

Міністерство внутрішніх справ України  
Львівський державний університет внутрішніх справ

# РОЛЬ OSINT-ДОСЛІДЖЕНЬ У ПІДВИЩЕННІ РІВНЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

*Матеріали Всеукраїнської  
науково-практичної конференції*

*7 травня 2026 року*

Львів  
2026

Рекомендовано до розміщення в електронних сервісах ЛьвДУВС  
Вченою радою навчально-наукового інституту управління, психології та безпеки  
Львівського державного університету внутрішніх справ  
(протокол від 11 травня 2026 р. № 9)

**Роль OSINT-досліджень у підвищенні рівня національної безпеки України :**  
Р 68 матеріали Всеукраїнської науково-практичної конференції (м. Львів, 7 травня  
2026 р.) / укладачі: О. І. Пацула, І. О. Ревак. Львів : ЛьвДУВС, 2026. 244 с.

**DOI <https://doi.org/10.5281/zenodo.20718088>**

У збірнику вміщено матеріали науково-практичного заходу, присвячені актуальним проблемам застосування розвідки на основі відкритих джерел (OSINT) у системі забезпечення національної безпеки України. Тези доповідей відображають результати наукових досліджень, спрямованих на висвітлення теоретичних і прикладних аспектів використання OSINT в умовах гібридних загроз, збройної агресії та інформаційного протистояння.

У виданні розкрито потенціал OSINT як інструменту безпекової аналітики, протидії дезінформації, виявлення ризиків і підтримки управлінських рішень.

Видання адресоване науковцям, аналітикам, фахівцям сектору безпеки і оборони, працівникам правоохоронних органів, а також усім, хто цікавиться проблематикою OSINT-досліджень.

The collection contains materials of a scientific and practical event devoted to current issues of applying Open Source Intelligence (OSINT) within the system of ensuring the national security of Ukraine. The published abstracts reflect the results of scientific research focused on the theoretical and practical aspects of OSINT use under conditions of hybrid threats, armed aggression, and information confrontation.

The publication highlights the potential of OSINT as a tool for security analytics, countering disinformation, identifying risks, and supporting decision-making processes.

The edition is intended for researchers, analysts, security and defense professionals, law enforcement officers, as well as everyone interested in OSINT studies.

Опубліковано мовою оригіналу та в авторській редакції.  
Відповідальність за зміст викладеного матеріалу несуть автори

**УДК 351.746.5:004.9:343.9(477)**

© Львівський державний університет  
внутрішніх справ, 2026

DOI <https://doi.org/10.5281/zenodo.20718088>

## ЗМІСТ

ВСТУПНЕ СЛОВО .....	9
<b>Batiuk O. V.</b> THE ROLE OF OSINT RESEARCH IN ENHANCING CRITICAL INFRASTRUCTURE SECURITY .....	11
<b>Downing D., Johns E.</b> CONTEXT AND CONNECTIONS: HOW OSINT STRENGTHENS SANCTIONS COMPLIANCE IN SUPPORT OF UKRAINE'S NATIONAL SECURITY THROUGH NETWORK ANALYSIS AND CONTEXTUAL INVESTIGATION .....	13
<b>Kudla M.-A. Ю., Bylen D.</b> THE ROLE OF AI IN STRENGTHENING INTELLIGENCE ANALYSIS IN MODERN SECURITY ENVIRONMENTS .....	14
<b>Ангеленюк А.-М. Ю., Бреславець В. В., Бура А. В.</b> ВИКОРИСТАННЯ ВІДКРИТИХ ДЖЕРЕЛ ДЛЯ ВИЯВЛЕННЯ НЕЗАКОННИХ ФІНАНСОВИХ СХЕМ .....	17
<b>Андросович Л. Г.</b> РОЛЬ OSINT У ВИЯВЛЕННІ ТА РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У ФІНАНСОВІЙ СИСТЕМІ УКРАЇНИ .....	19
<b>Березовський Є. О., Кісіль М. Л.</b> OSINT ЯК ДОКАЗОВА БАЗА У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ: ПРАВОВІ ТА ПРАКТИЧНІ АСПЕКТИ .....	23
<b>Блавацька Н. М.</b> ІІІ-ТЕХНОЛОГІЇ ТРАНСКРИБУВАННЯ ВІДЕО В СИСТЕМІ OSINT-ДОСЛІДЖЕНЬ .....	25
<b>Бондар В. С.</b> ЗАСТОСУВАННЯ OSINT-ТЕХНОЛОГІЙ У ДОКУМЕНТУВАННІ ТА РОЗСЛІДУВАННІ ОКРЕМИХ ВИДІВ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПІДСЛІДНИХ СЛІДЧИМ ОРГАНІВ БЕЗПЕКИ .....	27
<b>Бочаров С. В.</b> ВИКОРИСТАННЯ OSINT В ОПЕРАТИВНО-РОЗШУКОВІЙ ДІЯЛЬНОСТІ .....	29
<b>Бутко Р. Ю.</b> РОЛЬ КРИМІНАЛЬНОГО АНАЛІЗУ В РОЗВИТКУ ПОЛІЦЕЙСЬКОЇ АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ .....	32
<b>Винник С. С.</b> ІНФОРМАЦІЙНО-АНАЛІТИЧНІ МЕХАНІЗМИ ФІНАНСОВОГО МОНИТОРИНГУ БАНКІВ У ЗАБЕЗПЕЧЕННІ ДОТРИМАННЯ САНКЦІЙ .....	35
<b>Візничак І.-Д. В., Новаковська У. Ю.</b> ІНТЕГРАЦІЯ OSINT У ДІЯЛЬНІСТЬ ПРАВООХОРОННИХ ОРГАНІВ УКРАЇНИ .....	38
<b>Волобоєва З. О., Габорець О. А.</b> OSINT ЯК ЗАСІБ ВИЯВЛЕННЯ ТА ФІКСАЦІЇ ЗЛОЧИНІВ АГРЕСІЇ ПРОТИ УКРАЇНИ .....	40
<b>Воропаєв Д. В., Коцюба І. Ю.</b> ЦИФРОВА АНОНІМНІСТЬ У СУЧАСНОСТІ: ВИКЛИК ДЛЯ КІБЕРБЕЗПЕКИ ЧИ ОСНОВА ЦИФРОВИХ ПРАВ .....	43
<b>Гладій Б. В., Крючко К. С., Ревак І. О.</b> ЦИФРОВА ІНДИФІКАЦІЯ ВІЙСЬКОВИХ ЗЛОЧИНЦІВ ЗАСОБАМИ OSINT .....	45
<b>Горняков І. Д., Кривизюк Л. П.</b> ОСОБЛИВОСТІ ВИКОРИСТАННЯ МЕТОДІВ OSINT У КОГНІТИВНІЙ ВІЙНІ .....	48

<b>Грезіна О. М., Пядишев В. Г.</b> ІНТЕЛЕКТУАЛІЗАЦІЯ OSINT: ВІД ПОШУКУ ІНФОРМАЦІЇ ДО ПРОГНОЗУВАННЯ ЗАГРОЗ .....	50
<b>Гриньків О. О.</b> OSINT: МОЖЛИВОСТІ ТА ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ В НАЦІОНАЛЬНІЙ ГВАРДІЇ УКРАЇНИ.....	52
<b>Грінченко В. В., Дегалюк М. А.</b> OSINT-ДОСЛІДЖЕННЯ ЯК ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ.....	55
<b>Громяк С. І.</b> СТРУКТУРНІ ЧИННИКИ ВАРТОСТІ ТА ФІНАНСОВОЇ ЕФЕКТИВНОСТІ OSINT-СИСТЕМИ У СФЕРІ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ .....	57
<b>Гуцуляк Ю. В.</b> ОСОБЛИВОСТІ ВИКОРИСТАННЯ ФАКТИЧНИХ ДАНИХ, ОТРИМАНИХ ЗА ДОПОМОГОЮ OSINT-ТЕХНОЛОГІЙ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ (ЗА РЕЗУЛЬТАТАМИ АНАЛІЗУ ВОРОЖИХ TELEGRAM-КАНАЛІВ).....	61
<b>Гуцуляк Ю. В., Гонта С. Ю.</b> ЗАСТОСУВАННЯ МЕТОДУ OSINT ДЛЯ ЗБОРУ ДОКАЗІВ У ВОЄННИХ КОНФЛІКТАХ.....	63
<b>Деркач Д., Підхомний О. М.</b> ІНТЕГРАЦІЯ ІНСТРУМЕНТІВ ШІ ТА OSINT ДЛЯ МІНІМІЗАЦІЇ БЕЗПЕКОВИХ ЗАГРОЗ У СФЕРІ КОРПОРАТИВНИХ ФІНАНСІВ .....	66
<b>Дмитрук П. А., Ревак І. О.</b> РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ У ВДОСКОНАЛЕННІ OSINT-ІНСТРУМЕНТАРІЮ В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ .....	68
<b>Д'яков А. В.</b> ІНТЕГРАЦІЯ OSINT ТА ГЕОІНФОРМАЦІЙНОГО АНАЛІЗУ У ВЕРИФІКАЦІЇ ВОЄННИХ ЗЛОЧИНІВ .....	70
<b>Зоренко Д. С.</b> ВИКОРИСТАННЯ РЕКЛАМНИХ ІДЕНТИФІКАТОРІВ У КОНТЕКСТІ РОЗВІДКИ З ВІДКРИТИХ ДЖЕРЕЛ .....	73
<b>Іванишин М. І., Ленівий О. Ю.</b> ЗАСТОСУВАННЯ OSINT У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ ТА ЗАБЕЗПЕЧЕННІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ .....	76
<b>Іванченко А. О.</b> ІНТЕГРАЦІЯ OSINT У СИСТЕМУ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ .....	78
<b>Ігнат'єв Б. М.</b> ВПЛИВ ЦИФРОВОГО ВІДБИТКУ ПРОФІЛЮ ВЕБОГЛЯДАЧА НА КОНФІДЕНЦІЙНІСТЬ OSINT-АНАЛІТИКА .....	80
<b>Кіреєва О. С.</b> ТРАНСФОРМАЦІЯ OSINT-ДОСЛІДЖЕНЬ У ПАРАДИГМІ INTELLIGENCE-LED POLICING ДЛЯ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ.....	83
<b>Кісіль З. Р.</b> ІНСТРУМЕНТАРІЙ OSINT ЯК ЧИННИК ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ОПЕРАТИВНО-СЛУЖБОВОЇ ДІЯЛЬНОСТІ ПОЛІЦІЇ.....	86
<b>Кісіль Р.-В. В.</b> СТРАТЕГІЧНІ ТА ПРИКЛАДНІ АСПЕКТИ ЗАСТОСУВАННЯ ІНСТРУМЕНТАРІЮ OSINT У ПРОЦЕСУАЛЬНІЙ ДІЯЛЬНОСТІ НА ЕТАПІ ДОСУДОВОГО РОЗСЛІДУВАННЯ .....	88

<b>Колесников М. Є.</b> ВИЯВЛЕННЯ ОЗНАК ОБХОДУ САНКЦІЙ ІЗ ВИКОРИСТАННЯМ ВІРТУАЛЬНИХ АКТИВІВ ЗАСОБАМИ OSINT: ВІДКРИТІ ДЖЕРЕЛА ТА БЛОКЧЕЙН-ОГЛЯДАЧІ .....	90
<b>Коляда А. О., Прокопов С. О.</b> ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ІДЕНТИФІКАЦІЇ ТА РОЗШУКУ ОСІБ В УМОВАХ ВОЄННОГО СТАНУ МЕТОДАМИ OSINT-ТЕХНОЛОГІЙ .....	93
<b>Копитко М. І., Мойса Т. В.</b> OSINT-ДОСЛІДЖЕННЯ У СИСТЕМІ КОМПЛАЄНС-КОНТРОЛЮ НА ПІДПРИЄМСТВАХ.....	96
<b>Косяченко Є. О., Ришков Е. В.</b> АНАЛІТИЧНА ПІДТРИМКА ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ У СФЕРІ ПРОТИДІЇ ОРГАНІЗОВАНИЙ ЗЛОЧИННОСТІ ПІД ЧАС ВОЄННОГО СТАНУ .....	99
<b>Кудимов С. М., Жук О. В., Гунько Л. В.</b> OSINT ЯК СКЛАДОВА ПРОТИДІЇ НЕЛЕГАЛЬНІЙ ТОРГІВЛІ ТА ОБХОДУ САНКЦІЙ.....	102
<b>Кудінов В. А., Пакриш О. Є.</b> ІНТЕГРАЦІЯ МОЖЛИВОСТЕЙ OSINT У СИСТЕМУ ОПЕРАТИВНОГО ІНФОРМУВАННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ .....	105
<b>Кузьменко В. В., Кісіль М. Л.</b> ВИКОРИСТАННЯ OSINT-ТЕХНОЛОГІЙ У ПРОТИДІЇ КІБЕРЗАГРОЗАМ: ДОСВІД ПРАВООХОРОННИХ ОРГАНІВ УКРАЇНИ .....	108
<b>Ленівий О. Ю., Матала І. В.</b> OSINT-ДОСЛІДЖЕННЯ ЯК НАПРЯМ РОЗСЛІДУВАННЯ ВОЄННИХ ЗЛОЧИНІВ, СКОЄНИХ АРМІЄЮ АГРЕСОРА .....	110
<b>Лисенко Б. О., Шаповаленко Є. В.</b> АСПЕКТИ ФІКСАЦІЇ ШАХРАЙСТВ, ВЧИНЕНИХ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЙ DEEPFAKE ТА СИНТЕЗУ ГОЛОСУ ШТУЧНИМ ІНТЕЛЕКТОМ .....	112
<b>Ліва С. О., Огірко О. І.</b> OSINT: ЯК ОДНА ФОТОГРАФІЯ МОЖЕ РОЗКРИТИ ВСЮ ІНФОРМАЦІЮ ПРО ЛЮДИНУ .....	115
<b>Ліліченко Є. С., Зайченко В. В.</b> ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ ВІДКРИТОЇ РОЗВІДКИ У КНР .....	117
<b>Лісов О. С., Меншаков А. С.</b> МЕТОДИЧНІ АСПЕКТИ ІМПЛЕМЕНТАЦІЇ ШІ В СЛУЖБОВУ ДІЯЛЬНІСТЬ ДЛЯ ПОСИЛЕННЯ OSINT-СПРОМОЖНОСТЕЙ СУБ'ЄКТІВ РОЗВІДУВАЛЬНОГО СПІВТОВАРИСТВА.....	120
<b>Лукашук Ю. А.</b> ІНТЕЛЕКТУАЛІЗАЦІЯ OSINT-ДОСЛІДЖЕНЬ: РОЛЬ ГЛИБОКОГО НАВЧАННЯ У ЗАБЕЗПЕЧЕННІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ .....	122
<b>Лук'яненко С. М.</b> OSINT-ДОСЛІДЖЕННЯ: ОСОБЛИВОСТІ ВИКОРИСТАННЯ ПРОГРАМНИХ ПРОДУКТІВ ДЛЯ ЗБИРАННЯ ЦИФРОВИХ ДОКАЗІВ У КРИМІНАЛЬНИХ ПРОВАДЖЕННЯХ ЩОДО ВОЄННИХ ЗЛОЧИНІВ .....	125
<b>Манжсай О. В., Манжсай І. А.</b> СПЕЦИФІКА ВИЯВЛЕННЯ ЦИФРОВИХ СЛІДІВ НЕЗАКОННОГО ОБІГУ ПРЕКУРСОРІВ МЕТОДАМИ OSINT .....	129
<b>Мисик А. Б., Бурбела С. В.</b> МЕТОДИКА ОЦІНЮВАННЯ ОБСТАНОВКИ ШТАБОМ ПРИКОРДОННОГО ЗАГОНУ.....	132
<b>Михаліцька Н. Я., Яцик М. Р.</b> ІНТЕГРАЦІЯ OSINT-АНАЛІТИКИ ТА ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В УПРАВЛІННЯ ЛЮДСЬКИМ КАПІТАЛОМ В УМОВАХ КРИЗОВИХ ТРАНСФОРМАЦІЙ .....	135

<b>Мовчан А. В.</b> НАПРЯМИ ВИКОРИСТАННЯ OSINT У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ ТА ЗАБЕЗПЕЧЕННІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ .....	138
<b>Овдійчук Д. Е., Гуцуляк Ю. В.</b> ЗАСТОСУВАННЯ МЕТОДІВ OSINT У ДОСУДОВОМУ РОЗСЛІДУВАННІ.....	141
<b>Пацула О. І.</b> АНАЛІТИЧНИЙ ПОТЕНЦІАЛ ВІДКРИТИХ ДЖЕРЕЛ У ПРОТИДІЇ ФІНАНСОВИМ ПРАВОПОРУШЕННЯМ.....	144
<b>Перемибіда Д. О., Перемибіда І. В.</b> ВАЖЛИВІСТЬ ДОСЛІДЖЕННЯ ВІДКРИТИХ ДЖЕРЕЛ У КОНТЕКСТІ ВЖИТТЯ ЗАХОДІВ КОНТР-OSINT.....	146
<b>Пилипенко Є. О.</b> ЩОДО ВИКОРИСТАННЯ OSINT ПІД ЧАС РОЗШУКУ ВОЄННИХ ЗЛОЧИНЦІВ .....	148
<b>Підхомний О. М.</b> ТАКТИЧНІ ПРИЙОМИ ДОСЛІДЖЕННЯ СИСТЕМ ІЗ ЗАКРИТИМ ІНФОРМАЦІЙНИМ ПРОСТОРОМ .....	150
<b>Поляк А. Ю., Огірко О. І.</b> OSINT ЯК ЗАСІБ ЗБОРУ ДОКАЗОВОЇ ІНФОРМАЦІЇ У КРИМІНАЛЬНИХ РОЗСЛІДУВАННЯХ .....	152
<b>Попович К. Г.</b> ВИКОРИСТАННЯ OSINT (OPEN SOURCE INTELLIGENCE) У ВСТАНОВЛЕННІ ЮРИДИЧНО ЗНАЧУЩИХ ФАКТІВ ПРИ СПАДКУВАННІ В УМОВАХ ВОЄННОГО СТАНУ .....	154
<b>Прокопов С. О.</b> ДОСЛІДЖЕННЯ ЦИФРОВИХ ФОТО ТА ВІДЕО ЗА МЕТОДИКОЮ OSINT .....	156
<b>Проценко М. В., Галайко Н. В.</b> ЕТИКО-ПРАВОВІ РЕГУЛЮВАННЯ OSINT У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ.....	159
<b>Пряхіна Н. О., Пряхіна В. Є.</b> ІНТЕГРАЦІЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПРОЦЕСИ ВІДКРИТОЇ РОЗВІДКИ (OSINT) .....	161
<b>Радик В. В.</b> НАПРЯМИ ВИКОРИСТАННЯ OSINT У СИСТЕМІ САНКЦІЙНОГО КОНТРОЛЮ .....	163
<b>Ревак І. О.</b> РОЙОВИЙ ІНТЕЛЕКТ ЯК КОНЦЕПТУАЛЬНА ОСНОВА КОЛЕКТИВНИХ OSINT-РОЗСЛІДУВАНЬ.....	166
<b>Решетняков М. А., Гриньків О. О.</b> ІІІ ТА OSINT У СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ: ПЕРСПЕКТИВИ ЇХ РОЗВИТКУ ДЛЯ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ .....	168
<b>Рибка Д. М.</b> РОЛЬ АРІ У МАСШТАБУВАННІ ТА ВЕРИФІКАЦІЇ ДАНИХ В OSINT-ДОСЛІДЖЕННЯХ .....	170
<b>Рижков Е. В.</b> ПРИКЛАДНІ АСПЕКТИ ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМІ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ТА ВІДЕОАНАЛІТИКИ В ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ .....	172
<b>Руцишин Р. Р.</b> OSINT ЯК ІНСТРУМЕНТ ДОКУМЕНТУВАННЯ ВОЄННИХ ЗЛОЧИНІВ І ВЕРИФІКАЦІЇ ЦИФРОВИХ ДОКАЗІВ .....	176

