка В. В. Сташиса НАПрН України)

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В OSINT ЯК НАПРЯМ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РОЗСЛІДУВАННЯ ВОЄННИХ ЗЛОЧИНІВ

В умовах гібридних конфліктів і збройної агресії проти України особливої актуальності набувають проблеми виявлення, документування та розслідування воєнних злочинів [3, с. 76]. Підвищення ефективності розслідування таких злочинів потребує не лише високої кваліфікації практичних працівників, які здійснюють досудове розслідування воєнних злочинів в Україні, а й передбачає застосування інноваційних підходів до збору доказової бази. Одним із ключових напрямів підвищення ефективності такої роботи є використання OSINT (open-source intelligence) – розвідки на основі відкритих джерел [6; 7].

Разом із цим, практика показує, що традиційні методи OSINT мають обмеження – значний обсяг інформації, її динамічність та складність перевірки автентичності вимагають нових технологічних рішень. Саме в цьому контексті штучний інтелект (ШІ) відкриває нові можливості для підвищення ефективності збору, аналізу, дослідження, верифікації та структурування великих обсягів відкритої інформації. Відтак, актуальним напрямом досліджень у цій сфері є комплексне вивчення та аналіз потенціалу використання ШІ в OSINT як інструменту підвищення ефективності розслідування воєнних злочинів.

Штучний інтелект стає революційним інструментом у сфері OSINT. Його здатність обробляти великі обсяги даних, аналізувати складні інформаційні структури та знаходити приховані зв’язки значно змінює підхід до розслідувань загалом і зокрема до розслі-

дування воєнних злочинів [4, с. 12-46]. Практика показує, що використання ШІ дозволяє зробити OSINT більш ефективним і точним і суттєво підвищити ефективність таких розслідувань [1, с. 135-140].

OSINT охоплює збирання, аналіз та інтерпретацію інформації з публічно доступних джерел, таких як інтернет-сайти, соціальні мережі, відкриті бази даних, публічні реєстри, ЗМІ, форуми, геолокаційні сервіси тощо. Основними перевагами є швидкість доступу, об'єм даних та актуальність інформації. У криміналістиці OSINT використовується для: ідентифікації осіб та об'єктів; відстеження цифрового сліду підозрюваних; аналізу зв'язків між учасниками подій; збору додаткових доказів; виявлення аномалій або ризиків.

Штучний інтелект відіграє важливу роль в обробці відкритих даних. Технології штучного інтелекту значно розширюють межі OSINT-аналізу. Серед ключових можливостей ШІ, що застосовуються у правоохоронній сфері, можна виділити: 1) НЛП (Natural Language Processing) – аналіз текстів з відкритих джерел, виявлення ключових слів, тем, емоційних тонів; 2) розпізнавання зображень та відео – ідентифікація осіб, автомобілів, об'єктів на фото та відео (наприклад, із камер спостереження або соціальних мереж); 3) обробка Big Data – ефективне фільтрування великих обсягів інформації; 4) автоматизоване створення звітів – побудова зв'язків, тимчасових ліній, географічних карт, якісна візуалізація даних; 5) прогнозна аналітика – виявлення закономірностей поведінки, тенденцій, можливих сценаріїв розвитку подій та ін.

Застосування ШІ в діяльності слідчого, прокурора та інших субєктів під час розслідування воєнних злочинів має свої особливості. Інтеграція ШІ в OSINT-системи може суттєво скоротити час на первинне збирання інформації та підвищити її релевантність. Це проявляється в тому, що: AI може автоматично здійснювати моніторинг соціальних мереж за ключовими словами; класифікувати інформацію за рівнем довіри; виявляти зв'язки між особами за непрямими ознаками; формувати аналітичні досьє. Наприклад, при розслідуванні воєнних злочинів ШІ здатен виявити мережу пов'язаних між собою акаунтів на різних платформах, які вказують на координовану діяльність окремих керівників та вищого воєнного керівництва країни-агресора, що дає змогу збирати доказову базу вчинення таких міжнародних воєнних злочинів.

Роль використання ШІ в OSINT під час розслідування воєнних злочинів охоплює збирання, аналіз і верифікацію інформації з відкритих джерел: соцмереж, публічних баз даних, супутникових знімків, новинних сайтів, відеоархівів тощо. У контексті воєнних злочинів OSINT виконує функції:фіксації фактів порушення МГП (наприклад, обстрілів цивільної інфраструктури); ідентифікації підрозділів чи осіб, які вчинили такі злочини; встановлення геолокації подій; підтвердження послідовності подій у часі.

Значення використання ШІ у зборі та аналізі OSINT-даних полягає в тому, що такі технології застосовуються на всіх етапах роботи з OSINT, зокрема:

1. *Автоматизоване збирання інформації*: **а) парсери та краулери,** які за допомогою NLP та ML відбирають релевантний контент; б) виявлення нових публікацій за ключовими словами, геомітками або зображеннями);

2. *Аналіз мультимедійних матеріалів*: **а) розпізнавання облич і номерів** (Facial & License Plate Recognition) у фото та відео; б) **розпізнавання об'єктів та дій** (наприклад, запуск ракети, присутність військової техніки); в) **геолокація зображень** – ШІ аналізує ландшафт, архітектуру, погоду для встановлення місця зйомки.

3. *Аналіз тексту*: **а)** інструменти **NLP** (Natural Language Processing) аналізують свідчення, коментарі, дописи; б) виявлення намірів, емоційної тональності, джерел фейкової інформації.

4. *Хронологізація подій*: **а)** ШІ допомагає синхронізувати відео, повідомлення і дані GPS для точного встановлення послідовності подій; б) аналіз соціальних мереж та ін.

Як приклади ефективного практичного застосування використання ШІ у зборі та аналізі OSINT-даних можна назвати такі: а) ***Bellingcat*** - використовує алгоритми ШІ для перевірки відео з полів бою, встановлення геолокації та ідентифікації підозрюваних у воєнних злочинах; б) ***Yale Humanitarian Research Lab*** - застосовує супутникові знімки та нейронні мережі для фіксації знищених цивільних об'єктів; в) ***українські OSINT-групи***, які створюють ботів для ідентифікації окупаційних військ у TikTok, Telegram та VK та ін.

Вбачається, що перевагою OSINT з використанням технологій ШІ є широта охоплення інформації про воєнні злочини в Україні, а також можливість оперативного доступу та відкритість дже-

рел, що має важливе значення для збору доказів [2, с.147]. Разом з тим, слід враховувати обмеження, пов'язані з аутентифікацією, маніпулятивністю контенту, а також із необхідністю структурованого аналізу отриманої інформації та іншими проблемами та складнощами у процесі збирання доказів та документування таких злочинів.

З огляду на викладене, варто зауважити, що за таких умов штучний інтелект стає ключовим інструментом у трансформації OSINT як джерела цифрових доказів у розслідуванні воєнних злочинів. Його ефективність залежить від якості алгоритмів, доступу до відкритих джерел та юридичного оформлення зібраної інформації. В умовах сучасної війни ШІ-інструменти стають не лише технічним засобом, але й фактором забезпечення справедливості та притягнення злочинців до відповідальності.

Щодо перспектив та активізації можливостей і потенціалу використання ШІ в OSINT як інструменту підвищення ефективності розслідування воєнних злочинів необхідно зауважити наступне. У контексті цифровізації кримінального процесу, впровадження ШІ в OSINT може стати невід'ємною частиною криміналістичного інструментарію. Для цього можна запропонувати: розробити державну концепцію цифрового OSINT у діяльності органів досудового розслідування; створити національні AI-платформи для розвідки з відкритих джерел, з урахуванням української мови та правового поля; запровадити етичні стандарти застосування ШІ в правозастосовній практиці; підвищити цифрову грамотність слідчих і криміналістів, у т.ч. через спеціалізовані тренінги з OSINT та AI.

Таким чином, застосування технологій штучного інтелекту в OSINT відкриває нові горизонти для розслідування воєнних злочинів, роблячи цей процес більш оперативним, точним і технологічно оснащеним. У цих умовах використання відкритих джерел інформації (OSINT) стає важливою складовою криміналістичного забезпечення досудового розслідування воєнних злочинів.

Використання ШІ дозволяє якісно змінити можливості OSINT, зокрема щодо обробки великих обсягів інформації, автоматизації рутинних завдань та виявлення прихованих зв'язків і формування доказової бази таких злочинів та підвищення ефективності їх розслідування та у майбутньому судового розгляду. Водночас, необхідно забезпечити належне правове, етичне й процесуальне

регулювання використання таких даних. У майбутньому інтеграція ШІ в OSINT стане невід'ємною частиною цифрової трансформації криміналістики, кримінального процесу та міжнародного правосуддя.