<b>Ряшко О. В.</b> ВИКОРИСТАННЯ ВІДКРИТИХ ДЖЕРЕЛ ІНФОРМАЦІЇ OSINT ТА ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПОШУКУ БЕЗВІСТИ ЗНИКЛИХ ОСІБ ЗА ОСОБЛИВИХ ОБСТАВИН.....	179
<b>Савайда О. І., Фукал А. Д.</b> РОЛЬ OSINT-СПІЛЬНОТ У ЗАБЕЗПЕЧЕННІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ДОТРИМАННІ ПРАВ ЛЮДИНИ: ВЗАЄМОДІЯ ДЕРЖАВИ ТА ВОЛОНТЕРІВ.....	182
<b>Сашиуріна О.</b> ПСИХОЛОГІЧНІ АСПЕКТИ ВИКОРИСТАННЯ ВІДКРИТИХ ДЖЕРЕЛ ДЛЯ ПОШУКУ ТА АНАЛІЗУ ІНФОРМАЦІЇ В УМОВАХ ВОЄННОГО СТАНУ.....	185
<b>Світличний В. А., Вітвіцька К. Е.</b> МЕТОДОЛОГІЯ ІДЕНТИФІКАЦІЇ ЦИФРОВИХ ПРИМАНОК (HONEYTOKENS) У СИСТЕМІ ЗАХОДІВ КОНТР-OSINT.....	187
<b>Стеценко Я. В.</b> ВИКОРИСТАННЯ ІНСТРУМЕНТІВ OSINT-АНАЛІЗУ ДЛЯ ВИЯВЛЕННЯ ФЕЙКОВИХ ДОКУМЕНТІВ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ: ПОРУШЕННЯ СТАНДАРТІВ ДІЛОВОДСТВА ТА ЛІНГВІСТИЧНІ МАРКЕРИ.....	189
<b>Тищенко С. С.</b> РОЛЬ OSINT-ДОСЛІДЖЕНЬ У ВИЯВЛЕННІ, АНАЛІЗІ ТА ПРОТИДІЇ ПРОПАГАНДИ ТА ДЕЗІНФОРМАЦІЇ В УМОВАХ ВІЙНИ В УКРАЇНІ.....	192
<b>Токар П. Т., Кріцак І. В., Кобилев О. А.</b> OSINT І НИНІШНЯ РОСІЙСЬКО-УКРАЇНСЬКА ВІЙНА: ВІД НАУКОМЕТРІЇ ДО ПРАКТИЧНИХ АСПЕКТІВ РОЗСЛІДУВАННЯ ВОЄННИХ ЗЛОЧИНІВ.....	194
<b>Фігура В. О.,</b> ЗАСТОСУВАННЯ OSINT ДЛЯ ПОСИЛЕННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ МОЖЛИВОСТЕЙ ПЕРСПЕКТИВНОГО ПІДРОЗДІЛУ ОБРОБКИ ДАНИХ ПАСАЖИРІВ (PIU).....	204
<b>Форос Г. В., Калугін В. Ю.</b> КЛЮЧОВІ НАПРЯМИ ЗАСТОСУВАННЯ МЕТОДОЛОГІЇ OSINT У СФЕРІ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ.....	206
<b>Франчук В. І.</b> КОНЦЕПТУАЛЬНА МОДЕЛЬ OSINT ЯК ВИДУ БЕЗПЕКОВОЇ ДІЯЛЬНОСТІ.....	208
<b>Фуртес О. О., Кудимов С. М., Дорота А. С.</b> OSINT У РОЗКРИТТІ ВОЄННИХ ЗЛОЧИНІВ В УКРАЇНІ.....	211
<b>Хізанов О. Д., Моргун Н. С.</b> МІЖНАРОДНЕ СПІВРОБІТНИЦТВО У СФЕРІ КІБЕРЗАХИСТУ ТА НАЦІОНАЛЬНА БЕЗПЕКА УКРАЇНИ: ВИКОРИСТАННЯ МЕХАНІЗМІВ ЄВРОПЕЙСЬКОГО СОЮЗУ ДЛЯ РЕАГУВАННЯ НА МАСШТАБНІ КІБЕРАТАКИ.....	214
<b>Цмоць У. О.</b> ЗАСАДИ ПРАВОВОГО ТА ЕТИЧНОГО РЕГУЛЮВАННЯ КОЛЕКТИВНОЇ OSINT-ДІЯЛЬНОСТІ: МІЖ ЕФЕКТИВНІСТЮ ТА ЗАХИСТОМ ПРАВ ЛЮДИНИ.....	216
<b>Чаленко П. В.</b> МЕТОДОЛОГІЯ OSINT-РОЗСЛІДУВАННЯ ВОЄННИХ ЗЛОЧИНІВ: КЕЙС-АНАЛІЗ ПОДІЙ У ІЗЬОМСЬКОМУ ЛІСІ ІЗ ЗАСТОСУВАННЯМ ЦИФРОВИХ ІНСТРУМЕНТІВ ВЕРИФІКАЦІЇ ТА ГЕОЛОКАЦІЇ.....	219
<b>Чирук Б. Р., Калугін В. Ю.</b> OSINT ЯК ІНСТРУМЕНТ ВИЯВЛЕННЯ ТА ФІКСАЦІЇ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ: ПРИКЛАДНИЙ АСПЕКТ.....	223

<b>Чубенко А. Г.</b> РОЛЬ OSINT-FORENSICS У ПРОТИДІІ НЕЛЕГАЛЬНОМУ ОБІГУ КУЛЬТУРНИХ ЦІННОСТЕЙ ТА ЗАХИСТІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ .....	225
<b>Швець Д. В.</b> СТРАТЕГІЧНІ ПРІОРИТЕТИ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ OSINT У НАЦІОНАЛЬНУ ЕКОСИСТЕМУ КІБЕРБЕЗПЕКИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ .....	227
<b>Ширкунов О. Д., Фільченко С. В., Каптелян С. О.</b> ІНТЕГРАЦІЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В OSINT-МОНІТОРИНГ ЯК ЧИННИК ПОСИЛЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ .....	229
<b>Школьніков В. І.</b> АВТОМАТИЗАЦІЯ ЗБОРУ, ОБРОБКИ ТА АНАЛІЗУ ІНФОРМАЦІЇ З ВІДКРИТИХ ДЖЕРЕЛ ЗА ДОПОМОГОЮ ШІ-АГЕНТІВ .....	231
<b>Юрх Н. Г.</b> АНАЛІЗ РИЗИКІВ ВИКОРИСТАННЯ ХМАРНИХ ПЛАТФОРМ ДЛЯ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ У КОНТЕКСТІ OSINT-ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ ТА ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ .....	233
<b>Юрченко Р. В., Івахів О. С., Лібрук-Ліпкевич С. Я.</b> ВИКОРИСТАННЯ МЕТОДІВ OSINT У РОСІЙСЬКО-УКРАЇНСЬКІЙ КІБЕРПРОСТОРОВІЙ КОГНІТИВНІЙ ВІЙНІ: ОСОБЛИВОСТІ ТА ПРОТИДІЯ .....	235
<b>Ярема О. Г., Єсімов С. С.</b> ПИТАННЯ ВНЕСЕННЯ У НАВЧАЛЬНИЙ ПРОЦЕС ЗА СПЕЦІАЛЬНІСТЮ К9 «ПРАВООХОРОННА ДІЯЛЬНІСТЬ» ТЕХНОЛОГІЙ OSINT .....	238
<b>Ящур П. О., Моргун Н. С.</b> РОЛЬ ПІДРОЗДІЛІВ КІБЕРПОЛІЦІЇ ТА КРИМІНАЛЬНОГО АНАЛІЗУ У ВЗАЄМОДІЇ ЗІ СЛІДЧИМ ПІД ЧАС ДОСУДОВОГО РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВООПОРУШЕНЬ, ПОВ'ЯЗАНИХ ІЗ НЕЗАКОННИМ РУХОМ ФІНАНСОВИХ РЕСУРСІВ .....	241

**ШАНОВНІ КОЛЕГИ, ВИСОКОПОВАЖНІ УЧАСНИКИ  
ТА ГОСТІ КОНФЕРЕНЦІЇ!**

Від імені Львівського державного університету внутрішніх справ щиро вітаю вас на Всеукраїнській науково-практичній конференції «Роль OSINT-досліджень у підвищенні рівня національної безпеки України».

Сьогоднішній захід об'єднує провідних науковців, аналітиків, представників сектору безпеки і оборони, правоохоронних органів, а також експертів у сфері інформаційних технологій. Така міждисциплінарна взаємодія є не просто актуальною, а критично необхідною в умовах сучасних викликів, що постають перед нашою державою.

Російська збройна агресія проти України, гібридні загрози, інформаційні операції, кібератаки й інші форми впливу на державність і суспільство зумовлюють потребу в нових підходах до забезпечення національної безпеки. У цьому контексті особливого значення набувають OSINT-дослідження – інструмент, що дає змогу ефективно використовувати відкриті джерела інформації для виявлення, аналізу та попередження загроз.

Для нашого університету ця тематика не є новою чи випадковою. Львівський державний університет внутрішніх справ послідовно розвиває наукові й освітні напрями, пов'язані з інформаційною безпекою, аналітичною діяльністю та цифровими технологіями у правоохоронній сфері. Ми з гордістю можемо зазначити, що в університеті успішно функціонує науково-дослідна лабораторія OSINT-досліджень, яка стала важливим осередком генерації сучасних знань, інноваційних підходів і практичних рішень у сфері роботи з відкритими даними.

Діяльність лабораторії спрямована не лише на проведення фундаментальних і прикладних досліджень, а й на підготовку висококваліфікованих фахівців, здатних ефективно діяти в умовах інформаційного протистояння. Її напрацювання сьогодні використовуються в освітньому процесі, а також мають прикладне значення для практичних підрозділів.

Проведення цієї конференції є логічним продовженням нашої системної роботи. Важливо підкреслити, що наш університет проводить подібні науково-комунікаційні заходи не вперше. Ми послідовно утверджуємося як відкрита і постійна платформа для об'єднання зусиль науковців і практиків, для обміну досвідом, обговорення актуальних проблем та пошуку ефективних шляхів їх вирішення.

Саме в такому форматі виникають нові ідеї, формуються професійні спільноти та зміцнюється взаємодія між різними інституціями. Ми переконані, що лише через синергію науки і практики можливо досягти реальних результатів у сфері забезпечення національної безпеки.

Сьогодні OSINT перестає бути допоміжним інструментом і перетворюється на повноцінний напрям аналітичної діяльності, який активно використовується і на національному, і на міжнародному рівнях. Відкриті джерела інформації стають невичерпним ресурсом для отримання даних, однак водночас потребують високого рівня професійної підготовки для їхньої правильної інтерпретації, перевірки та застосування.

Саме тому надзвичайно важливою є підготовка фахівців нового покоління – аналітиків, які володіють сучасними цифровими інструментами, критичним мисленням і здатністю працювати з великими обсягами інформації. У цьому контексті роль закладів вищої освіти, зокрема нашого університету, є визначальною.

Ми прагнемо не лише реагувати на сучасні виклики, а й формувати порядок денний у сфері наукових досліджень і професійної підготовки. Саме тому подібні конференції є надзвичайно важливими – вони дають змогу окреслити ключові тенденції, визначити пріоритетні напрями розвитку та налагодити ефективну співпрацю між усіма зацікавленими сторонами.

Переконаний, що сьогоднішня конференція буде потужним майданчиком для змістовного діалогу, обміну ідеями та напрацювання практичних рекомендацій. Вірю, що результати ваших дискусій матимуть не лише наукову цінність, а й реальний вплив на підвищення ефективності діяльності органів сектору безпеки і оборони України.

Дозвольте також висловити щире подяку всім учасникам за інтерес до тематики конференції, за вашу активну позицію та готовність долучатися до спільної справи зміцнення національної безпеки нашої держави.

Бажаю всім плідної роботи, конструктивних дискусій, нових наукових здобутків і професійних звершень.

Слава Україні!

*Дмитро ШВЕЦЬ,  
ректор,  
доктор юридичних наук, професор,  
заслужений працівник освіти України,  
полковник поліції*

**Batiuk O. V.,**  
Doctor of Laws, Professor  
Leading Research Fellow  
Research Laboratory for Force Development  
and Operational Employment  
*(National Academy of the National Guard of Ukraine)*

## **THE ROLE OF OSINT RESEARCH IN ENHANCING CRITICAL INFRASTRUCTURE SECURITY**

The enhancement of critical infrastructure (CI) security is driven by a multifaceted set of modern challenges associated with the digitisation of society, the burgeoning volume of information and the transformation of national and information security threats. In the contemporary environment, critical infrastructure, encompassing energy, transport, communications, the financial sector and other strategic assets, has become a primary target for both cybercrime and hybrid attacks that integrate informational, technological and physical impacts. Consequently, the article asserts that the effective security of CI assets necessitates the practical implementation of Open Source Intelligence (OSINT), which is predicated on the collection, analysis and interpretation of publicly available information. Open sources include social networks, websites, news outlets, academic publications, state registries and other publicly accessible data, enabling the acquisition of substantial volumes of actionable intelligence without resorting to specialised intelligence collection methods. In our view, OSINT technologies play a pivotal role in identifying potential threats to critical infrastructure. Continuous monitoring of the information environment enables the detection of cyberattack preparations, the dissemination of malware and indicators of coordinated physical illicit activities. A significant advantage of OSINT lies in its capacity for early threat warning, allowing security stakeholders to respond promptly and mitigate risks. Current scholarly research indicates that companies and state entities frequently obtain information regarding potential attacks prior to their execution specifically from open sources. The contemporary information environment is characterised by data redundancy, which presents both opportunities and challenges. The primary issue is not access to information, but rather its filtration, verification of authenticity and transformation into a format suitable for managerial decision-making [1]. In the context of CI security, this necessitates, in our view, the implementation of effective analytical tools and data processing methodologies.

We concur with Professors I. Revak and O. Pidkhomnyi, who posit that OSINT plays a vital role in identifying the digital footprints of illicit activities. The utilisation of open-source data facilitates the tracking of asset movements, financial transactions and inter-entity links, as well as other indicators of the preparation or commission of crimes. For instance, in the field of criminal investigation, OSINT is employed to establish an evidentiary base, identify individuals, and map their connections – all of which are essential components of security provision [2].

OSINT assumes particular significance within the framework of contemporary armed conflicts and hybrid threats. In Ukraine, OSINT technologies are actively utilised to detect adversary activities, document war crimes and analyse information operations. This underscores the substantial potential of open-source intelligence in the spheres of national security and the protection of critical infrastructure [3].

At the same time, the employment of OSINT entails certain risks. Specifically, a significant challenge lies in the potential dissemination of unreliable or manipulative information, which can

lead to erroneous managerial decisions. Within the context of information warfare, this issue becomes particularly pertinent, as the adversary may deliberately plant disinformation to disorient analysts. Consequently, an essential component of OSINT research is the verification of source credibility and the rigorous application of fact-checking methodologies.

In conclusion, we assert that to enhance the effectiveness of OSINT in securing CI assets, it is necessary to implement a comprehensive approach comprising:

- The development of analytical competencies among specialists, aimed at acquiring the skills and practical techniques for fact-checking and the cultivation of analytical thinking;
- The deployment of advanced data processing tools, encompassing a suite of technologies, methodologies, and software solutions that facilitate the collection, processing, analysis, interpretation, and visualisation of large datasets for the timely detection of threats and informed managerial decision-making regarding CI;
- Inter-agency and international collaboration between CI security forces, defined as systemic, coordinated interaction among various state bodies, institutions, and international partners to facilitate information exchange, the alignment of actions, and joint response to security threats;
- The refinement of the regulatory and legal framework, understood as a purposeful process of updating, systematising, and developing legislation and bylaws that govern the collection, processing, analysis, and utilisation of open-source information to prevent, detect, and neutralise threats to CI;
- Enhancing public digital literacy, which entails a systemic process of fostering knowledge, skills, and behavioural models among citizens to ensure the safe use of digital technologies and mitigate risks to the functioning of critical state systems.

We contend that through the continuous monitoring of the information environment and the analysis of large datasets, security stakeholders gain the opportunity to transition from a reactive response model to a preventative one, thereby significantly enhancing the protection of CI. Consequently, OSINT research serves as a powerful instrument for bolstering the security of CI assets, as its application enables the timely detection of threats, comprehensive risk analysis and the formulation of informed managerial decisions. In the contemporary landscape, the role of OSINT research is poised for continued growth, which necessitates the further development of methodologies, tools and modern practices in the field of open-source intelligence for critical infrastructure security.

## References

1. Horbach M. M. OSINT technology use in information collecting, summarizing, and analyzing based on various social networks [Vykorystannia tekhnolohii OSINT dlia zboru, uzahalnennia ta analizu informatsii na osnovi riznykh sotsialnykh merezh]. Ternopil, 2023. [In Ukrainian].
2. Revak Iryna, Oleh Pidkhomnyi. The Use of OSINT Tools for Gathering Evidence of Theft and Illicit Trafficking of Cultural Property: Methodological Recommendations [Vykorystannia instrumentarii OSINT dlia zboru dokaziv vykradennia ta nelehalnogo obihu kulturnykh tsinnostei: Metodychni rekomendatsii]. Lviv: Lviv State University of Internal Affairs, 2025. [In Ukrainian].
3. Hlavatska A. L., Anhelska O. V., Opirskyi I. R. (2024). Investigation of the use of osint technology as a new threat of de-anonymized persons on the internet space [Doslidzhennia tekhnolohii vykorystannia OSINT yak novoi zahrozy z deanonimizatsii osoby v internet prostori]. *Cybersecurity: Education, Science, Technique* [Kiberbezpeka: osvita, nauka, tekhnika]. 1 (25). 19–50. [In Ukrainian].

**Downing D.,**  
**Johns E.,**  
*(Founders, Spyrian Limited)*

## **CONTEXT AND CONNECTIONS: HOW OSINT STRENGTHENS SANCTIONS COMPLIANCE IN SUPPORT OF UKRAINE'S NATIONAL SECURITY THROUGH NETWORK ANALYSIS AND CONTEXTUAL INVESTIGATION**

Sanctions compliance increasingly requires more than simple screening or a checklist. This paper situates sanctions evasion, illicit trade, and proxy networks as part of the wider security challenge facing Ukraine and shows how OSINT can help expose and disrupt those structures. In a complex and fast-moving world, we need to understand not only who an entity is, but also how it operates, who it is connected to, and what context may reveal hidden involvement in illicit activity. This paper uses case studies to illustrate how open-source intelligence (OSINT) can enable this process, strengthening sanctions compliance.

The first case explores an apparently "clean" entity that was ultimately linked, through deeper research, cultural context, and intelligence analysis, to the likely laundering of stolen Ukrainian grain. This example shows how sanctions evasion, illicit trade, and war-related economic crime can be identified through analysis of indicators which may be missed by simple screening tools and databases.

The second case study looks at a major oligarch network and shows how OSINT can be used to map enablers, proxies, and associated actors who may sit outside formal sanctions lists but still facilitate harmful activity. This helps us to identify broader ecosystems that sustain their influence and allow for newly identified actors to be sanctioned.

The paper will also outline the methodological foundations of effective OSINT practice, including source validation, corroboration, iterative hypothesis testing, and integration within the intelligence cycle. Before pulling all these strands together to argue that effective sanctions compliance must incorporate these two key ideas, contextual analysis and structured network investigation to produce defensible, actionable intelligence.