---

1. Baltrūnienė Ju., Shevchuk V. (2022). Artificial intelligence technologies in law enforcement and justice: Ukrainian and European experience. *Цифрова трансформація кримінального провадження в умовах воєнного стану*: матеріали круглого столу (м. Харків, 23 груд. 2022 р.): електрон. наук. вид.; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України. Харків: Право, 2022. С.135-140.

2. Kaplina, O., Tumanyants, A., Krytska, I., & Verhoglyad-Gerasymenko, O. (2023). Application of artificial intelligence systems in criminal procedure: Key areas, basic legal principles and problems of correlation with fundamental human rights. *Access to Justice in Eastern Europe*, 6(3), 147-166.

3. Konovalova V.O., Shevchuk V.M. (2023). Digital criminalistics as a strategic direction of formation of criminalistic knowledge. *Advanced discoveries of modern science: experience, approaches and innovations*: collection of scientific papers III International Scientific and Theoretical Conference, January 20, 2023. Amsterdam: European Scientific Platform. Pp. 73-77.

4. Матулєне С., Шевчук В., Балтрунене Ю. (2023). Штучний інтелект в діяльності органів правопорядку та юстиції: український та європейський досвід. *Теорія та практика судової експертизи і криміналістики.* Вип. 4 (29). 2023. С.12-46.

5. Шевчук В. М. (2024). Роль технологій штучного інтелекту у правоохоронній діяльності та забезпеченні безпеки і обороноздатності України. *Юридичний науковий електронний журнал.* № 6. 2024. С. 356 – 361.

6. Штучний інтелект в OSINT: Як покращити розслідування у 2024 році | InfoLightUA https://infolight.in.ua/2024/12/01/shtuchnyj-intelekt-v-osint-yak-pokrashhyty-rozsliduvannya-u-2024-rotsi/

7. OSINT AI: Як Оптимізувати Своє Розслідування у 2025 році? – Molfar https://molfar.com/blog/osint-ai-yak-optymizuvaty-svoe-rozsliduvannya-u-2024-roci

Шукалович Тетяна,
здобувач вищої освіти
(Національна академія Служби безпеки України)
Науковий керівник:
Жевелєва Ірина,
кандидат юридичних наук, доцент
(Національна академія Служби безпеки України)

ВИКОРИСТАННЯ OSINT-ІНСТРУМЕНТІВ У НАЦІОНАЛЬНОМУ АГЕНТСТВІ УКРАЇНИ З ПИТАНЬ ВИЯВЛЕННЯ, РОЗШУКУ ТА УПРАВЛІННЯ АКТИВАМИ, ОДЕРЖАНИМИ ВІД КОРУПЦІЙНИХ ТА ІНШИХ ЗЛОЧИНІВ

У XXI столітті розвідка на основі відкритих джерел (OSINT) є одним з основних засобів пошуку інформації не тільки у приватних компаніях, але й в державних установах. Розвідка на основі відкритих джерел зародилась у 1941 році із створенням Служби закордонних трансляцій у США (Foreign Broadcast Monitoring Service – FBMS) [1]. OSINT – це технологія добування військової, політичної, економічної та іншої інформації, що передбачає отримання даних з відкритих джерел (публічно чи комерційно доступних), їх обробку, аналіз та поширення для підтримки управлінських рішень у певних галузях [2]. У напрямку наукових досліджень OSINT-технологій працювали такі дослідники, як Демедюк С., Кіреєва О., Бурба В., Орел О., Щербань Д.тощо.

Одним з ключових інструментів, який використовують працівники Національного агенства України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів, є розвідка з відкритих джерел (Open Source Intelligence, OSINT). Фахівці АРМА на постійній основі удосконалюють навички використання OSINT-технологій у своїй організації, що дозволяє отримувати об'єктивну та повну інформацію в певному обсязі, так як схеми злочинів можуть змінюватись [3].

Працівники АРМА використовують безліч джерел інформації, в тому числі, – державні реєстри, соціальні мережі, блоги, новинні сайти, пошукові системи тощо. Також використовуються спеціальні інструменти для збору інформації, такі як сканери веб-

сайтів та соціальних мереж, які надають змогу в автоматизованому режимі переглядати затребувану інформацію.

Використання OSINT-технологій є ефективним інструментом збору, аналізу та систематизації інформації, що дозволяє отримувати доступ до великої кількості даних з відкритих джерел [3].