**Kudla M.-A. IO,**  
Professor  
*(Lviv State University of Internal Affairs)*  
**Bylen D.,**  
2nd year cadet  
*(Lviv State University of Internal Affairs)*

## **THE ROLE OF AI IN STRENGTHENING INTELLIGENCE ANALYSIS IN MODERN SECURITY ENVIRONMENTS**

In the context of current global security dynamics, it has become evident that traditional methods are increasingly inadequate in responding to evolving challenges. Contemporary security environments are increasingly characterized not only by the challenge of information acquisition, but also by the overwhelming volume of available data. Each day, vast quantities of digital information are generated from multiple sources, creating a situation that can be described as comparable to attempting to contain a waterfall within a limited vessel. For intelligence professionals, this represents a significant operational challenge, as there are inherent limits to human cognitive capacity before information overload occurs.

This phenomenon is often referred to as “information overload” or “data fatigue,” and it results in the concealment of relevant signals within large volumes of irrelevant or low-value data. In this context, artificial intelligence should not be viewed merely as an emerging technological innovation, but rather as an essential operational tool. Its purpose is not to replace human analysts, but to support them in structuring and interpreting complex and chaotic information environments [5].

The discussion first addresses the procedural dimension of intelligence work, specifically the collection and structured analysis of extensive data sets. Modern agencies are basically flooded with info from satellites, social media feeds, radio signals, and even random local news from halfway across the world. In the past, you’d need a literal army of people to read through all that, and they’d still miss half of it because they’re tired or bored. But today, we have things like Natural Language Processing (NLP). As a student of philology, I think this is one of the coolest parts of the tech. AI is actually getting good at picking up on things like local slang, cultural hints, and even the emotional tone of a text in dozens of languages at once. It’s not just about simple translation anymore; it’s about understanding what’s being said between the lines, like catching coded messages used by extremist groups. When the machine does this heavy lifting, human analysts can finally focus on what they’re actually good at — critical thinking and giving real advice to the people in charge.

Then there’s the predictive side of things, which feels like something out of a movie, but it’s very much real. The key objective for any intelligence officer is knowing about a threat before it actually happens. Machine learning models can now be trained on decades of old data to find those tiny, quiet signs that usually pop up right before a terror attack or a cyber-hack. It’s all about finding those “weak signals” that no human would ever notice. In cybersecurity, for instance, waiting for a virus to hit your network is a losing game. AI lets us see weird little “glitches” or patterns in network traffic that shouldn’t be there, giving us a heads-up long before the attack actually launches. It’s about flipping the script — moving from a reactive mode to a proactive one. Honestly, I think this is the biggest advantage that technology has given us in this century. It gives us back the most valuable thing in security: time to react [3].

We also have to mention visual intelligence, or GEOINT. Modern AI systems can scan through thousands of satellite photos and immediately flag if a tank has moved or if a new military base is being built. What used to take a whole room of people days to confirm is now done by an algorithm in seconds. In a modern conflict, where every second literally counts, that kind of speed is a matter of life and death. But it's not just about seeing; it's about combining different types of data. When you mix these space photos with radio signals and internet data, you get a clear, multi-layered view of the whole situation. It really helps clear up that information ambiguity in warfare that always makes everything so confusing for commanders on the ground. We are moving toward a world where it's becoming harder and harder for adversaries to hide what they are doing.

However, it is important to acknowledge that artificial intelligence is not infallible and should not be regarded as a universal solution. Alongside its advantages, it presents a range of significant challenges that require careful consideration. One of the most critical issues is the "black box" problem, whereby AI systems may produce outputs whose underlying decision-making processes are not fully transparent or interpretable, even to their developers. This lack of explainability raises concerns regarding the reliability and accountability of such systems, particularly in high-stakes domains such as national security [4].

Another key limitation is the presence of bias. If the training data is incomplete, unbalanced, or of low quality, the resulting outputs will inevitably reflect and potentially amplify these deficiencies. In addition, it must be acknowledged that adversarial actors may also exploit AI technologies. Hostile states, for instance, may engage in data poisoning or deliberately introduce misleading information in order to manipulate system outputs [1].

For these reasons, it is essential that AI systems are not deployed in a fully autonomous manner. Human oversight remains crucial, ensuring that final decisions are critically evaluated and that anomalous or unreliable outputs are appropriately questioned and verified. Ethical considerations also constitute a fundamental dimension of this discussion and cannot be disregarded. The use of AI for continuous surveillance or for the identification of potential targets raises significant concerns regarding privacy and fundamental human rights. It is therefore imperative that decisions concerning the classification of individuals as threats are not made without meaningful human supervision.

In this context, the development of Explainable AI (XAI) is of particular importance. Such systems are designed to provide transparent and interpretable decision-making processes, thereby enhancing accountability and public trust. Transparency in algorithmic reasoning also contributes to ensuring that outcomes remain legally and ethically acceptable. Accountability is a central requirement in this regard: in the event of an error, it must be possible to determine both its cause and the responsible actors. Since algorithms cannot be held accountable in a legal or moral sense, ultimate responsibility must remain with human decision-makers.

Looking forward, the future of intelligence analysis is likely to be characterized by a "centaur" model, in which human analysts and AI systems operate in close collaboration. While AI excels in processing speed and quantitative analysis, humans retain a comparative advantage in interpreting cultural context, emotional nuance, and the underlying rationale behind actions. For example, whereas an algorithm may identify behavioural patterns as suspicious, a human analyst is better positioned to interpret the political or historical context that may explain such behaviour [6].

In conclusion, artificial intelligence can no longer be considered an optional enhancement, but rather a fundamental component of contemporary security systems. It enables the processing and interpretation of vast volumes of information, thereby enhancing situational awareness and

improving the capacity to anticipate and respond to emerging threats. At the same time, the deployment of such technologies requires a cautious and responsible approach [2].

It is essential that technological advancement remains aligned with ethical principles and subject to meaningful human oversight. A balance must therefore be maintained between computational efficiency and human judgment. If an effective integration of machine-driven analytical capabilities and human expertise can be achieved, it will significantly strengthen the ability to address the complex security challenges of the twenty-first century.

Achieving this equilibrium is not without difficulty. However, it is a necessary condition for ensuring both security and responsible technological development in an increasingly complex and unpredictable global environment.

### **References**

1. Agrell, W., & Treverton, G. F. (2015). *National Intelligence and Science: Beyond the Great Divide*. Oxford University Press.
2. Babbage, R. (2020). *The Next Leg of the Intelligence Revolution*. Center for Strategic and Budgetary Assessments.
3. Hoadley, D. S., & Lucas, N. J. (2018). *Artificial Intelligence and National Security*. Congressional Research Service.
4. Johnson, J. (2021). *Artificial Intelligence and the Future of Warfare*. Manchester University Press.
5. Lahneman, W. J., & Arcos, R. (2019). *The Art of Intelligence*. Rowman & Littlefield.
6. Zwetloot, R., & Dafoe, A. (2019). *Bridging the AI Governance Gap*. Center for a New American Security.

**Ангеленюк А.-М. Ю.,**  
доцент кафедри  
фінансових розслідувань та економічної безпеки,  
кандидат юридичних наук, старший дослідник  
(Державний податковий університет)

**Бреславець В. В.,**  
здобувач вищої освіти  
(Державний податковий університет)

**Бура А. В.,**  
здобувач вищої освіти  
(Державний податковий університет)

## **ВИКОРИСТАННЯ ВІДКРИТИХ ДЖЕРЕЛ ДЛЯ ВИЯВЛЕННЯ НЕЗАКОННИХ ФІНАНСОВИХ СХЕМ**

Сучасний етап розвитку глобальної фінансової системи характеризується ускладненням методів легалізації доходів, одержаних злочинним шляхом. У відповідь на це розвідка на основі відкритих джерел (OSINT) стала критично важливим елементом у сфері протидії незаконним фінансовим операціям. Традиційні методи банківського моніторингу часто обмежені внутрішньою інформацією та закритими міжбанківськими реєстрами, тоді як інструменти OSINT дозволяють вибудувати значно ширшу мережу зв'язків між номінальними власниками та реальними бенефіціарами фінансових потоків. Основна перевага використання відкритих даних полягає у можливості незалежної верифікації інформації, наданої клієнтом, через аналіз його цифрового сліду та публічних баз даних.

Ефективний моніторинг для виявлення незаконних схем, таких як відмивання коштів, фіктивне підприємництво або ухилення від міжнародних санкцій, вимагає чіткої класифікації джерел. Насамперед це державні реєстри юридичних осіб та прав власності. В Україні ключову роль відіграє Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань, який дозволяє аналітикам відстежувати історію змін засновників, керівників та статутного капіталу, що часто є маркером підготовки компанії до участі у фінансових махінаціях. Не менш важливим є аналіз судових рішень. Через Єдиний державний реєстр судових рішень можна ідентифікувати участь контрагента у кримінальних провадженнях або виявити ознаки створення фіктивних заборгованостей, які традиційно використовуються для легального виведення капіталу за кордон.

Вагомим складником аналітичної роботи є дослідження антикорупційних декларацій представників влади та опрацювання масивів інформації з публічних витоків. Найбільш ефективним інструментом для перевірки майнових звітів є Єдиний державний реєстр декларацій, адміністрування якого забезпечує Національне агентство з питань запобігання корупції (НАЗК).

Цей ресурс акумулює щорічні звіти та сповіщення про вагомні зміни у фінансовому стані суб'єктів декларування. Варто враховувати, що на час дії правового режиму воєнного стану доступ до певних категорій декларацій у публічному сегменті обмежений з міркувань безпеки.

Функціонал Реєстру дозволяє здійснювати пошук інформації за ПІБ декларанта або застосовувати систему фільтрації. Зокрема, користувачі можуть групувати документи за звітними періодами, типом посади чи рівнем її відповідальності. Особливо цінною для розслідувачів є можливість виокремити перелік осіб, чия професійна діяльність пов'язана з підвищеними корупційними ризиками або належить до категорії особливо відповідального становища [1].

Проекти на кшталт Panama Papers або Pandora Papers, що агрегуються платформою OCCRP, надають унікальну можливість виявити приховані офшорні структури, які не фігурують у національних реєстрах [2]. Порівняння офіційних статків особи з фактичним стилем життя, який фіксується у медіа та соціальних мережах, залишається одним із найбільш ефективних методів виявлення корупційних схем.

Методологія OSINT спрямована на пошук так званих «червоних прапорців» (red flags). До них належать складні багаторівневі структури власності з використанням компаній-оболонки у юрисдикціях з низькою прозорістю. Також підозрілою ознакою є масові адреси реєстрації. Використання сервісів на кшталт Google Maps у поєднанні з реєстрами нерухомості дозволяє перевірити реальний офіс компанії: якщо за адресою зареєстровано сотні фірм або це занедбане житлове приміщення, це прямо вказує на фіктивність підприємства. Додатково аномальна активність у соціальних мережах керівництва може розкрити неформальні зв'язки з політично значущими особами (PEPs), що є критичним для оцінки ризиків.

Для обробки великих масивів інформації сьогодні використовуються спеціалізовані агрегатори та інструменти автоматизації. В українському контексті системи YouControl та Clarity Project дозволяють у реальному часі візуалізувати зв'язки між контрагентами та виявляти санкційні ризики. На міжнародному рівні незамінним є ресурс OpenCorporates — найбільша відкрита база даних компаній у світі, що значно полегшує транскордонні розслідування. Для глибинного аналізу використовується програмне забезпечення типу Maltego, яке дозволяє будувати інтерактивні графи взаємовідносин між фізичними особами та бізнес-структурами.

Сучасні фінансові схеми все частіше інтегрують криптовалюти, проте блокчейн за своєю природою є «відкритою книгою». Використання публічних браузерів блоків, таких як Etherscan, дозволяє відстежувати рух активів у реальному часі. Хоча адреси гаманців анонімні, їх поєднання з даними з відкритих форумів, Telegram-каналів або соцмереж часто дозволяє деанонізувати учасників незаконних схем. Водночас, при здійсненні таких розслідувань необхідно суворо дотримуватися правових норм. Інформація з відкритих джерел повинна слугувати фундаментом для офіційних запитів або бути належним чином процесуально зафіксована для використання як доказ у кримінальному провадженні [3]. Підсумовуючи, можна стверджувати, що системне використання OSINT забезпечує глибину аналізу, яка дозволяє не просто фіксувати окремі транзакції, а розкривати цілісні механізми приховування незаконних доходів.

Отже, використання відкритих джерел є важливим та перспективним напрямом у виявленні незаконних фінансових схем. Поєднання можливостей OSINT з інструментами фінансового моніторингу та сучасними аналітичними технологіями (зокрема, штучним інтелектом) дозволяє значно підвищити ефективність протидії економічним правопорушенням. Водночас подальший розвиток цього напрямку потребує удосконалення нормативного регулювання, підвищення якості відкритих даних та розвитку міжвідомчої взаємодії.

#### **Список використаних джерел**

1. Офіційний портал НАЗК. Розділ: Декларування. URL: <https://public.nazk.gov.ua> (дата звернення: 28.04.2026).
2. Organized Crime and Corruption Reporting Project (OCCRP). Aleph Data Search Platform. URL: <https://aleph.occrp.org> (дата звернення: 28.04.2026).
3. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення : Закон України від 06.12.2019 № 361-IX

**Андросович Л. Г.,**  
старший викладач кафедри  
кримінального процесу  
та криміналістики  
(Національна академія Служби безпеки України)

## **РОЛЬ OSINT У ВИЯВЛЕННІ ТА РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У ФІНАНСОВІЙ СИСТЕМІ УКРАЇНИ**

Трансформація фінансового ринку в умовах цифровізації, поширення криптовалют та офшорних схем кардинально змінила обличчя економічної злочинності в Україні. Легалізація (відмивання) доходів, отриманих злочинним шляхом, шахрайство у банківській сфері, ухилення від сплати податків і незаконне виведення капіталів набули нових форм, що фактично вимагають від правоохоронних органів оновлення методологічного арсеналу. Відповіддю на цей виклик стала розвідка на основі відкритих джерел (Open Source Intelligence — OSINT) — системна методологія збору, аналізу та верифікації загальнодоступних даних з метою отримання орієнтуючої чи доказової інформації у кримінальному провадженні.

*Довідково: Питання застосування відкритих джерел у кримінальному провадженні привертає дедалі більшу увагу науковців. Значний внесок у розробку теоретичної бази зробив О.О. Торбас, підручник якого «OSINT при розслідуванні кримінальних правопорушень» систематизував основні методи та інструменти галузі. Учений цілком обґрунтовано наголошує, що всі наукові розробки доцільно розвивати у двох напрямках: загальний алгоритм OSINT-розслідування та спеціалізовані інструкції стосовно окремих видів злочинів, зокрема економічних. Нам імпонує ця позиція, оскільки фінансова злочинність вирізняється особливою латентністю та складністю слідів, що залишаються, і потребує саме таргетованого підходу [1].*

*Проблематику допустимості електронних доказів, отриманих через OSINT, у кримінальному провадженні ґрунтовно дослідила О.В. Бабаєва. Дослідниця справедливо констатує, що результати OSINT-розслідувань мають доказове значення лише за умови їх належної правової фіксації, а саме — у формі протоколу огляду з використанням фото- чи відеозапису. Водночас вона критикує вітчизняний КПК за ігнорування електронних доказів як самостійного виду, вказуючи на колізію між практичними потребами та законодавчими реаліями [2, с. 171].*

*Питання міжнародного досвіду впровадження OSINT у правоохоронну діяльність, зокрема в контексті ЄС і НАТО, детально висвітлили В. Зуй та О. Мицик. Як зазначено у цитованій роботі, 23 листопада 2023 року Європол заснував спеціальну робочу групу з відкритої розвідки для координації збору, аналізу та верифікації цифрових доказів, що є прямим свідченням: міжнародне правозастосовне середовище вже прийняло OSINT як стандарт, тоді як Україна лише на початку цього шляху [3, с. 207].*

Враховуючі наведені наукові підходи, слід зазначити, що як вітчизняні, так і зарубіжні дослідники одноставно підкреслюють зростаюче значення OSINT як інструменту виявлення, фіксації та аналізу цифрових доказів у сучасних умовах. Водночас практична реалізація цих підходів безпосередньо залежить від специфіки тієї сфери суспільних відносин, у межах якої здійснюється розслідування, а також від характеру правопорушень, що підлягають виявленню та доказуванню.

У цьому контексті особливої уваги потребує фінансова сфера, яка являє собою складний міжгалузевий комплекс відносин, де злочинні схеми нерідко маскуються під

легальні операції. Відмивання коштів, шахрайство з банківськими інструментами, ухилення від сплати податків і незаконний відтік капіталу — це далеко не повний перелік правопорушень, що становлять загрозу для її стабільності. Зазначені злочини, як правило, залишають численні цифрові сліди у відкритому просторі — реєстраційні дані юридичних осіб, відомості про власників активів, публічні фінансові декларації, профілі у соціальних мережах, архіви новин тощо.

Розвідка на основі відкритих джерел (OSINT) охоплює широкий спектр методів і інструментів для збору, аналізу та інтерпретації даних з публічно доступних джерел. У контексті фінансових розслідувань OSINT передбачає аналіз відкритих реєстрів (ЄДР, Opendatabot, YouControl), публічних баз даних декларацій НАЗК, моніторинг рахунків у публічних блокчейн-оглядачах (Etherscan, BTC Explorer), перевірку корпоративних структур в офшорних реєстрах (OpenCorporates, ICIJ Offshore Leaks), а також верифікацію транзакцій та пошук ідентифікаційних зв'язків у соціальних мережах і медіапросторі [4].

З практичної точки зору, OSINT-розслідування фінансового злочину будується за логічним алгоритмом: формування завдання → збір даних → їх перевірка та верифікація → аналітичний синтез → підготовка OSINT-звіту чи протоколу огляду. Кожна з цих стадій потребує документування задля забезпечення подальшої допустимості отриманих даних у суді. Відповідно до чинного КПК України, зібрані через OSINT відомості можуть набути статусу документального доказу у розумінні ч. 1 ст. 99 КПК лише за умови їх належного процесуального оформлення — зокрема, у вигляді протоколу огляду з відтворенням змісту джерела засобами фіксації [2, с. 173].

Нормативне підґрунтя для застосування OSINT у фінансових розслідуваннях формується кількома рівнями правового регулювання. На рівні спеціального законодавства ключову роль відіграє Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» № 361-IX від 06.12.2019. Цей нормативний акт запровадив систему ризик-орієнтованого нагляду та розширив коло суб'єктів первинного фінансового моніторингу, що об'єктивно збільшило масив відкритих аналітичних даних, доступних слідству [4].

Водночас у самому законі відсутня будь-яка згадка про OSINT-технології, що є суттєвою прогалиною, яка ускладнює системну координацію між фінансовим моніторингом і кримінальним провадженням

В той же час відсутність легального визначення термінів «електронні докази» та «розвідка на основі відкритих джерел» у КПК України — це не просто техніко-юридичний недолік, а реальна проблема на практиці. Оскільки без чіткого нормативного закріплення цих понять суди стикаються з невизначеністю під час оцінки OSINT-матеріалів, і захисна сторона нерідко успішно оспорує їх допустимість. Подібну критику на адресу законодавства висловлюють і міжнародні партнери: Протокол Берклі щодо розслідувань з використанням відкритих цифрових даних (Berkeley Protocol on Digital Open Source Investigations) фіксує стандарти збору та верифікації OSINT-доказів, однак Україна досі не імплементувала ці стандарти на рівні КПК [5].

Окремою темою, яка активно обговорюється у науковому середовищі, є застосування OSINT при розслідуванні відмивання коштів через криптовалюти. І.В. Пашинська небезпідставно стверджує, що блокчейн-технологія, попри псевдоанонімний характер адрес гаманців, залишає публічний та незмінний запис усіх транзакцій, що перетворює публічні реєстри на унікальне «відкрите джерело» для слідчого [6, с. 112].

Аналіз ланцюжків транзакцій (chain analysis) з використанням таких інструментів, як Chainalysis або Crystal Blockchain, по суті є OSINT-методологією у фінансовому розслідуванні. Водночас учені звертають увагу на те, що відповідна методика залишається поза межами процесуальної регламентації, а висновки спеціалістів, отримані таким шляхом, мають невизначений доказовий статус [5].

*Довідково: З процесуальної точки зору OSINT не завжди визнається повноцінним доказом у кримінальному провадженні, оскільки джерело такої інформації не завжди є надійним, а спосіб її здобуття – не завжди відповідає нормам Кримінального процесуального кодексу України. Наприклад, самостійно отриманий скріншот з веб-сайту або збережена копія сторінки без засвідченого джерела, хеш-підтвердження чи протоколу огляду в режимі фіксації (наприклад, з використанням програми «WebPreserver») можуть бути визнані неналежним доказом. Тому OSINT-дані переважно мають аналітичне значення – як джерело орієнтувальної або попередньої інформації для формування версій, обґрунтування підстав для клопотання про обшук, тимчасовий доступ або експертизу. У деяких випадках така інформація може бути використана в ході слідчих (розшукових) дій, але з обов'язковим процесуальним закріпленням: наприклад, у вигляді протоколу огляду вебресурсу з технічним фіксуванням, залученням спеціаліста та створенням цифрового снейпшоту (snapshot) із хеш-сертифікацією. Крім того, низка країн і міжнародних організацій розробляють стандарти допустимості OSINT-даних як доказів у кримінальному провадженні. Таким чином, у сфері розслідування економічних злочинів OSINT може виступати як ефективний засіб: побудови гіпотез і аналітичних моделей злочинної діяльності; ідентифікації цифрових слідів і потенційних суб'єктів злочину; доповнення цифрових доказів, отриманих у процесуальний спосіб; збирання інформації для подальших процесуальних рішень. Водночас його правове значення обмежене рамками чинного процесуального регулювання, що актуалізує необхідність законодавчої деталізації статусу відкритих цифрових джерел у кримінальному процесі України [7, с. 627].*

Резюмуючи вище викладене, слід зазначити, що OSINT є ефективним і перспективним інструментом виявлення та розслідування кримінальних правопорушень у фінансовій системі України, оскільки фінансові злочини генерують значний масив відкритих цифрових слідів, аналіз яких здатний суттєво прискорити встановлення обставин справи та розкрити складні корпоративні схеми.

Водночас, поряд із очевидними перевагами, застосування OSINT у вітчизняній практиці супроводжується низка системних проблем, які потребують комплексного вирішення:

- нормативне забезпечення у цій сфері залишається вкрай недостатнім: КПК України не визначає поняття «розвідка на основі відкритих джерел» і не встановлює чіткого порядку процесуального оформлення OSINT-матеріалів як доказів, що породжує правову невизначеність і ризики для обвинувачення у судовому процесі.

- інституційний розрив між системою фінансового моніторингу та кримінальним провадженням потребує усунення шляхом закріплення механізмів передачі OSINT-аналітики від ДСФМ та суб'єктів первинного фінансового моніторингу безпосередньо до слідчих органів у процесуально легітимній формі.

Перспективними напрямками вдосконалення є: імплементація стандартів Протоколу Берклі до КПК України; запровадження підготовки слідчих і прокурорів з OSINT-методологій; розроблення спеціалізованих інструкцій для розслідування фінансових злочинів із застосуванням відкритих реєстрів, криптоаналізу блокчейн-транзакцій та аналізу офшорних структур.

Загалом, враховуючи вищесказане, слід констатувати, що OSINT є не лише технічним засобом, а й новою методологічною парадигмою фінансового розслідування, і завдання вітчизняної правової системи — якнайшвидше наповнити цю парадигму відповідним нормативним змістом.

### Список використаних джерел

1. Торбас О. О. OSINT при розслідуванні кримінальних правопорушень : підручник. Одеса : Юридика, 2024. 180 с. URL: <https://dspace.onua.edu.ua/items/73cc7efb-a97e-44b5-a99b-9761ff0d07b7>
2. Бабаєва О. В., Авербах Д. В. Щодо питання використання доказів з відкритих джерел у кримінальному провадженні. *Науковий вісник Ужгородського національного університету*. Серія: Право. 2024. Вип. 83. Ч. 3. С. 169–174. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/07/28-2.pdf>.
3. Борисова К., Жмуровська К., Кришталь Є., Деревягін О. OSINT у правоохоронній діяльності: міжнародний досвід та українські перспективи. *UNIVERSUM*. 2025. № 25. С. 205–210. URL: <https://archive.liga.science/index.php/universum/article/view/2155>
4. OSINT — що це таке, суть, визначення та приклади, види, методи та інструменти розвідки на основі відкритих джерел. URL: <https://termin.in.ua/osint-rozvidka-na-osnovi-vidkrytykh-dzherel/>
5. Андросович Л. Г. Розслідування кримінальних правопорушень, вчинених організованими злочинними угрупованнями у фінансовій сфері: виклики цифрової епохи. *Сто сьома економіко-правова дискусія* : матеріали Міжнародної мультидисциплінарної наукової конференції. Серія: Соціальні та гуманітарні науки. 2026. URL: <http://www.spilnota.net.ua/ua/article/id-5604/>
6. Пашинська І. В. Теоретико-методологічні основи розслідування організованої злочинності у сфері господарської діяльності : дис. ... д-ра філос. : 081 «Право». Харківський національний університет внутрішніх справ. Харків, 2023. 294 с.
7. Кутєпов І. О. Роль цифрових доказів під час розслідування економічних злочинів. *Юридичний науковий електронний журнал*. 2025. № 2. С. 626–630. URL: [http://lsej.org.ua/2\\_2025/153.pdf](http://lsej.org.ua/2_2025/153.pdf).

**Березовський Є. О.,**  
курсант 1 курсу навчально-наукового інституту  
підготовки фахівців для підрозділів кримінальної поліції  
імені Е. О. Дідоренка  
*(Донецький державний університет внутрішніх справ)*  
Науковий керівник: **Кісіль М. Л.,**  
викладач кафедри адміністративно-правових дисциплін  
*(Донецький державний університет внутрішніх справ)*

## **OSINT ЯК ДОКАЗОВА БАЗА У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ: ПРАВОВІ ТА ПРАКТИЧНІ АСПЕКТИ**

В умовах повномасштабного збройного конфлікту та прискореної цифровізації суспільного життя правоохоронні органи України дедалі частіше стикаються з необхідністю залучення інформації з відкритих джерел у кримінальних провадженнях. OSINT (Open Source Intelligence) - розвідка на основі відкритих джерел - дає змогу збирати, аналізувати та верифікувати публічно доступну інформацію з соціальних мереж, вебсайтів, геолокаційних сервісів, баз даних та інших відкритих платформ. Попри широке практичне застосування, питання допустимості OSINT-матеріалів як доказів у кримінальному провадженні залишається недостатньо врегульованим у вітчизняному законодавстві.

Мета дослідження - визначити правові підстави та практичні механізми використання результатів OSINT-досліджень як доказової бази у кримінальному провадженні України.

Кримінальний процесуальний кодекс України (далі - КПК) закріплює вичерпний перелік процесуальних джерел доказів у ч. 2 ст. 84: показання, речові докази, документи та висновки експертів. Водночас КПК не містить жодної згадки про електронні (цифрові) докази як самостійний вид, що створює суттєві правозастосовні труднощі. На цю прогалину вказував А. В. Столітній, наголошуючи на необхідності формування повноцінного інституту електронного кримінального провадження, який охоплював би й правила поведіння з цифровими доказами [1, с. 28].

OSINT-матеріали - скріншоти публікацій, відеозаписи, геодані, метадані файлів, архівні версії вебсторінок тощо - за змістом підпадають під поняття документів у розумінні ст. 99 КПК або речових доказів (ст. 98 КПК), однак практика їх процесуального закріплення залишається суперечливою. О. П. Метелев звертає увагу на особливу нематеріальну природу цифрових доказів, які виникають, існують, копіюються та зберігаються принципово інакше, ніж традиційні докази, що зумовлює потребу виділення «цифрового огляду» як самостійної слідчої дії [2, с. 82].

Ключовою проблемою є допустимість OSINT-матеріалів у суді. О. П. Метелев виокремлює три основні критерії допустимості цифрових доказів: 1) законність джерела їх отримання; 2) дотримання встановленої процесуальної форми фіксації; 3) забезпечення цілісності та автентичності даних на всіх етапах - від збору до долучення до матеріалів провадження [3, с. 228]. Стосовно OSINT-матеріалів задоволення цих критеріїв потребує застосування криптографічного хешування (MD5, SHA-256) та дотримання стандартів ланцюга зберігання (chain of custody).

Практичним орієнтиром для процесуальної роботи з OSINT-матеріалами слугують методичні рекомендації Національної академії внутрішніх справ «Використання електронних

(цифрових) доказів у кримінальних провадженнях» за загальною редакцією О. В. Корнейка. У цьому виданні, зокрема, зазначено, що вилучення цифрових доказів із відкритих джерел слід здійснювати з дотриманням вимог Протоколу Берклі - міжнародного стандарту збору та верифікації цифрових доказів, розробленого Школою права Каліфорнійського університету спільно з ООН [4, с. 78].

Зазначені вимоги безпосередньо позначаються на процесуальному оформленні OSINT-матеріалів. Відповідно до ст. 237 КПК слідчий (детектив) зобов'язаний скласти протокол огляду речей та документів, фіксуючи всі ідентифікаційні ознаки цифрового об'єкта: URL-адресу, дату та час збереження, хеш-суму, метадані. Ігнорування цих вимог є підставою для визнання доказів недопустимими відповідно до ст. 87 КПК. У контексті документування воєнних злочинів Офіс Генерального прокурора спільно з міжнародними партнерами (Eurojust, ICC) вже напрацьовує відповідні стандарти, однак єдиного процесуального механізму для OSINT-матеріалів у КПК досі не закріплено.

Отже, використання OSINT як доказової бази у кримінальному провадженні є перспективним і практично затребуваним напрямом, однак потребує чіткої правової регламентації. Зокрема, необхідно забезпечити: внесення змін до КПК України для закріплення електронних (цифрових) доказів як самостійного виду процесуальних джерел із визначенням вимог до їх збору та фіксації; запровадження стандартизованих протоколів верифікації цифрового контенту в діяльності правоохоронних органів на основі Протоколу Берклі; включення підготовки з основ OSINT-аналітики до обов'язкової фахової підготовки слідчих та детективів.

### **Список використаних джерел**

1. Столітній А. В. Електронне кримінальне провадження на досудовому розслідуванні : автореф. дис. на здобуття наук ступеня д-ра. юрид. наук : спец. 12.00.09. Дніпропетровський державний університет внутрішніх справ. Дніпро, 2018. 42 с. URL: <https://surli.li/qiplqv> (дата звернення: 20.04.2026).
2. Метелев О. П. Гносеологічна і правова природа цифрових доказів у кримінальному провадженні. *Правова позиція*. 2018. № 1 (20). С. 75–86. URL: <https://surli.cc/mmrqoo> (дата звернення: 20.04.2026).
3. Метелев О. П. Проблеми визначення допустимості і належності електронних (цифрових) доказів у кримінальному процесі. *Вісник кримінального судочинства*. 2019. № 3. С. 224–238. URL: <https://surli.li/bqxceb> (дата звернення: 21.04.2026).
4. Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. реком. / М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін. ; за заг. ред. О. В. Корнейка. 2-ге вид., допов. Київ : Нац. акад. внутр. справ, 2020. 104 с. URL: <https://surli.li/dvmxth> (дата звернення: 21.04.2026).

**Блавацька Н. М.,**  
доцент кафедри, кандидат технічних наук, доцент  
(Національна академія Служби безпеки України)

### **III-ТЕХНОЛОГІЇ ТРАНСКРИБУВАННЯ ВІДЕО В СИСТЕМІ OSINT-ДОСЛІДЖЕНЬ**

В умовах стрімкого зростання обсягів відеоконтенту в мережі Інтернет відеоматеріали стають одним із ключових джерел інформації для аналітиків розвідки відкритих джерел. Ручне опрацювання великих масивів відеоданих є надзвичайно трудомістким процесом, що обумовлює необхідність впровадження автоматизованих III-рішень для транскрибування. Особливої актуальності ця проблематика набуває в контексті інформаційного протиборства, журналістських розслідувань та правоохоронної діяльності, де своєчасність і точність аналізу відіграють вирішальну роль.

Автоматичне транскрибування передбачає перетворення аудіо та відеоданих у текстовий формат за допомогою технологій штучного інтелекту, зокрема систем розпізнавання мовлення. Отримані тексти можуть інтегруватися з аналітичними платформами, що значно розширює можливості пошуку, обробки та інтерпретації інформації.

Застосування таких інструментів у OSINT-дослідженнях забезпечує суттєві переваги, зокрема значне прискорення обробки великих обсягів інформації, покращення можливостей пошуку через переведення аудіо та відеоконтенту у текстову форму, а також ефективну індексацію даних для подальшого аналізу. Отримані транскрипти дозволяють миттєво знаходити згадки конкретних імен, географічних назв, організацій або подій у великих масивах відеоматеріалів. Це відкриває можливості для побудови аналізу зв'язків між суб'єктами, виявлення повторюваних наративів і пропагандистських шаблонів, а також відстеження еволюції риторики конкретних осіб або організацій у часі.

Крім того, це дозволяє виявляти ключові слова та теми, що є критично важливим для глибокого аналітичного дослідження та масштабування OSINT-операцій.

Практичне застосування автоматичного транскрибування охоплює аналіз інтерв'ю, публічних заяв, стрімів та подкастів, моніторинг соціальних мереж і відеоплатформ, а також виявлення дезінформації та пропагандистських повідомлень. Окрім цього, такі інструменти можуть використовуватися для документування доказової бази, зокрема у розслідуваннях, пов'язаних із порушеннями міжнародного права.

Автоматичне транскрибування відео кардинально змінює підхід до роботи з відкритими джерелами, перетворюючи відеоконтент із пасивного об'єкта перегляду на активний масив структурованих даних, придатних для глибокого аналізу.

Транскрибування суттєво посилює можливості верифікації інформації, одного з ключових завдань OSINT-аналітики. Зіставлення текстового транскрипту з візуальним рядом відео дозволяє виявляти розбіжності між тим, що говориться, і тим, що показується, що є важливим індикатором маніпуляції або монтажу. Крім того, порівняння транскриптів різних версій одного відео може свідчити про його редагування або фальсифікацію.

Окремим напрямом є мультимовний аналіз, який набуває особливого значення в умовах міжнародних конфліктів та геополітичних криз. Сучасні III-інструменти дозволяють транскрибувати відео іноземними мовами з подальшим автоматичним перекладом, що дає змогу аналітикам працювати з першоджерелами без знання відповідної мови. Це суттєво розширює географічне охоплення OSINT-досліджень і знижує залежність від перекладачів.

Важливою функцією є також автоматична ідентифікація спікерів, яка дозволяє у багатоголосих записах, а саме: дискусіях, переговорах, нарадах розмежовувати висловлювання різних учасників та приписувати конкретні заяви конкретним особам. У поєднанні з біометричним аналізом голосу це відкриває можливості для ідентифікації анонімних або замаскованих осіб у відеоматеріалах. Нарешті, інтеграція транскрибування з іншими OSINT-інструментами, такими як системи геолокації, аналізу метаданих та моніторингу соціальних мереж, дозволяє будувати комплексні аналітичні цикли, що значно підвищують глибину та достовірність досліджень.

Застосування III-технологій транскрибування у сфері OSINT має як очевидні переваги, так і певні обмеження. До переваг належать висока швидкість обробки даних, підтримка великої кількості мов, масштабованість рішень та можливість інтеграції з іншими OSINT-інструментами. Водночас існують і суттєві обмеження. До обмежень можна віднести помилки розпізнавання при низькій якості звуку, складнощі з діалектами та специфічною термінологією, ризики, пов'язані з конфіденційністю даних, а також юридичні обмеження, що діють у різних юрисдикціях. Усі ці фактори вказують на необхідність обов'язкової верифікації отриманих результатів аналітиком.

Використання III-транскрибування в OSINT-дослідженнях пов'язане з низкою правових та етичних викликів. Насамперед постає питання дотримання авторських прав на відеоматеріали, що використовуються в процесі дослідження. Не менш важливим є захист персональних даних відповідно до вимог Загального регламенту про захист даних та норм національного законодавства. Особливої уваги потребує недопущення маніпуляцій із транскриптами з метою фальсифікації інформації або дезінформації, що є особливо актуальним в умовах інформаційного протиборства.

Висновки. III-технології транскрибування відео є перспективним і практично значущим інструментом у системі OSINT-досліджень. Їх інтеграція в аналітичні процеси дозволяє суттєво підвищити ефективність роботи з відкритими джерелами, скоротити час обробки інформації та розширити можливості виявлення релевантних даних. Разом із тим успішне застосування цих технологій вимагає комплексного підходу, що поєднує технічну грамотність, критичне мислення та дотримання правових норм. Подальший розвиток III у сфері розпізнавання мовлення визначатиме нові стандарти розвідувально-аналітичної діяльності та відкриватиме нові можливості для дослідників у галузі OSINT.

### **Список використаних джерел**

1. Nautsch A., Patino J., Treiber A., Stafylakis T., Mizera P., Todisco M., Schneider T., Evans N. Privacy-Preserving Speaker Recognition with Cohort Score Normalisation. URL: [https://www.researchgate.net/publication/335828982\\_Privacy-Preserving\\_Speaker\\_Recognition\\_with\\_Cohort\\_Score\\_Normalisation](https://www.researchgate.net/publication/335828982_Privacy-Preserving_Speaker_Recognition_with_Cohort_Score_Normalisation) (дата звернення: 24.04.2026).
2. European Parliament. (2016). General Data Protection Regulation (GDPR). Regulation (EU) 2016/679. URL: <https://gdpr-info.eu> (дата звернення: 24.04.2026).
3. Левикін І. В., Шимко Д. І. Підхід до автоматизації конверсії відео та аудіо матеріалів у текст. *Радіоелектроніка та молодь у XXI столітті* : матеріали 29 Міжнар. молодіжн. форуму, м. Харків, 16–18 квітня 2025 р. Харків, 2025. Т. 6. С. 619–621.
4. Левикін І. В., Шимко Д. І. Методи автоматизованої конверсії відеоконтенту в структурований медіаматеріал. URL: <https://surl.lu/ggmai> (дата звернення: 24.04.2026).

**Бондар В. С.,**  
завідувач кафедри кримінального процесу  
та криміналістики,  
кандидат юридичних наук, професор  
(Національна академія Служби безпеки України)

## **ЗАСТОСУВАННЯ OSINT-ТЕХНОЛОГІЙ У ДОКУМЕНТУВАННІ ТА РОЗСЛІДУВАННІ ОКРЕМИХ ВИДІВ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПІДСЛІДНИХ СЛІДЧИМ ОРГАНІВ БЕЗПЕКИ**

Серед злочинів, учинених в період повномасштабного вторгнення РФ до України воєнні злочини взагалі та воєнні злочини зокрема, а саме умисні вбивства військовополонених, катування та інше жорстоке поводження з військовополоненими, передбачені ст. 438 Кримінального кодексу України (далі – КК України) є найбільш складними в сенсі документування та розслідування. Суттєвим чинником цього є заходи протидії, котрі вживаються фігурантами даних проваджень: приховання зовнішності, припинення катувань за певний період до обміну задля усунення тілесних ушкоджень відповідного характеру тощо. Зазначене актуалізує необхідність пошуку співробітниками органів правопорядку нових шляхів документування та розслідування кримінальних правопорушень даної категорії.