OSINT також включає в себе аналіз отриманої інформації. Одним з головних аспектів є уміння проводити ретельний пошук та аналіз зібраної інформації. В роботі з OSINT-технологіями потрібно розрізняти важливу інформацію від менш важливої або такої, що має ознаки дискредитованої. Проаналізувавши відомості, зібрані з різних релевантних джерел, фахівці АРМА отримують більш повну картину щодо активів одержаними від корупційних та інших злочинів.

Крім того, OSINT допомагає виявити зв'язки між різними людьми, компаніями та організаціями, що можуть мати важливе значення для проведення розслідування. Використання таких поширених джерел, як соціальні мережі, форуми та блоги допомагає виявити зв'язки між особами та організаціями, які можуть мати спільні інтереси або бути пов'язаними з певними злочинними діями [3].

Національним агенством України з питань виявлення, розшуку та управління активами налагоджено співпрацю з українськими та міжнародними ресурсами, які надають послуги у сфері збору інформації про корпоративну структуру, майновий стан юридичних та фізичних осіб, визначення місцезнаходження активів тощо. До таких ресурсів належать: YouControl, RuAssets, Orbis, Sayari, Maltego, Hunchly, ArcGis, деякі з них використовуються на платній основі, доступ до окремих наданий за фінансової підтримки міжнародних організацій в межах взаємодії [4].

---

1. Бурба В.В. Організаційно-правові засади використання розвідки з відкритих джерел інформації (OSINT) в діяльності розвідувальних служб європейських країн. *Юридичний бюлетень*, 2019. № 11. С. 11-19.
2. Н.В. Жмур. Історія становлення та сучасний стан технології пошуку інформації OSINT. *Юридичний вісник*, 2022. № 3 (64). С. 95-101.
3. Як працює OSINT-розвідка у сфері розшуку незаконних активів? URL: https://arma.gov.ua/news/typical/yak-pratsyue-osint-rozvidka-u-sferi-rozshuku-nezakonnih-aktiviv (дата звернення: 21.04.2025).
4. Джерела одержання інформації, до яких має доступ АРМА з метою виявлення та розшуку активів та автоматизація процесів. URL: https://arma.gov.ua/dostup_do_informacii (дата звернення: 21.04.2025).

Юрх Наталія,
співробітник
(Національна академія
Служби безпеки України)

OSINT-ДОСЛІДЖЕННЯ ЯК ІНСТРУМЕНТ ВИЯВЛЕННЯ, ДОКУМЕНТУВАННЯ ТА РОЗСЛІДУВАННЯ ВОЄННИХ ЗЛОЧИНІВ: МАНІПУЛЯЦІЯ НЕПОВНОЛІТНІМИ ЧЕРЕЗ ЦИФРОВІ ПЛАТФОРМИ

Російські спеціальні служби, зокрема Федеральна служба безпеки (ФСБ) та Головне розвідувальне управління (ГРУ), у межах реалізації елементів гібридної агресії проти України, активно застосовують інструменти цифрового впливу, серед яких домінуючу роль відіграє месенджер Telegram. Аналіз зібраних даних свідчить про цілеспрямоване використання цієї платформи для інформаційно-психологічного впливу на неповнолітніх громадян України, зокрема з метою їх вербування до вчинення деструктивних дій.

До типових прикладів таких дій належить організація підпалів транспортних засобів, що належать військовослужбовцям Збройних Сил України, а також будівель територіальних центрів комплектування (ТЦК). Відповідна діяльність здійснюється у форматі цифрово-маскованої взаємодії: через Telegram-ботів або анонімні канали особам пропонуються грошові винагороди за виконання протиправних завдань, що супроводжується докладною інструкцією щодо способу виконання та засобів маскування.

Але месенджер Telegram не єдина платформа, яка несе загрозу для неповнолітніх.

Цифрові платформи, зокрема Discord та Steam, все частіше використовуються не лише для комунікації чи розваг, а й у цілях деструктивного психологічного впливу на молодь. В умовах гібридної війни, що триває в Україні, такі платформи можуть бути використані ворожими структурами для поширення деструктивного контенту, координації флешмобів, формування субкультур та нав'язування ідеологічних установок.

Це можливо реалізувати шляхом створення закритих чатів і каналів, де поширюється контент, що формує антидержавні або

проросійські наративи; організацію флешмобів або акцій протесту з залученням неповнолітніх, часто без усвідомлення ними повної суті того, в чому вони беруть участь; поширення чуток, фейкових новин, відео, мемів, спрямованих на підрив довіри до державних інституцій, ЗСУ, волонтерів тощо; мобілізації емоційно вразливих груп (діти, підлітки) для участі в деструктивній діяльності – від масових бійок до актів вандалізму або підпалів.