Цілком очевидним є те, що відповідна оперативно-розшукова (контррозвідальна) діяльність буде більш ефективною за умови застосування новітніх технологій, у тому числі інформаційних, які базують на штучному інтелекті, зокрема нейромереж для розпізнавання вербальної інформації, а також розпізнавання ознак зовнішності людини за фото- та відеоматеріалами.

Як правило, відео позасудових страт розміщується суб'єктами даних злочинів у відповідних групах у месенджері «Телеграм», відеохостінгу YouTube. Ефективність в ідентифікації воєнних злочинців демонструють нейронні мережі, які завдяки відповідній комбінації спеціальних лінгвістичних знань, аналітиків та фахівців у сфері машинного навчання дозволяють визначати ймовірність того, що конкретний голос належить певному фігуранту.

Так, у рамках аналізу відео розстрілу військовослужбовці Збройних Сил України, викладеного в мережі було виокремлено аудіо-треки для навчання нейромережі та порівняння зі зразками фонограм, досліджених у рамках OSINT-розвідки. Крім того, з відкритих джерел проаналізовано відео, в якому зафіксовано військовослужбовця 85-ї бригади «южною групування військ» із позивним Варяг. Під час аналізу здійснено порівняння відповідних матеріалів, зафіксованих на відео розстрілу та відео, отриманого під час проведення OSINT-розвідки, в результаті якого встановлено 60% співпадіння.

Крім того, у теперішній час штучний інтелект використовується для планування розслідування, аналізу матеріалів кримінальних проваджень, а також вибору тактики проведення тієї чи іншої слідчої (розшукової) дії (ресурси на базі Палантір). Наприклад, із урахуванням даних про слідчу ситуацію та психологічні типи підозрюваних штучний інтелект може запропонувати найбільш раціональні прийоми допиту, його тривалість тощо.

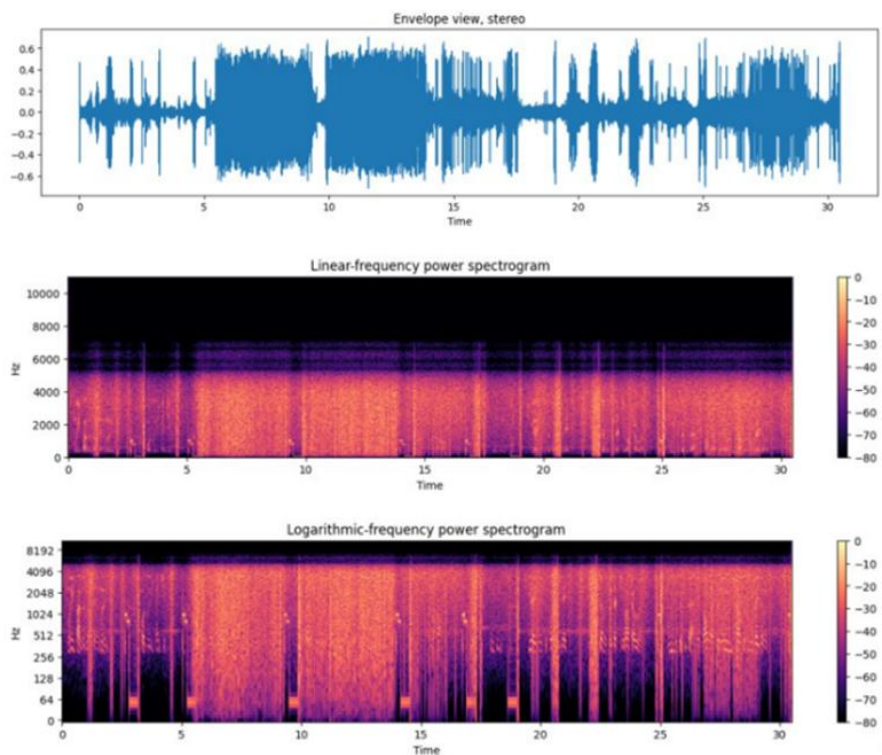


Рис. 1.

Використання інформаційних ресурсів банків даних, колекцій, систем та підсистем має здійснюватися в рамках оперативно-розшукової справи (контррозвідувальної справи) або кримінального провадження і тільки особою, якою заведено оперативно-розшукову справу, або яка входить до складу слідчої групи, створеної для розслідування кримінального провадження. Інформація про доступ до банку даних повинна фіксуватися та зберігатися в автоматизованій системі обробки даних, включно з інформацією про особу, яка отримала доступ, та про обсяг даних, доступ до яких було отримано. Кожна дія особи щодо отримання інформації з інформаційних ресурсів, фіксується у спеціальному електронному архіві інформаційно-комунікаційної системи, за допомогою якої отримано відомості.

Використання інформації отриманої з банків даних підсистем що містять відомості стосовно осіб, причетних до вчинення воєнних та інших злочинів буде найефективнішою за умови комплексної обробки з інформацією, яка міститься в закритих базах даних органів правопорядку, результатами оперативно-розшукових та оперативно-технічних заходів (у тому числі проведених оперативними службами), контррозвідувальних заходів, оброблених та проаналізованих з залученням аналітиків.

Тому, перспективними напрямками подальших наукових розвідок у цій сфері вважаємо:

- подальше машинне навчання нейромереж;
- залучення до процесу відповідного ідентифікаційного пошуку фахівців у галузі семантико-текстуальної, портретної та фототехнічної експертизи, експертизи аудіо-, звукозапису з подальшим призначенням відповідних судових експертиз для верифікації відповідних матеріалів та ідентифікації осіб (трупів) за ознаками обличчя, голосу, предметів одягу, взуття, місць підготовки, вчинення та приховання воєнних злочинів за ознаками місцевості з метою ймовірного використання в якості судових доказів;
- створення єдиної бази даних (картотеки) фонограм воєнних злочинців/державних зрадників;
- врегулювання (створення) процесуального механізму звернення з клопотанням до прокурора під час ведення контррозвідувальних заходів (у рамках контррозвідувального пошуку) з метою створення можливості використання матеріалів контррозвідувальної діяльності як доказів.

**Бочаров С. В.,**  
старший офіцер відділу,  
доктор філософії (PhD) в галузі воєнних наук  
(*Національна академія Державної прикордонної  
служби України імені Богдана Хмельницького*)

## **ВИКОРИСТАННЯ OSINT В ОПЕРАТИВНО-РОЗШУКОВІЙ ДІЯЛЬНОСТІ**

Сучасний розвиток технологій суттєво трансформував підходи до збору, обробки та аналізу інформації в оперативно-розшуковій діяльності (ОРД). Одним із ключових інструментів у цій сфері стала розвідка на основі відкритих джерел – OSINT (Open-Source Intelligence). Вона передбачає використання загальнодоступних ресурсів, таких як засоби масової інформації, соціальні мережі, відкриті державні реєстри, а також супутникові знімки.

OSINT – це сукупність підходів, методів і технологій, спрямованих на отримання та подальше використання інформації військового, політичного, економічного та іншого характеру з відкритих джерел без порушення чинного законодавства. Така розвідка широко застосовується у сфері національної безпеки й оборони, а також під час проведення розслідувань. Вона охоплює повний цикл роботи з інформацією – від її пошуку й відбору до аналітичної обробки та практичного використання для вирішення спеціальних завдань.

У контексті ОРД OSINT є допоміжним інструментом, який дозволяє оперативним підрозділам швидко отримувати та перевіряти інформацію без залучення складних дозвільних процедур, які обмежують права і свободи громадян.

На відміну від традиційних способів ОРД, OSINT використовує виключно доступні дані, такі як відкриті бази даних і реєстри, засоби масової інформації (онлайн- та друковані видання), соціальні мережі (SOCMINT), аналітичні звіти та публічні дослідження, супутникові знімки та геопросторові дані (GEOINT). OSINT дає змогу виявляти зв'язки між особами, групами та подіями, оцінювати рівень загроз і відстежувати діяльність підозрюваних без необхідності безпосереднього контакту з ними.

Розвідка з відкритих джерел часто інтегрується з іншими напрямками збору оперативних даних, які застосовуються західними партнерами, зокрема: HUMINT (Human Intelligence) – агентурна розвідка, що базується на особистих контактах; SIGINT (Signals Intelligence) – перехоплення комунікаційних сигналів; COMINT (Communications Intelligence) – аналіз змісту перехоплених повідомлень; IMINT (Imagery Intelligence) – аналіз зображень, отриманих із супутників або безпілотних систем. Ключова відмінність OSINT, від згаданих заходів, полягає у відкритому характері отриманої інформації, що робить цю діяльність більш доступною, але водночас менш надійною порівняно зі способами, які передбачають роботу з конфіденційними (інсайдерськими) даними.

OSINT як окремий напрям діяльності активно розвивається з кінця XX століття завдяки поширенню цифрових технологій. У 1990-х роках у США його офіційно визнали джерелом стратегічної інформації, а після терактів 11 вересня 2001 року значення OSINT суттєво зросло, особливо для сфери національної безпеки. У країнах НАТО він використовується для моніторингу військових загроз, виявлення терористичних угруповань і боротьби з гібридними загрозами. В Україні цей підхід набув особливої важливості після 2014 року в контексті інформаційної та військової боротьби з агресією.

Використання OSINT в ОРД базується на різних способах збору, які дозволяють оперативним підрозділам отримувати інформацію з відкритих джерел. Основні методи включають: моніторинг засобів масової інформації – аналіз публікацій у друкованих та онлайн-виданнях для виявлення ознак злочинної діяльності, політичних загроз чи тенденцій у суспільстві; аналіз соціальних мереж (SOCMINT – Social Media Intelligence) – відстеження активності підозрюваних у Facebook, Twitter, Instagram, Telegram та інших платформах для виявлення зв'язків, намірів та місцезнаходження; обробка відкритих баз даних – використання державних реєстрів, комерційних баз, судових рішень та корпоративної документації для отримання інформації про осіб, компанії та фінансові операції; геопросторовий аналіз (GEOINT – Geospatial Intelligence) – використання супутникових знімків, даних геолокації та картографічних сервісів для встановлення місцезнаходження об'єктів або осіб; веб-скреїпінг (Web Scraping) – автоматизоване вилучення інформації з веб-сайтів, форумів, баз даних та інших онлайн-ресурсів; зворотний пошук зображень – використання інструментів для перевірки достовірності фотографій та ідентифікації осіб або об'єктів; Dark Web OSINT – збір інформації з ресурсів у «темному» сегменті інтернету [1].

Сучасні технології дозволяють значно прискорити обробку даних за допомогою спеціалізованих інструментів. Серед найбільш популярних: Maltego – платформа для аналізу зв'язків між особами, компаніями, IP-адресами та доменами; Shodan – пошукова система для виявлення відкритих пристроїв та мережевих інфраструктур, що можуть бути вразливими для кібератак; Google Dorking – методика розширеного пошуку в Google для знаходження прихованих або незахищених файлів та сторінок; SpiderFoot – автоматизований інструмент збору даних про IP-адреси, домени, електронні адреси та цифрові сліди; CheckUserNames – сервіси для перевірки реєстрації користувачів у різних соцмережах та форумах; ExifTool – програма для аналізу метаданих фото- та відеофайлів, що дозволяє отримати інформацію про місце та час зйомки; The Wayback Machine – архіватор веб-сайтів, який допомагає відстежувати зміни сторінок у часі та отримувати доступ до видаленого контенту [2].

Використання OSINT у правоохоронній діяльності потребує чіткої правової регламентації, оскільки збір і аналіз інформації з відкритих джерел можуть впливати на права людини. В Україні ОРД регулюється Законом України «Про оперативно-розшукову діяльність» [3], який визначає правові підстави, методи та обмеження збору інформації. Водночас конкретного нормативного акту, що детально регулював би використання OSINT, поки немає, тому застосування цього методу пошуку здійснюється в межах загального законодавства, зокрема: Конституції України, яка гарантує право на захист особистої інформації (ст. 32) [4]; Закону України «Про інформацію» [5], що визначає принципи доступу до відкритих джерел. Закону України «Про захист персональних даних» [6], який регламентує обробку інформації про осіб. Кримінального процесуального кодексу України, що встановлює вимоги до доказової бази.

Подальший розвиток цієї сфери залежить як від технологічних досягнень, зокрема впровадження штучного інтелекту та новітніх аналітичних інструментів, так і від здатності державних органів пристосувати правову базу до сучасних викликів, серед яких протидія дезінформації та забезпечення міжнародної координації у сфері цифрової розвідки.

### Список використаних джерел

1. Задерейко О., Долінко К. GEOINT: можливості геопросторової розвідки. *Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика* : матеріали Міжнародної науково-практичної конференції (м. Одеса, 24 листопада 2023 року). Одеса, 2023. С. 118–122. URL: <https://dspace.onua.edu.ua/items/e0713052-8aa4-40b3-b182-e45bff5ebf36> (дата звернення: 03.03.2025 р.).
2. Sayer P., Brenner B. 21 best free security tools. CSO. 2021. URL: <https://www.csoonline.com/article/565492/21-best-free-security-tools.html> (дата звернення: 03.03.2025 р.).
3. Про оперативно-розшукову діяльність : Закон України від 18 лютого 1992 року № 2135-XII. *Відомості Верховної Ради України*. 1992. № 22. Ст. 303.
4. Конституція України. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.
5. Про інформацію : Закон України від 02 жовтня 1992 року № 2657-XII. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650.
6. Про захист персональних даних : Закон України від 01 червня 2010 року № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481.

## **РОЛЬ КРИМІНАЛЬНОГО АНАЛІЗУ В РОЗВИТКУ ПОЛІЦЕЙСЬКОЇ АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ**

Сучасна правоохоронна діяльність - це комплексна динамічна система, що має постійно розвиватися, балансує між різноманітними загрозами та забезпечуючи необхідний рівень громадської безпеки. У світі, де злочинність стає дедалі більш прихованою, мережевою та високотехнологічною, традиційних методів патрулювання чи реагування на окремі виклики вже недостатньо для стабілізації криміногенної ситуації.

Ефективне управління такою складною системою вимагає не просто фізичної присутності поліції, а насамперед розуміння прихованих процесів у злочинному середовищі.

За таких умов Департамент кримінального аналізу виступає підрозділом, на який 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.

На постійній основі Департаментом вживаються заходи щодо розбудови та розширення аналітичних спроможностей служби, підвищення рівня ефективності інформаційно-аналітичної діяльності з урахуванням дії правового режиму воєнного стану. Ця робота супроводжується співпрацею з міжнародними партнерами та адаптацією досвіду розвинених поліцейських систем світу.

Основою цієї трансформації виступає філософія ІІР (Intelligence-led policing – далі ІІР) – модель правоохоронної діяльності, що керується аналітичною розвідкою. Дана концепція передбачає впровадження комплексного проактивно-превентивного підходу, який базується на використанні надійних статистичних даних, глибинного аналізу та якісних аналітичних продуктів для формування картини криміногенної ситуації та забезпечення ефективного планування діяльності й ухвалення рішень керівництвом.

Основою сучасної аналітичної діяльності є розвідка з відкритих джерел (OSINT), роль якої у структурі кримінального аналізу сьогодні неocenenna. У сучасному світі, де кожен крок залишає цифровий відбиток, OSINT дозволяє перетворити розрізнений цифровий слід у доказ, а загальнодоступну інформацію – у юридично підтверджений факт. Це не просто збір даних, а високотехнологічний інструмент, що забезпечує моніторинг медіапростору, виявлення ворожих інформаційно-психологічних операцій (ІІСО) та верифікацію даних, що впливають на національну безпеку.

Логіка цієї діяльності базується на переході від хаотичного споживання контенту до системного вилучення знань, де аналітик виступає ключовою ланкою у перетворенні «цифрового шуму» на структуровану аналітичну картину. Для забезпечення безперервності цього процесу, аналітики підрозділів кримінального аналізу мають автоматизований доступ до 26 інформаційних і довідкових систем, державних реєстрів та банків даних, перелік яких постійно розширюється. Зазначене дозволяє не лише встановлювати хронологію подій чи авторство повідомлень, а й проводити геопросторовий аналіз, ідентифікуючи об'єкти та місцевість за найдрібнішими візуальними деталями.

В роботі з аналітикою основний акцент робиться на точності, актуальності та структурованості аналітичних продуктів. Однак відсутність єдиних загальноприйнятих міжнародних стандартів для OSINT створює виклики у питанні уніфікації практик та забезпеченні якості кінцевих результатів.

У зв'язку з цим, головним орієнтиром під час підготовки матеріалів виступає Протокол Берклі, представлений у 2020 році Центром прав людини Університету Берклі в Каліфорнії та Офісом Верховного комісара ООН з прав людини. Цей документ став першою в історії успішною спробою систематизувати етичні, правові та технічні вимоги до збору, зберігання та аналізу цифрових даних з відкритих джерел, який закладає підґрунтя для дотримання принципів надійності та допустимості цифрових доказів у судових процесах, що є важливим для документування воєнних злочинів та злочинів проти людяності. В умовах воєнного стану впровадження стандартів Протоколу Берклі є пріоритетним напрямом для України, оскільки він забезпечує професіоналізацію збору інформації та дозволяє готувати аналітичні матеріали, придатні для подальшого використання у 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 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. Це дозволяє аналітикам не лише відстежувати інформаційне поле, а й своєчасно розпізнавати ознаки підготовки дестабілізаційних заходів чи ворожих операцій впливу.

Окремим напрямом OSINT є геопросторовий аналіз, що базується на вивченні фото, відео та супутникових знімків. Аналітики здатні ідентифікувати місцевість за архітектурними особливостями, дорожньою розміткою, специфічними видами рослинності чи навіть за напрямком і довжиною тіней, що вказують на точну пору доби та орієнтацію об'єкта у просторі. Такий аналіз ґрунтується на деталях, що можуть здаватися другорядними, але містять інформацію для ідентифікації локації та верифікації подій. Це дозволяє з високою точністю підтверджувати факти та оцінювати оперативну обстановку в районах, де фізичний доступ наразі обмежений, зокрема на тимчасово окупованих територіях або в зонах активних бойових дій.

Повномасштабна війна внесла корективи в діяльність підрозділів кримінального аналізу, суттєво розширивши спектр завдань та змінивши методіку роботи в умовах високої невизначеності. Сьогодні аналітик змушений працювати з вкрай розрізненими та фрагментарними джерелами, що походять безпосередньо із зон активних бойових дій та тимчасово окупованих територій. Його ключовим завданням стає здатність «зшивати» окремі інформаційні пазли у цілісну та несуперечливу аналітичну картину, яка дозволяє приймати точні оперативні та стратегічні рішення.

Така робота потребує від аналітиків не лише професійної майстерності, а й обізнаності у специфічних деталях: від технічних характеристик військової техніки та знання позивних до розпізнавання типів військової форми та знаків розрізнення підрозділів агресора. Володіння такими знаннями забезпечує спроможність ідентифікації осіб, причетних до вчинення воєнних злочинів та злочинів проти людяності. Навіть у ситуаціях, коли мотив правопорушення виглядає ірраціональним, а основні докази перебувають під окупацією, кримінальний аналіз забезпечує обґрунтування та доказовість висновків слідчих і оперативників.

Вміння перетворювати розрізнені цифрові відбитки на структуроване знання дозволяє правоохоронним органам долати інформаційну асиметрію війни та забезпечувати невідворотність покарання. Таким чином, кримінальний аналітик сьогодні виступає інтелектуальною опорою для всього процесу розслідування, забезпечуючи перехід від простого збору фактів до глибокого розуміння прихованої логіки злочинних дій.

Майбутнє кримінального аналізу визначається синергією методів обробки великих даних (Big Data) та комплексного інструментарію OSINT, що інтегруються у межах моделі ІІР для формування цілісної аналітичної картини. Системна обробка цифрових слідів у сукупності з автоматизованим доступом до державних реєстрів забезпечує верифікацію фактів і логічне обґрунтування висновків навіть за умови роботи з фрагментарними джерелами у зонах бойових дій. Спроможність трансформувати цей інформаційний масив на стратегічну перевагу забезпечує ефективне виконання основних завдань поліції у сферах протидії злочинності та підтримання публічної безпеки і порядку.

**Винник С. С.,**  
аспірант кафедри менеджменту та економічної безпеки  
навчально-наукового інституту  
управління, психології та безпеки  
(Львівський державний університет внутрішніх справ)

## **ІНФОРМАЦІЙНО-АНАЛІТИЧНІ МЕХАНІЗМИ ФІНАНСОВОГО МОНІТОРИНГУ БАНКІВ У ЗАБЕЗПЕЧЕННІ ДОТРИМАННЯ САНКЦІЙ**

У сучасній системі міжнародної фінансової безпеки дотримання санкційних режимів значною мірою залежить від ефективності інформаційно-аналітичних механізмів фінансового моніторингу, у межах якого санкційна політика дедалі тісніше інтегрується з архітектурою протидії фінансовим злочинам (*AML/CFT framework*). Банки, як первинні суб'єкти фінансового моніторингу, виконують ключову роль у виявленні операцій, пов'язаних із підсанкційними особами, обходом санкційних обмежень та прихованими фінансовими потоками. Ці механізми забезпечують виявлення, аналіз та передачу інформації про фінансові операції, які можуть бути пов'язані з підсанкційними особами, обходом санкцій або фінансуванням забороненої діяльності.

Згідно з підходами *FATF*, фінансові установи повинні застосовувати ризик-орієнтований підхід (*risk-based approach*) до ідентифікації та управління ризиками відмивання коштів, фінансування тероризму та фінансування розповсюдження зброї масового знищення, що включає і ризики, пов'язані з міжнародними санкціями. Так, відповідно до Рекомендації 6 *FATF*, держави повинні забезпечити механізми цільових фінансових санкцій (*targeted financial sanctions*), а фінансові установи – негайне виконання заходів із блокування активів та недопущення проведення фінансових операцій підсанкційними суб'єктами [1].

Хоча санкції встановлюються державами або міжнародними організаціями (наприклад, ЄС чи США), саме банки здійснюють практичне забезпечення їх виконання через контроль фінансових потоків. Зокрема, у праві ЄС банки відповідають за реалізацію та моніторинг дотримання санкційних режимів, тоді як національні органи влади забезпечують розслідування порушень і застосування санкційних заходів [2]. Це означає, що банківська система фактично виконує роль первинного фільтра фінансових транзакцій, через який проходить переважна більшість міжнародних економічних операцій.

Однією з базових функцій банків є перевірка клієнтів і контрагентів щодо наявності у санкційних списках. Цей процес передбачає ідентифікацію клієнтів та їхніх бенефіціарних власників (*CDD/KYC*), регулярний скринінг клієнтів щодо санкційних списків, оновлення баз даних у разі змін санкційних режимів [3].

Інформаційно-аналітичні механізми фінансового моніторингу фактично формують інфраструктуру раннього виявлення ризиків обходу санкцій, яка інтегрована з інформаційними системами банків, базами санкційних списків, аналітичними інструментами обробки транзакцій, каналами взаємодії з органами фінансової розвідки тощо.

Функціонування аналітичних механізмів фінансового моніторингу ґрунтується на використанні широкого кола інформаційних джерел. До основних інформаційних масивів належать:

- санкційні списки міжнародних організацій та держав;
- внутрішні бази даних клієнтів фінансових установ;
- інформація про бенефіціарних власників;
- дані про транзакції та фінансові операції;
- звіти про підозрілі фінансові операції.

Фінансові установи повинні регулярно оновлювати власні інформаційні системи відповідно до змін у цих списках, що дає змогу здійснювати оперативну ідентифікацію підсанкційних суб'єктів. Дослідники наголошують, що санкційний комплаєнс дедалі більше набуває характеру діяльності, керованої даними (*data-driven*), в якій ключову роль відіграють інформаційні системи аналізу великих масивів фінансових даних. Інформаційно-аналітичний механізм фінансового моніторингу включає комплекс процедур обробки даних, спрямованих на виявлення ризиків санкційних порушень.

Першим етапом аналітичної обробки є скринінг клієнтів і транзакцій щодо санкційних списків. Цей процес передбачає автоматизовану перевірку клієнтів, перевірку бенефіціарних власників, перевірку контрагентів у платіжних операціях. Санкційний скринінг здійснюється як під час встановлення ділових відносин із клієнтом, так і на постійній основі під час проведення фінансових операцій.

Наступним ключовим елементом є моніторинг фінансових операцій, який дає змогу виявляти аномальні або підозрілі фінансові потоки шляхом аналізу структури платежів, географії фінансових потоків, частоти операцій, взаємозв'язків між учасниками фінансових операцій. У практиці фінансового моніторингу дедалі ширше застосовуються алгоритми машинного навчання, які виявляють складні схеми обходу санкцій через мережі посередників або транзитні юрисдикції.

Одним із найбільш перспективних аналітичних інструментів є мережевий аналіз фінансових зв'язків. Цей підхід дає змогу встановлювати приховані зв'язки між компаніями, ідентифікувати ланцюги транзакцій, виявляти складні схеми посередництва. Мережевий аналіз активно використовується органами фінансової розвідки, які входять до міжнародної мережі *Egmont Group*, що забезпечує обмін аналітичною інформацією між фінансовими розвідками різних держав.

Результатом функціонування інформаційно-аналітичних механізмів фінансового моніторингу є формування повідомлень про підозрілі фінансові операції. Такі повідомлення передаються до органів фінансової розвідки для подальшого аналізу з метою співставлення даних із різних джерел, встановлення зв'язків між транзакціями, виявлення схем обходу санкцій, формування аналітичних матеріалів для правоохоронних органів.

Ефективність інформаційно-аналітичних механізмів фінансового моніторингу значною мірою залежить від міжнародного обміну фінансовою інформацією. Безпосередньо такий обмін здійснюється через міжнародні мережі фінансових розвідок, міждержавні угоди, механізми взаємної правової допомоги. Загалом міжнародна співпраця дає можливість встановлювати транскордонні фінансові схеми обходу санкцій, що особливо важливо в умовах використання складних багаторівневих фінансових структур.

Інформаційно-аналітичні механізми фінансового моніторингу є ключовим елементом забезпечення ефективності санкційної політики. Їх функціонування базується на інтеграції інформаційних ресурсів, автоматизованому аналізі фінансових операцій та міжнародному обміні фінансовою інформацією.

Завдяки використанню сучасних аналітичних технологій фінансовий моніторинг дає змогу не лише виявляти прямі порушення санкційного режиму, але й ідентифікувати складні схеми його обходу через мережі посередників, транзитні юрисдикції та підставні компанії. Таким чином, інформаційно-аналітичні механізми фінансового моніторингу формують основу інституційної спроможності держав забезпечувати дотримання міжнародних санкцій.

У цьому контексті фінансові розвідки виступають центральними аналітичними вузлами санкційного контролю для інтегрування інформації від банків, митних органів, правоохоронних органів та міжнародних партнерів.

### **Список використаних джерел**

1. Financial Action Task Force. URL: <https://www.fatf-gafi.org/en/home.html> (дата звернення: 20.04.2026)
2. FAQs on Russia's war against Ukraine and ECB Banking Supervision. URL: [https://www.bankingsupervision.europa.eu/press/other-publications/publications/html/ssm.faq\\_Russia\\_Ukraine\\_war\\_and\\_Banking\\_Supervision~8360ccdf6f.en.html](https://www.bankingsupervision.europa.eu/press/other-publications/publications/html/ssm.faq_Russia_Ukraine_war_and_Banking_Supervision~8360ccdf6f.en.html) (дата звернення: 20.04.2026)
3. OFAC Compliance for Banks: Requirements and Procedures. URL: <https://legalclarity.org/ofac-compliance-for-banks-requirements-and-procedures> (дата звернення: 20.04.2026)

**Візничак І.-Д. В.,**  
здобувач вищої освіти  
*(Львівський державний університет внутрішніх справ)*  
**Новаковська У. Ю.,**  
здобувач вищої освіти  
*(Львівський державний університет внутрішніх справ)*

## **ІНТЕГРАЦІЯ OSINT У ДІЯЛЬНІСТЬ ПРАВООХОРОННИХ ОРГАНІВ УКРАЇНИ**

Інтеграція OSINT у діяльність правоохоронних органів України є одним із напрямів модернізації системи кримінальної юстиції в умовах цифровізації та збройного конфлікту. Використання відкритих джерел забезпечує розширення можливостей збору доказової інформації, особливо за умов обмеженого доступу до місця подій. Разом з тим ефективність застосування OSINT залежить від нормативного врегулювання, технічного забезпечення та міжвідомчої координації. В Україні вже сформовано практику використання OSINT у розслідуванні воєнних злочинів, кіберзлочинів та економічних правопорушень.

OSINT застосовується у різних напрямках правоохоронної діяльності. У сфері кіберзлочинності та протидії контрабанді аналіз відкритих джерел дає змогу виявляти цифрові сліди злочинів, досліджувати фінансові потоки, соціальні зв'язки та транскордонні операції. Використання супутникових знімків, відкритих реєстрів і соціальних мереж забезпечує обробку великих масивів інформації та підвищує ефективність аналітичної роботи [1].

У сфері розслідування воєнних злочинів і терористичної діяльності OSINT виступає джерелом доказів, що відповідають міжнародним стандартам. Практика свідчить, за допомогою відкритих джерел можна ідентифікувати підозрюваних, встановлювати обставини подій і формувати доказову базу навіть за відсутності безпосереднього доступу до території [2]. Аналогічно, у сфері протидії корупції відкриті джерела використовуються для верифікації даних, зазначених у деклараціях, аналізу тендерних процедур та встановлення зв'язків посадових осіб.

Окремим напрямком є розшук осіб, зокрема зниклих безвісти, де застосовуються технології розпізнання обличчя, аналізу зображень та геолокації. Також OSINT часто використовується для превенції злочинності шляхом моніторингу інформаційного простору, виявлення дезінформації та прогнозування ризиків.

Організаційна інтеграція передбачає створення спеціалізованих підрозділів у структурі правоохоронних органів та забезпечення міжвідомчої взаємодії. Важливим елементом є використання єдиних інформаційних систем, зокрема ЄІС МВС, що забезпечує обмін даними та координацію аналітичної діяльності [3]. Технічна складова включає використання спеціалізованого програмного забезпечення, у тому числі аналітичні платформи, геоаналітики, а також автоматизація збору та аналізу даних, застосування штучного інтелекту [4].

Кадрове забезпечення є ключовим фактором ефективності. Підготовка фахівців повинна включати розвиток аналітичного мислення, цифрових навичок, знання правових обмежень і методів перевірки інформації. Практика міжнародних тренінгів підтверджує ефективність системного навчання та необхідність сертифікації спеціалістів.

Правове регулювання OSINT в Україні залишається недостатнім. Відсутність законодавчого визначення цього поняття призводить до різного тлумачення його статусу, як звичайного пошуку інформації або ж як елементу оперативно-розшукової діяльності. Це створює ризики визнання отриманих даних недопустимими доказами. Водночас законодавство про захист персональних даних дає змогу використовувати інформацію, оприлюднену самою особою, що формує правову основу для OSINT, але потребує дотримання принципів законності, пропорційності та мінімізації втручання [5].

Підсумовуючи, інтеграція OSINT у діяльність правоохоронних органів України забезпечує підвищення ефективності розслідування злочинів, розширення можливостей доказування та розвиток аналітичних інструментів. Водночас повноцінне використання цього інструменту можливе лише за умов нормативного врегулювання, підготовки кадрів і забезпечення міжвідомчої взаємодії. Усунення правової невизначеності, впровадження єдиних стандартів роботи з відкритими даними та розвиток технічної бази є необхідними умовами для ефективного та правомірного застосування OSINT у правоохоронній діяльності.

### **Список використаних джерел**

1. OSCE assists Ukrainian law enforcers in investigating cybercrimes and trafficking in human beings. URL: <https://www.osce.org/support-programme-for-ukraine/545248>
2. Європол створив оперативну робочу групу OSINT для підтримки розслідувань воєнних злочинів в Україні. URL: <https://mvs.gov.ua/news/jevropol-stvoriv-operativnu-robocugrupu-osint-dlia-pidtrimki-rozsliduvan-vojennix-zlociniv-v-ukrayini>
3. Єдина інформаційна система МВС України. URL: <https://infotech.gov.ua/projects/eis-mvs>
4. Ukrainian Law Enforcement Officers Strengthen OSINT Skills in Joint EUBAM and OLAF Training. URL: <https://eubam.org/newsroom/ukrainian-law-enforcement-officers-strengthen-osint-skills-in-joint-eubam-and-olaf-training/>
5. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>

**Волобоєва З. О.,**  
здобувач вищої освіти  
*(Донецький державний університет внутрішніх справ)*  
Науковий керівник: **Габорець О. А.,**  
доцент кафедри оперативної розшукової  
діяльності та інформаційної безпеки, доктор філософії, доцент  
*(Донецький державний університет внутрішніх справ)*

## **OSINT ЯК ЗАСІБ ВИЯВЛЕННЯ ТА ФІКСАЦІЇ ЗЛОЧИНІВ АГРЕСІЇ ПРОТИ УКРАЇНИ**

Збройна агресія росії проти України стала не лише найбільшим безпековим викликом для Європи ХХІ століття, а й своєрідним випробуванням для сучасної системи міжнародного правосуддя. Якщо в попередні історичні періоди факти агресивних війн, воєнних злочинів та злочинів проти людяності встановлювалися переважно на підставі дипломатичних архівів, свідчень очевидців, матеріалів військових місій та документів державних органів, то сучасний збройний конфлікт існує одночасно у фізичному та цифровому вимірах. Майже кожна ракетна атака, пересування військової техніки, обстріл цивільного об'єкта чи поява окупаційних сил залишають цифровий слід у вигляді супутникових знімків, відеозаписів, публікацій у соціальних мережах, геолокаційних даних, електронних повідомлень та метаданих. За цих умов відкрита розвідка перетворюється з допоміжного інструменту аналізу на самостійний механізм фіксації міжнародних злочинів.

Саме тому дослідження OSINT як засобу виявлення та документування злочинів агресії проти України набуває не лише прикладного, а й фундаментального значення. Йдеться про переосмислення самої природи доказування в умовах цифрової війни, коли доказ нерідко виникає раніше, ніж на місце події прибуває слідчий, а джерелом відомостей стають не державні інституції, а цивільні особи, журналісти, волонтери або автоматизовані цифрові сервіси.

Поняття OSINT традиційно розкривається як процес пошуку, збору, аналізу та використання інформації з відкритих джерел для вирішення конкретних завдань у сфері безпеки, розслідувань чи аналітики. В сучасних умовах його зміст суттєво розширився. Якщо раніше йшлося переважно про моніторинг друкованих видань, радіомовлення або відкритих державних реєстрів, то сьогодні ключовими джерелами виступають цифрові платформи, супутникові сервіси, месенджери, відеохостинги та архіви мережевого контенту. Як слушно зазначають С. Кудінов і Р. Шехавцов, розвиток цифрових комунікацій створив нові можливості використання відкритої розвідки у кримінальному провадженні та встановленні обставин правопорушень [1].

Повномасштабне вторгнення РФ показало, що OSINT може використовуватися вже на етапі виявлення ознак підготовки злочину агресії. Ще до 24 лютого 2022 року міжнародні аналітичні групи на основі супутникових знімків, відео з прикордонних районів та відкритих повідомлень у мережі фіксували концентрацію російських військ, польових шпиталів, логістичних баз та військової техніки поблизу державного кордону України. Сукупність таких даних дозволяла зробити висновок про підготовку масштабної наступальної операції. Отже, відкрита розвідка стала інструментом раннього виявлення агресивних дій ще до їх формального початку.

Після початку вторгнення значення OSINT лише посилюється. Саме за допомогою відкритих джерел світова спільнота отримувала докази ракетних ударів по житлових кварталах, пологових будинках, школах, вокзалах, енергетичних об'єктах та гуманітарних маршрутах. У багатьох випадках фото і відео, оприлюднені очевидцями, були першими свідченнями злочину. Подальше зіставлення цих матеріалів із супутниковими знімками, метеорологічними даними, геолокацією та часовими мітками дозволяло підтвердити достовірність інформації.

Значна доказова цінність OSINT проявляється у можливості встановлення просторово-часових параметрів події. Наприклад, аналіз тіней на фото дозволяє орієнтовно визначити час зйомки, особливості ландшафту – місце події, а повторне співставлення з картографічними сервісами – точні координати. Такі методи вже стали звичними у міжнародних розслідуваннях. О. Нарожна, досліджуючи використання відкритої розвідки у справах про знищення культурної спадщини, зазначає, що поєднання супутникових матеріалів, архівних фото, метаданих та соціальних мереж дозволяє не лише зафіксувати факт руйнування, а й відтворити його механізм та часові межі [2]. Аналогічна логіка повною мірою застосовується й до документування злочинів агресії.

Не менш важливим напрямом є ідентифікація осіб, причетних до злочинних дій. Якщо воєнні злочини часто пов'язані з конкретними виконавцями на місці події, то злочин агресії має інший рівень суб'єкта – це особи, які здатні фактично контролювати політичні чи військові дії держави. Водночас саме відкриті джерела нерідко містять відомості про структуру командування, кадрові рішення, переміщення генералів, нагородження підрозділів, офіційні заяви посадових осіб, координацію військових операцій. Такі дані мають значення для встановлення вертикалі відповідальності та зв'язку між наказом і наслідками.

О. Сіфоров та В. Калугін слушно наголошують, що OSINT особливо ефективний у встановленні фактів воєнних злочинів та осіб, причетних до їх вчинення, оскільки поєднує оперативність отримання інформації з можливістю її багаторазової перевірки [3]. Для України це має особливе значення, адже значна кількість злочинів була вчинена на тимчасово окупованих територіях, доступ до яких тривалий час був відсутній.

Окремого значення відкрита розвідка набуває у протидії інформаційним операціям держави-агресора. Сучасна війна супроводжується масштабним використанням фейкових повідомлень, постановочних матеріалів, маніпулятивних нарративів та кампаній із заперечення очевидних фактів. Після кожного масованого обстрілу цивільної інфраструктури російська пропаганда системно поширює версії про «самообстріли», «військові цілі» або «інсценування». У таких умовах OSINT виконує не лише доказову, а й контрdezінформаційну функцію. Як справедливо зауважує М. О. Думчиков, відкрита розвідка стала одним із ключових механізмів викриття фейкових нарративів та встановлення реального перебігу подій у сучасних інформаційних війнах [4].

Разом із тим використання OSINT у кримінальному процесі породжує низку складних юридичних питань. Передусім ідеться про допустимість цифрових доказів. Для використання фото, відео чи архівованих вебматеріалів необхідно встановити їх походження, цілісність, відсутність змін та маніпуляцій. Особливого значення набуває ланцюг збереження доказу, тобто фіксація того, ким, коли і яким способом було отримано матеріал. За відсутності належної процедури сторона захисту може ставити під сумнів достовірність таких відомостей.

Українська правова система поступово адаптується до нових реалій, однак чинне кримінальне процесуальне законодавство ще не містить достатньо чіткої регламентації використання OSINT-матеріалів. У зв'язку з цим пропозиції щодо внесення відповідних змін до КПК України, висловлені у науковій літературі, видаються своєчасними та обґрунтованими [5]. Ідеться не лише про формальне визнання відкритої розвідки як джерела доказів, а й про встановлення процедур їх фіксації, оцінки та процесуального оформлення.