У лютому-березні 2023 року в українських містах (Харків, Київ, Одеса та інші) фіксувалися масові скупчення підлітків, учасників так званої субкультури «Редан». Вона прийшла з Росії через платформи Discord, Telegram та Steam. Молодь кооперувалась у закритих чатах, створювала ігрові команди на Steam, використовуючи ігрову ідентичність як прикриття для координації дій у реальному житті. Учасники зустрічались у громадських місцях для проведення бійок, організованих нібито в межах субкультурного протистояння. Як зазначали у Національній поліції, координування цих зібрань здійснювалося з-за кордону (зокрема з рф), що вказує на чіткий ознаковий характер інформаційної атаки через молодь.

Зазначені дії є складовою широкомасштабної дезінформаційної кампанії, спрямованої на створення хибного уявлення про наявність значного внутрішнього спротиву мобілізаційним заходам в Україні. Таким чином, противник прагне сформувати ілюзорну картину соціального розколу в українському суспільстві, водночас дискредитуючи державні інституції та підриваючи рівень довіри до сектору національної безпеки та оборони.

Такі дії мають ознаки інформаційно-психологічної операції в умовах збройного конфлікту та, відповідно до норм міжнародного гуманітарного права, можуть розглядатися як воєнні злочини, особливо у випадках залучення неповнолітніх осіб до виконання вказаних завдань.

Для виявлення та документування подібних дій використовуються OSINT-інструменти, що дозволяють здійснити:

– аналіз Telegram-ботів та каналів;

– пошук відеофайлів підпалів та геолокація, за допомогою ресурсів: InVID, Google Lens, YouTube DataViewer;

– ідентифікація платників та фінансових слідів, за допомогою BTCscan, Blockchair;

– побудова соціальних графів злочинної діяльності, використовуючи Maltego, Lampyre, Spiderfoot;

– перевірка цифрових акаунтів за допомогою: Sherlock, Social Analyzer, CheckUsernames.

Висновок. Ці події свідчать про те, що цифрові платформи стають полем бойових дій нового типу. Неповнолітні – одна з найбільш вразливих груп, які потребують захисту не лише з боку держави, а й родини, школи, суспільства. Telegram, завдяки своїй архітектурі, залишається основною платформою вербування, однак використання таких платформ як Discord і Steam в інформаційно-психологічних операціях є додатковим викликом для кібербезпеки держави, особливо в умовах війни. Платформи Discord, Steam та Telegram можуть і повинні бути об'єктами системного моніторингу в межах кібербезпеки та протидії тероризму. Крім того бажано розробити міжвідомчі методики OSINT-розслідувань для роботи з Telegram та ігровими платформами.

OSINT-методи є унікальним інструментом для цифрової фіксації фактів підбурювання до вчинення актів насильства проти військових цілей. Інформація, зібрана за допомогою технології OSINT, може бути юридично релевантною під час розслідувань воєнних злочинів, у т.ч. для Міжнародного кримінального суду.

OSINT дає змогу не лише виявити цифрові сліди координації диверсійних дій, але й створити доказову базу для міжнародних органів правосуддя.

---

1. Rome Statute of the International Criminal Court, Article 8. URL: https://www.law.cornell.edu/gender-justice/resource/rome_statute_of_ the_international_ criminal_court_article_8 (дата звернення: 22.04.2025).

2. «Редан» серед молоді: ІПСО росії з використанням підлітків. URL: https://vseosvita.ua/c/news/post/84570 (дата звернення: 22.04.2025).

3. IntelTechniques. URL: https://inteltechniques.com/links.html (дата звернення: 22.04.2025).

4. Інструменти мережевої розвідки. URL: https://hackyourmom.com/kibervijna/zbir-informacziyi-pro-suprotyvnyka/osint-akademiya/instrumenty-merezhevoyi-rozvidky (дата звернення: 22.04.2025).

НАУКОВЕ ВИДАННЯ

РОЛЬ OSINT-ДОСЛІДЖЕНЬ У ПІДВИЩЕННІ РІВНЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ :

Матеріали круглого столу

7 травня 2025 року

Укладач
І. О. Ревак

Макетування
Андрій Радченко

Зам № 32-25.

Львівський державний університет внутрішніх справ
Україна, 79007, м. Львів, вул. Городоцька, 26.

Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції
ДК № 2541 від 26 червня 2006 р.