Таким чином, OSINT у сучасних умовах став одним із найефективніших засобів виявлення та фіксації злочинів агресії проти України. Його значення полягає у здатності оперативно документувати події, встановлювати причетних осіб, спростовувати дезінформацію та формувати доказову базу для національних і міжнародних судових інстанцій. Водночас подальший розвиток цього інструменту потребує належного нормативного врегулювання, підготовки фахівців у сфері цифрової криміналістики та вироблення єдиних стандартів оцінки цифрових доказів.

### **Список використаних джерел**

1. Кудінов С. С., Шехавцов Р. М. Правове регулювання використання OSINT та його результатів під час встановлення обставин кримінальних правопорушень. *Науковий вісник Львівського державного університету внутрішніх справ*. Серія юридична. 2025. № 3. С. 126–133.
2. Нарожна О. Використання відкритої розвідки у розслідуванні знищення культурної спадщини під час війни. *Криміналістика і судова експертиза*. 2025. Вип. 70. С. 191–205.
3. Сіфоров О., Калугін В. Використання OSINT у встановленні фактів воєнних злочинів та особи воєнних злочинців. *Правове регулювання дотримання прав і свобод людини та громадянина в умовах адміністративно-правового режиму воєнного стану* : колективна монографія / за заг. ред. А. В. Денисової. Одеса : Юридика, 2025. С. 811–830.
4. Думчиков М. О. Відкрита розвідка (OSINT) у протидії інформаційним війнам: аналітичні інструменти та правові межі. *Аналітично-порівняльне правознавство*. 2025. Вип. 06. Ч. 2. С. 273–278.
5. Тома М. Г., Василюва О. В. Інструменти OSINT: фіксація воєнних злочинів в Україні. *Аналітично-порівняльне правознавство*. 2025. Вип. 02. С. 905–910.

**Воропаєв Д. В.,**  
здобувач вищої освіти  
*(Харківський національний університет внутрішніх справ)*  
**Коцюба І. Ю.,**  
здобувач вищої освіти  
*(Харківський національний університет внутрішніх справ)*

## **ЦИФРОВА АНОНІМНІСТЬ У СУЧАСНОСТІ: ВИКЛИК ДЛЯ КІБЕРБЕЗПЕКИ ЧИ ОСНОВА ЦИФРОВИХ ПРАВ**

За останні роки Україна перебуває у важкому стані війни, в процесі якої важливо зберігати кібергігієну. Одна із складових кіберзахисту є анонімність. Вона дозволяє приховувати цифрову ідентичність, зокрема з використанням VPN, мережі Tor, криптографічних інструментів та децентралізованих платформ. Але слід зауважити, що анонімність працює не лише на користь звичайних користувачів, а й на кіберзлочинців, створюючи їм сприятливі для здійснення злочинів. Тому зростання рівня кіберзагроз включає в собі проблему пошуку балансу між забезпеченням цифрових прав та необхідністю протидії кіберзлочинам. Анонімність це і про інструмент захисту особистої свободи, так і про механізм уникнення відповідальності та приховування протиправної діяльності.

В загальному розумінні цифрова анонімність – це право людини контролювати приватні дані про себе під час будь-яких дій в інтернеті, зокрема використання вебсайтів, соціальних мереж, месенджерів, мобільних застосунків та онлайн-сервісів. Це право було визнане в ООН у 2015. Організація закликала уряди країн забезпечити умови для його реалізації. Так, вже 14 квітня 2016 Європейський Союз прийняв GDPR – Загальний регламент про захист даних – документ, що покликаний надати громадянам та резидентам ЄС контроль за їхніми персональними даними. В Україні питання збирання, використання та поширення конфіденційної інформації про особу без її згоди регулюється Конституцією України, зокрема статтею 32, Законами України «Про захист персональних даних» та «Про інформацію», Наказом Омбудсмана України «Про затвердження документів у сфері захисту персональних даних»[1].

Для забезпечення анонімності користувачі звертаються до технологій, які дозволяють приховати особу користувача та його слід у мережі. Найпопулярніший такий метод є VPN-сервіси, які шифрують трафік та приховують IP-адрес. Також слід звернути на мережу Tor, яка працює за рахунок розподілу системи вузлів ускладнює відстеження джерела трафіку [2].

Також важливу роль у забезпеченні анонімності відіграють криптографічні методи захисту інформації, зокрема використання безпечних протоколів передачі даних, що забезпечують конфіденційність комунікацій [3].

Так само використання технологій створює можливості не лише для захисту конфіденційності, а й для незаконної діяльності, що робить правову базу ще важливішою з точки зору кібербезпеки.

Окрім захисту конфіденційності користувачів, онлайн-анонімність також становить загрозу безпеці в Інтернеті. Кіберзлочинці можуть використовувати її, щоб приховати свою особу, що ускладнює їхню ідентифікацію та відстеження. Зокрема, анонімні мережі та пристрої створюють можливість здійснювати фішингові атаки, розповсюдженню шкідливого програмного забезпечення та несанкціонований доступ до інформаційних систем.[4]

Існують приховані області інтернету, такі як Tor, які зазвичай використовуються для діяльності в даркнеті. Такі платформи ускладнюють ідентифікацію користувачів та моніторинг їхньої діяльності, що викликає занепокоєння щодо незаконних ринків, обмеженого доступу до інформації та координації кіберзлочинності.[5]

В умовах гібридних конфліктів анонімність також використовується для проведення інформаційно-психологічних операцій та кібератак на критичну інфраструктуру держави, що підвищує рівень загроз національній безпеці.[6]

У сучасному цифровому середовищі постійно існує конфлікт між забезпеченням права та приватність та необхідністю підтримання кібербезпеки. З одного боку, цифрова анонімність та захист персональних даних є фундаментальними правами людини, що гарантують свободу слова та конфіденційність. З іншого боку, повна анонімність мережі ускладнює роботу правоохоронних органів у боротьбі з кіберзлочинністю.

У міжнародній практиці зусилля щодо досягнення цієї мети відображені в документах ООН, де наголошується на важливості захисту приватності та збереження національної безпеки. Аналогічний підхід реалізований у General Data Protecting Regulation (GDPR) який встановлює принципи обробки даних, але передбачає винятки для правоохоронних цілей.[7]

В Україні цей баланс забезпечується Конституцією та спеціальним законом про захист інформації, які обмежують втручання у приватність лише за умов законності, обґрунтованості та пропорційності.[8]

Цифрова анонімність у сучасних цифрових технологіях – це багатогранне явище, яке одночасно становить загрозу правам людини та безпеці в Інтернеті. Вона забезпечує реалізацію права на приватність, свободу вираження поглядів та захист персональних даних, що підтверджується міжнародними та національними правовими нормами.

Водночас, поява технологій анонімності, таких як віртуальні приватні мережі (VPN), інструменти шифрування та мережа Tor, відкрила можливості для використання цих інструментів для скоєння злочинів, особливо кіберзлочинів та хакерських атак.

Тому головним завданням кібербезпеки сьогодні є пошук правильного балансу між захистом цифрових прав користувачів та ефективною протидією кіберзагрозам. Подальший розвиток у цій галузі включає інтеграцію правових, технологічних та організаційних рамок захисту даних.

#### **Список використаних джерел**

1. Горін Є. Факт. Артем Ляшанов про цифрову анонімність людини. *KP.UA*. URL: <https://kp.ua/ua/politics/a703508-fakt-artem-ljashanov-pro-tsifrovu-anonimnist-ljudini> (дата звернення: 17.04.2026).
2. The Tor Project | Privacy & Freedom Online. *Tor Project Anonymity Online*. URL: <https://www.torproject.org/about/history/> (дата звернення: 01.05.2026).
3. Frankel S., Hoffman P., Orebaugh A., Park R. Guide to SSL VPNs (NIST Special Publication 800-113). Gaithersburg: National Institute of Standards and Technology, 2008. URL: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-113.pdf> (дата звернення: 19.04.2026).
4. Cybercrime. *INTERPOL | The International Criminal Police Organization*. URL: <https://www.interpol.int/en/Crimes/Cybercrime> (дата звернення: 19.04.2026).
5. Cyber-attacks | Europol. *Europol*. URL: <https://www.europol.europa.eu/crime-areas/cyber-attacks> (дата звернення: 22.04.2026).
6. United Nations Convention against Cybercrime. *United Nations : Office on Drugs and Crime*. URL: <https://www.unodc.org/unodc/en/cybercrime/index.html> (дата звернення: 23.04.2026).
7. Regulation - 2016/679 - EN - gdpr - EUR-Lex. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (дата звернення: 25.04.2026).
8. Про інформацію. *Офіційний вебпортал парламенту України*. URL: <https://zakon.rada.gov.ua/laws/show/2657-12> (дата звернення: 28.04.2026).

**Гладій Б. В., Крючко К. С.,**  
здобувачі вищої освіти  
(Львівський державний університет внутрішніх справ)  
Науковий керівник: **Ревак І. О.,**  
завідувач науково-дослідної лабораторії  
OSINT-досліджень та безпекової аналітики ННІУПБ,  
доктор економічних наук, професор  
(Львівський державний університет внутрішніх справ)

## **ЦИФРОВА ІНДИФІКАЦІЯ ВІЙСЬКОВИХ ЗЛОЧИНЦІВ ЗАСОБАМИ OSINT**

У сучасному світі характер ведення збройних конфліктів зазнав фундаментальних трансформацій. Поряд із традиційним полем бою виник цифровий простір, який став не лише інструментом інформаційних операцій, а й безпрецедентним за масштабами архівом доказів. Традиційні методи розслідування воєнних злочинів, що базуються на фізичному доступі до місця події та опитуванні свідків, часто виявляються неможливими в умовах триваючих бойових дій або окупації територій. У цьому контексті особливого значення набуває OSINT Open-Source Intelligence – розвідка на основі відкритих джерел: супутникові зображення, соцмережі, відео, онлайн-платформи, офіційні реєстри. Цей метод забезпечує об'єктивність завдяки використанню відкритих даних, які можна незалежно перевірити. OSINT дає змогу фіксувати цифрові сліди злочинців: геолокації, фото, відео, коментарі, пости, метадані. За даними експертів спільнот, таких як *Molfar* та *OsintFlow*, аналітики можуть «збирати фрагменти правди», з яких реконструюють картину подій і доводять причетність конкретних осіб до злочинів.

Цифрова ідентифікація воєнних злочинців засобами OSINT сьогодні є не просто допоміжним методом, а ключовим елементом системи міжнародного правосуддя. Кожне відео в TikTok, допис у Threads, Instagram, супутниковий знімок або випадкове селфі військовослужбовця стає потенційним доказом, який за умови правильної фіксації може бути використаний у Міжнародному кримінальному суді або національних трибуналах. Інтернет-середовище є динамічним: контент може бути видалений, змінений або сфальсифікований за допомогою штучного інтелекту (дипфейків). Тому питання того, як саме проводиться цифрова ідентифікація – від верифікації особи до прив'язки її до конкретного часу та локації – є критично важливим для встановлення істини.

Впровадження OSINT-технологій дає змогу реалізувати принцип неминучості покарання: навіть якщо злочинець перебуває за межами досяжності фізичного правосуддя, його цифрова ідентифікація створює підґрунтя для міжнародного розшуку та майбутніх судових процесів, що є стратегічно важливим для відновлення правопорядку та справедливості.

Застосування OSINT базується на аналізі цифрових слідів, які залишають військові та техніка. Основні техніки включають:

- **Аналіз соціальних мереж:** дослідження профілів військових у VK, OK, Threads, Instagram та Telegram. Аналітики вивчають фотографії, списки друзів та коментарі, що дає змогу виявити підрозділ, звання та особисті дані. Нейромережевий пошук (Face Recognition): такі сервіси, як PimEyes або Clearview AI, індексують мільярди зображень із відкритих джерел, будують математичну модель обличчя, зокрема відстань між очима, висота вилиць, лінія підборіддя, яка є унікальною. Навіть якщо злочинець видалив свій профіль у соцмережі

«VK» або «OK», алгоритми знаходять його фото на групових знімках друзів, родичів або в архівах медіа. Цифрова антропометрія: коли обличчя частково закрите, аналітики застосовують метод співставлення незмінних ознак, наприклад, вушні раковини, оскільки форма вуха є такою ж унікальною, як відбиток пальця. Татування та шрами: аналіз «Body Marks» дозволяє ідентифікувати особу за фотографіями з мирного життя наприклад, із пляжних фото у соцмережах. Ергономіка зброї та спорядження: часто ідентифікація відбувається через нестандартне модифікування особистої зброї або специфічні нашивки, які військовий демонстрував раніше.

- **Методологія геолокації:** геолокація в OSINT – це процес встановлення точного географічного місця, де було зроблено фото або відео. Вона реалізується через три послідовні етапи: аналіз орієнтирів Landmark Analysis, коли аналітик шукає на кадрі унікальні об'єкти: вежі зв'язку, лінії електропередач, специфічну архітектуру, вигини доріг або гірські хребти. Навіть дрібні деталі, як-от тип вуличних ліхтарів або колір парканів, можуть звузати коло пошуку до конкретного району. Супутникове співставлення: використовуються платформи Google Earth Pro для аналізу 3D-рельєфу, Sentinel-2 для перегляду актуальних змін ландшафту, наприклад, слідів пожеж або фортифікацій та Махаг для знімків надвисокої роздільної здатності. Хронолокація за допомогою тіней (Shadow Analysis): якщо на відео видно чітку тінь від об'єкта, дослідники використовують інструмент SunCalc. Знаючи дату зйомки та кут нахилу тіні, можна вирахувати азимут сонця і встановити точну координату та час події з похибкою до декількох хвилин.

Для обробки великих масивів даних (Big Data) сучасні OSINT-центри використовують автоматизовані скрипти. Наприклад, інструменти для викачування всіх медіафайлів із Telegram-каналів конкретних підрозділів із подальшим автоматичним скануванням облич та метаданих (EXIF). Хоча більшість соцмереж видаляють метадані при завантаженні, оригінальні файли, знайдені в «хмарах» або на покинутих пристроях, часто містять точні GPS-теги та серійні номери камер.

У міжнародному кримінальному праві існує поняття «крихкості» цифрових доказів. Оскільки скріншот легко підробити за допомогою графічних редакторів або коду елемента сторінки (Inspect Element), суди вимагають суворого дотримання процедур архівації та хешування. Але є певні критерії, за якими скріншот може стати вагомим доказом в суді. Одним з таких критеріїв є ланцюжок зберігання – процес документування кожного кроку роботи з цифровим об'єктом з моменту його виявлення до представлення в суді. Його метою є довести, що доказ не був змінений, видалений або підмінений. Кожна копія файлу повинна супроводжуватися логом: хто, коли, за допомогою якого програмного забезпечення та з якою метою здійснював доступ до даних. Наступним можна виділити хешування – це математичний алгоритм (зазвичай SHA-256 або MD5), який перетворює будь-який обсяг даних у унікальний рядок символів. Якщо у вихідному скріншоті змінити хоча б один піксель, його хеш-сума повністю зміниться. Одразу після збереження доказу генерується його хеш. У суді сторона обвинувачення надає файл і цей код. Суддя може повторно запустити алгоритм і якщо отриманий код збігається з початковим, то автентичність файлу підтверджена.

Однак простого «знімка екрана» (PrtSc) недостатньо для суду. Належна фіксація включає в себе скріншот, який містить URL-адресу, системний час, назву браузера та панель завдань. Використання незалежних сервісів, як-от Wayback Machine або Archive.today. Ці ресурси роблять «зліпок» сторінки на своїх серверах, що унеможливує видалення доказу власником профілю. Для доказів, отриманих безпосередньо з фізичних носіїв наприклад,

покинутий телефон солдата або флеш-накопичувач, створюється повний образ диска («дзеркальна копія»). Робота проводиться лише з копією. Оригінал залишається недоторканим у спеціальному сейфі або Faraday bag для блокування сигналів, щоб уникнути віддаленого стирання даних.

Станом на 2026 рік ідентифікація воєнного злочинця вважається неповною без розкриття його фінансової інфраструктури. Напрямок OSINT-Forensics став сполучною ланкою між цифровими слідами в мережі та реальними грошовими потоками.

FININT (Financial Intelligence) дає змогу не лише підтвердити особу, а й задокументувати ресурси, які дозволяють їй уникати правосуддя. Аналіз криптоактивів: оскільки військові найманці та приватні військові компанії (ПВК) часто використовують криптовалюти для виплат та закупівель спорядження, OSINT-аналітики використовують блокчейн-експертизу.

Нова методологія базується на трьох ключових опорах:

- Blockchain Analysis: використання публічних адрес гаманців, що «світяться» у волонтерських зборах або особистих постах військових. Через інструменти на кшталт *Chainalysis* або *Crystal*, аналітики відстежують рух коштів до централізованих бірж, де особу можна ідентифікувати через процедуру KYC (Know Your Customer);

- Цифрові закупівлі як доказ: аналіз активності на маркетплейсах (eBay, Avito, Amazon, Wildberries). Факт закупівлі специфічного військового обладнання (тепловізорів, дронів, певних типів амуніції) конкретною особою з доставкою в прикордонні зони є непрямим, але вагомим доказом причетності до підрозділу;

- Моніторинг виплат та премій: зіставлення дат публічних нагороджень або звітів про бойові дії з активністю на рахунках або зміною майнового стану родин фігурантів.

Дослідження цифрової ідентифікації воєнних злочинців засобами OSINT дає змогу зробити висновок, що у 2024–2026 роках відбулася фундаментальна зміна архітектури міжнародного розслідування. Відкриті джерела перестали бути лише інструментом медіа та перетворилися на автономну, юридично значущу галузь цифрової криміналістики. Попри значні успіхи, галузь зіштовхується з новими викликами, зокрема масовим поширенням дипфейків та використанням ШІ для дезінформації. Подальший розвиток OSINT вимагатиме впровадження автоматизованих систем верифікації контенту на основі блокчейн-підписів для камер та розробки нових протоколів психологічної підтримки аналітиків, що працюють із візуальними доказами жорстокості.

Отже, OSINT став глобальним механізмом справедливості, який дає змогу документувати історію в режимі реального часу. Це гарантує, що воєнні злочини не матимуть терміну давності, а винні будуть ідентифіковані та притягнуті до відповідальності, незалежно від політичної кон'юнктури чи географічного розташування.

### **Список використаних джерел**

1. URL: <https://bookofmemory.com.ua/uk/analytics/how-analysts-use-osint-uncover-russian-war-crimes-satellite-imagery-social-media-analysis-and-ai/>
2. Bellingcat's Digital Forensic Toolkit.
3. Journal of Digital Forensics, Security and Law.
4. The Berkeley Protocol on Digital Open Source Investigations (Section 5: Collection and Preservation).
5. Chainalysis: The 2026 Crypto Crime Report.

**Горняков І. Д.,**  
молодший науковий співробітник  
(*Національна академія сухопутних військ  
імені гетьмана Петра Сагайдачного*)

**Кривизюк Л. П.,**  
провідний науковий співробітник,  
кандидат історичних наук, доцент  
(*Національна академія сухопутних військ  
імені гетьмана Петра Сагайдачного*)

## **ОСОБЛИВОСТІ ВИКОРИСТАННЯ МЕТОДІВ OSINT У КОГНІТИВНІЙ ВІЙНІ**

Когнітивна війна є одним із ключових вимірів сучасного гібридного протистояння, метою якого є вплив на свідомість, переконання та поведінку як окремих осіб, так і суспільства загалом. Повномасштабне вторгнення російської федерації в Україну 24 лютого 2022 року супроводжується безпрецедентним за масштабами та інтенсивністю інформаційно-психологічного тиску, що спрямовані на дестабілізацію внутрішнього стану українського суспільства, підрив довіри до державних інституцій та формування вигідних агресору наративів у міжнародному інформаційному просторі. В умовах цього протистояння методи OSINT набувають стратегічного значення як інструмент виявлення, моніторингу та нейтралізації когнітивних атак.

Когнітивна війна, на відміну від традиційних форм інформаційного впливу, орієнтована не лише на поширення дезінформації, а й на системну трансформацію когнітивних процесів цільової аудиторії – здатності до критичного мислення, оцінки достовірності інформації та прийняття раціональних рішень [1]. Характерними інструментами когнітивної війни є: скоординовані кампанії дезінформації в соціальних мережах; використання ботоферм та мереж фейкових акаунтів для штучного підсилення певних наративів; маніпуляція алгоритмами видачі контенту; цілеспрямоване застосування технологій синтезу медіаконтенту (дипфейків). Ефективна протидія цим загрозам потребує систематичного моніторингу інформаційного простору, що й забезпечується методами OSINT.

OSINT-методи застосовуються у когнітивній війні за кількома взаємопов'язаними напрямками. Перший – виявлення та атрибуція операцій впливу. Аналіз публічних даних соціальних мереж дозволяє ідентифікувати скоординовану неавтентичну поведінку (coordinated inauthentic behavior): аномально синхронізовані публікації, нетипові патерни активності акаунтів, ознаки автоматизованого поширення контенту. Саме такими методами Meta, Twitter/X та інші соціальні платформи викривали численні мережі акаунтів, пов'язаних із російськими структурами впливу [2].

Другий напрям – верифікація та спростування дезінформації (fact-checking). OSINT-аналітики здійснюють перевірку вірусного контенту шляхом зворотного пошуку зображень, геолокації фото- та відеоматеріалів, зіставлення хронологічних метаданих. В Україні створені і ефективно діють спеціалізовані платформи – «Стоп Фейк», «Детектор медіа», VoxCheck, – які системно застосовують OSINT-інструменти для спростування фейків, пов'язаних із воєнними діями та державною політикою. Швидке публічне спростування маніпулятивного контенту зменшує його вірусний потенціал та знижує ефективність когнітивних атак.

Третій напрям – моніторинг нарративів та прогнозування інформаційних кампаній. Системний аналіз відкритих джерел дозволяє своєчасно відстежувати зародження та поширення певних нарративів у медіапросторі, виявляти координаційні центри їх просування, встановлювати зв'язки між різними «акторами» інформаційного впливу. Саме методи мережевого аналізу (network analysis) та обробки природної мови (NLP) дають змогу автоматизувати моніторинг великих масивів відкритих даних і виявляти патерни когнітивних атак на ранніх стадіях їх розгортання [3].

Четвертий напрям – документування та атрибуція джерел когнітивного впливу. Встановлення зв'язків між анонімними акаунтами, ЗМІ та державними структурами агресора здійснюється шляхом аналізу реєстраційних даних вебсайтів (WHOIS), мережевої інфраструктури, фінансових потоків, що піддаються публічному аналізу, та перехресного зіставлення цифрових слідів. Наприклад, дослідження EU DisinfoLab дозволили розкрити масштабну мережу псевдомедіа, пов'язаних із проросійськими структурами впливу, саме завдяки OSINT-методам атрибуції [4].

Попри значний потенціал, використання OSINT у протидії когнітивній війні пов'язане з низкою викликів. По-перше, технологічне прискорення: стрімкий розвиток генеративного штучного інтелекту суттєво знижує вартість виробництва синтетичного медіаконтенту, що ускладнює його виявлення традиційними методами верифікації. По-друге, проблема масштабу: обсяг інформаційного потоку в сучасному медіапросторі перевищує можливості ручного аналізу, що вимагає подальшого розвитку автоматизованих OSINT-інструментів. По-третє, ризик поширення упереджень: некваліфікований або ненейтральний OSINT-аналіз може сам стати інструментом когнітивного впливу, а тому потребує чітких методологічних стандартів та інституційного нагляду [5].

Для підвищення ефективності OSINT у протидії когнітивній війні необхідним є: розбудова системи публічно-приватного партнерства між державними органами, науковими установами та технологічними компаніями; впровадження стандартизованих методологій моніторингу інформаційного простору; розвиток освітніх програм із медіаграмотності та критичного мислення як елементів когнітивної стійкості суспільства; формування міжнародних коаліцій для координованої протидії транскордонним операціям впливу. Реалізація цих заходів дозволить перетворити OSINT на системний інструмент захисту національного когнітивного суверенітету України в умовах тривалого гібридного протистояння.

### **Список використаних джерел**

1. Rid T. *Active Measures: The Secret History of Disinformation and Political Warfare*. Farrar, Straus and Giroux, 2020. 528 p.
2. Nimmo B., François C., Eib C. S. et al. *Exposing Secondary Infection*. Stanford Internet Observatory, 2020. URL: <https://cyber.fsi.stanford.edu/io/news/secondary-infection> (дата звернення: 10.04.2025).
3. Wardle C., Derakhshan H. *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*. Council of Europe Report DGI(2017)09. Strasbourg, 2017. 109 p.
4. EU DisinfoLab. *Indian Chronicles: Deep Dive into a 15-year Operation Targeting the EU and UN to Serve Indian Interests*. Brussels, 2020. 78 p.
5. Горбань Ю. О. Когнітивна безпека в умовах інформаційної війни: теоретико-методологічні засади. *Стратегічна панорама*. 2023. № 1. С. 28–39.

**Грезіна О. М.,**  
доцент кафедри кримінального аналізу  
та інформаційних технологій,  
доктор філософії в галузі права  
*(Одеський державний університет внутрішніх справ)*

**Пядишев В. Г.,**  
професор кафедри кримінального аналізу  
та інформаційних технологій, доктор юридичних наук, професор  
*(Одеський державний університет внутрішніх справ)*

## **ІНТЕЛЕКТУАЛІЗАЦІЯ OSINT: ВІД ПОШУКУ ІНФОРМАЦІЇ ДО ПРОГНОЗУВАННЯ ЗАГРОЗ**

В умовах динамічного розвитку інформаційного простору та загострення гібридних загроз національній безпеці держав питання ефективного збору, аналізу й інтерпретації відкритих джерел розвідки (OSINT — Open Source Intelligence) набувають першочергового значення. Сучасний ландшафт кіберзагроз характеризується безпрецедентною складністю та динамічністю: щодоби в мережі Інтернет генерується понад 2,5 квінтільйони байт даних, з яких значну частку становить розвідувально-значуща інформація. Традиційні підходи до роботи з відкритими джерелами, що передбачають ручне збирання та категоризацію даних, об'єктивно не відповідають сучасним вимогам щодо швидкості й повноти аналізу. Саме тому інтеграція методів штучного інтелекту (ШІ) у процеси OSINT перетворюється на необхідну умову підвищення ефективності розвідувальної діяльності та своєчасного реагування на загрози.

Сучасний етап розвитку OSINT характеризується переходом від реактивного аналізу до прогнозування загроз. Традиційні підходи, орієнтовані на постфактум-аналіз інформації, поступаються місцем інтелектуалізованим моделям, що базуються на використанні алгоритмів машинного навчання та аналізу соціальних мереж. Формування поведінкових профілів і виявлення аномальних відхилень дозволяє ідентифікувати потенційні загрози ще на ранніх етапах їх виникнення. У цьому контексті OSINT трансформується з інструменту збору інформації в систему прогнозно-аналітичної підтримки прийняття рішень [1].

Концептуальна еволюція OSINT від суто пошукової діяльності до аналітичної розвідувальної системи з прогностичними функціями відбувається завдяки конвергенції кількох технологічних напрямів.

По-перше, великі мовні моделі (Large Language Models, LLM) демонструють здатність до семантичного розуміння текстів у природній мові, що дозволяє автоматизувати класифікацію та кластеризацію розвідувальних даних із різномірних джерел — соціальних мереж, форумів, урядових реєстрів, медіа та darknet-ресурсів.

По-друге, методи комп'ютерного зору забезпечують автоматичний аналіз візуального контенту — геолокацію за знімками, ідентифікацію техніки та інфраструктури на супутникових і аерофотознімках, верифікацію достовірності медіафайлів. Застосування цих технологій суттєво прискорює цикл розвідувального виробництва (Intelligence Cycle), скорочуючи час від збору сирих даних до формування аналітичного висновку.

Окремим виміром інтелектуалізації OSINT є розвиток систем моніторингу в реальному часі (near real-time monitoring) із застосуванням потокової обробки даних. Інструменти на зразок платформ Maltego та відкритих аналогів з використанням інструментів мови програмування Python дозволяють збирати й аналізувати сигнали з

інформаційних потоків одночасно, виявляти аномалії поведінки акторів у кіберпросторі та встановлювати зв'язки між подіями, що на перший погляд є непов'язаними.

Таким чином, формується принципово нова якість аналітики – перехід від реактивного реагування на вже реалізовані загрози до проактивного їх передбачення [2].

Прогнозна аналітика загроз (Predictive Threat Intelligence) на основі OSINT-даних ґрунтується на застосуванні алгоритмів машинного навчання для виявлення прихованих закономірностей і раних індикаторів компрометації (Indicators of Compromise, IoC).

Попри очевидні переваги, інтеграція ШІ у процеси OSINT породжує низку системних викликів, що потребують комплексного вирішення. Ключовою проблемою залишається висока частота хибнопозитивних спрацювань автоматизованих систем, що зумовлена надмірним шумом у відкритих джерелах, навмисним «отруєнням» даних (data poisoning) з боку супротивника та нездатністю моделей до повноцінного розуміння контексту. Загроза генерації правдоподібного, але недостовірного контенту (галюцинації LLM) становить особливу небезпеку в розвідувальному середовищі, де помилковий висновок може спричинити хибні управлінські рішення. Наголошується на необхідності обов'язкового верифікаційного рівня з участю аналітика-людини (human-in-the-loop) у критичних розвідувальних процесах.

Суттєвим обмеженням є також правова й етична невизначеність у сфері автоматизованого збору даних з відкритих джерел. Законодавство більшості держав, зокрема Регламент ЄС про захист даних (GDPR), встановлює обмеження щодо масового збору персональних даних навіть із публічно доступних ресурсів, що ускладнює легальне розгортання OSINT-систем у державних структурах [3]. Відповідно, розробка нормативно-правової бази, що регулює застосування ШІ в розвідувальній діяльності, є невідкладним завданням для законодавців і спеціалістів у сфері безпеки.

Інтелектуалізація OSINT являє собою якісний стрибок у розвитку розвідувальних можливостей державних та недержавних суб'єктів, трансформуючи збір відкритих даних із допоміжного інструменту в самостійний аналітичний напрям із прогностичними функціями. Ефективне застосування методів машинного навчання, обробки природної мови та комп'ютерного зору в межах OSINT-процесів дозволяє суттєво підвищити швидкість і точність виявлення загроз, забезпечуючи своєчасне попередження про кіберінциденти та інформаційні операції. Водночас подолання технічних, правових та етичних обмежень потребує міждисциплінарного підходу та тісної взаємодії між науковою спільнотою, органами державної влади й технологічним сектором. Перспективним напрямом подальших досліджень є розробка гібридних архітектур, що поєднують переваги автоматизованого аналізу ШІ з критичним мисленням людини-аналітика, забезпечуючи максимальну достовірність розвідувальних висновків в умовах сучасних гібридних загроз.

### **Список використаних джерел**

1. Грезіна О. М. Використання інструментів штучного інтелекту в кримінальному аналізі. *Штучний інтелект у правовій практиці: межі та можливості* : збірник тез міжнародного круглого столу (13 березня 2026 року) упор. О. О. Барабаш. Львів : ЛьвДУВС, 2026. С. 99–101.
2. Форос Г. В., Калугін В. Ю., Грезіна О. М. Методологія кримінального аналізу в умовах зростання кіберзагроз. *Юридичний науковий електронний журнал*. 2025. № 11. С. 356–359. URL: <https://doi.org/10.32782/2524-0374/2025-11/74>
3. GDPR-Text.com. *Загальний регламент про захист даних (GDPR): українська версія*. URL: <https://gdpr-text.com/uk/>

**Гриньків О. О.,**  
професор кафедри правових дисциплін,  
доктор юридичних наук  
(Національна академія Національної гвардії України)

## **OSINT: МОЖЛИВОСТІ ТА ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ В НАЦІОНАЛЬНІЙ ГВАРДІЇ УКРАЇНИ**

В умовах сьогодення інформація з відкритих джерел набуває вагомого значення та активно застосовується у практиці різних суб'єктів суспільних відносин. Зокрема, її використовують комерційні підприємства, неурядові організації, аналітичні центри, медіа, незалежні розслідувачі, а також окремі приватні особи. Така інформація є важливим інструментом не лише для прийняття управлінських рішень, проведення наукових досліджень, здійснення журналістських розслідувань, а й забезпечення прозорості суспільних процесів.

Абревіатура OSINT (англ. Open Source Intelligence) у буквальному перекладі означає «розвідка на основі відкритих джерел інформації». У науковій та фаховій літературі підхід до визначення цього поняття є неоднорідним. Так, OSINT розглядається як: діяльність щодо отримання розвідувальної інформації з відкритих джерел кіберпростору; процес здобування розвідувальної інформації з відкритих джерел; розвідка, що базується на аналізі відкритих джерел інформації; діяльність щодо отримання та аналізу розвідувальної інформації з відкритих джерел кіберпростору [1, с. 332].

Отже, наведене свідчить про відсутність єдиної сталої дефініції «OSINT» у сучасній науковій літературі. Водночас усі трактування сходяться на тому, що елементами OSINT є процеси збору, аналізу та інтерпретації інформації, отриманої з відкритих джерел.

Як зазначають науковці, в умовах цифровізації та стрімкого розвитку електронних комунікаційних мереж, традиційні методи виявлення, фіксації та документування правопорушень, які належать до компетенції уповноважених органів, подекуди є недостатньо ефективними, що відповідно зумовлює необхідність впровадження новітніх підходів та інструментів, зокрема заснованих на використанні відкритих джерел інформації [2, с. 43].

Наразі помічаємо зростання ролі відкритих джерел у діяльності органів безпеки і оборони провідних держав світу. Так, дедалі частіше і ширше вони застосовуються у процесах збору, аналізу та верифікації даних, що мають доказове значення. Особливої актуальності це набуває під час документування кримінальних правопорушень, зокрема воєнних, що в подальшому сприяє підвищенню ефективності розслідувань і притягненню винних осіб до юридичної відповідальності.

У сучасних умовах збір та опрацювання інформації з відкритих джерел становлять не лише важливу складову протидії актуальним викликам і загрозам державній безпеці України, а й слугують ефективним інструментом фіксації та документування кримінальних правопорушень. Зокрема, за допомогою OSINT можливо ідентифікувати осіб, причетних до вчинення кримінальних правопорушень, формувати належну доказову базу, а також виявляти зрадників і колаборантів.

Застосування методів розвідки з відкритих джерел у сфері протидії кримінальним правопорушенням ґрунтується на комплексному використанні різномірних інструментів аналізу інформації, що забезпечує її верифікацію та підвищує доказову цінність отриманих даних. Одним із таких поширених інструментів є «геолокація» та «хронолокація», які дають

зможу встановити точне місце і час створення фото- та відеоматеріалів, що можуть містити ознаки правопорушення. Це досягається шляхом зіставлення візуальних елементів із картографічними сервісами та архівними супутниковими знімками.

Важливим напрямом є також ідентифікація осіб, причетних до протиправної діяльності, що здійснюється через аналіз їхньої цифрової присутності в соціальних мережах. Такий підхід дозволяє встановлювати особисті дані, соціальні зв'язки та поведінкові характеристики відповідних суб'єктів.

Окрему роль відіграє використання супутникових знімків високої роздільної здатності для документування наслідків протиправних дій, зокрема руйнувань об'єктів цивільної інфраструктури, визначення масштабів таких руйнувань тощо.

Не менш важливим елементом є аналіз метаданих, який передбачає вилучення прихованої інформації (EXIF-даних) із цифрових файлів. Це дозволяє встановити технічні параметри зйомки, зокрема тип пристрою, точний час і географічні координати створення матеріалу, що суттєво підвищує достовірність доказів.

Крім того, системний моніторинг публічно доступного відеоконтенту забезпечує можливість відстеження переміщення військової техніки та особового складу шляхом аналізу таких ознак, як маркування, типи озброєння та напрямки руху, що в сукупності дає змогу формувати цілісне уявлення про оперативну обстановку.

Як зазначають фахівці [3, с. 5], в умовах сучасності OSINT є не лише інструментом аналітики, а високоефективним напрямом діяльності, що дозволяє отримувати відомості про військові об'єкти, плани та документи противника без безпосереднього ризику для життя персоналу. Водночас така діяльність потребує значних часових і ресурсних витрат, а також застосування сучасних програмних рішень і належного інформаційного забезпечення для якісного аналізу даних та оцінки їхнього впливу на національну безпеку.

Використання таких методів потребує від національної правової системи не лише поглибленого розуміння специфіки цифрових доказів, але й системного вивчення та впровадження передового досвіду у цій сфері.

З огляду на сучасні тенденції розвитку військової справи та зростання ролі інформаційного середовища в умовах збройного конфлікту, OSINT є невід'ємним елементом сучасної системи військової розвідки. Його застосування забезпечує підвищення ефективності аналітичного супроводу операцій, оперативності прийняття управлінських рішень, а також якості оцінювання оперативної обстановки в режимі реального часу.

Для Національна гвардія України (далі – НГУ) впровадження та системне використання OSINT об'єктивно зумовлено необхідністю, що випливає з змісту сучасних загроз. Йдеться як про безпосередні виклики у зоні бойових дій, так і про активне застосування противником інформаційних та когнітивних операцій, спрямованих на дезінформацію, дестабілізацію та вплив на прийняття рішень тощо.

У цьому розумінні OSINT доцільно розглядати не як допоміжний інструмент, а як повноцінний компонент розвідувального забезпечення, інтегрований у процеси оперативного планування та реалізації спеціальних операцій. Його розвиток у структурі НГУ є важливим чинником підвищення загальної бойової спроможності, інформаційної стійкості та ефективності міжпідроздільної взаємодії в сучасному операційному середовищі.

Вважаємо за необхідне приділяти системну увагу вивченню та практичному опануванню методів OSINT військовослужбовцями НГУ, що сприятиме формуванню й розвитку відповідних аналітичних компетентностей, передбачатиме цілеспрямоване

освоєння навичок роботи з відкритими джерелами інформації, критичну оцінку їх достовірності, верифікацію отриманих даних та подальшу аналітичну обробку в інтересах службово-бойової діяльності НГУ.

Окремого значення набуває інтеграція OSINT-інструментів у процеси оперативного планування та інформаційно-аналітичного забезпечення службово-бойової діяльності. Важливим напрямом також є удосконалення міждисциплінарної взаємодії між аналітичними підрозділами, підрозділами зв'язку та кібербезпеки з метою підвищення якості та ефективності використання інформаційних потоків.

Крім того, актуальним є впровадження системної підготовки та безперервного навчання фахівців у сфері OSINT з урахуванням сучасних технологічних рішень, зокрема автоматизованих систем збору та обробки даних, інструментів геоаналітики, а також методів протидії інформаційним загрозам. Реалізація зазначених заходів сприятиме підвищенню рівня інформаційної обізнаності, оперативної готовності та стійкості військовослужбовців підрозділів НГУ в умовах сьогодення.

### **Список використаних джерел**

1. Дикий О. В., Сидорчук В. В. Поняття OSINT та суміжні категорії. *Юридичний науковий електронний журнал*. С. 332–335. URL: [http://lsej.org.ua/9\\_2024/80.pdf](http://lsej.org.ua/9_2024/80.pdf)

2. Зоренко Д. Використання інструментів і методів OSINT для виявлення, фіксації та документування посягань на державну безпеку України. *Актуальні напрями підвищення спроможностей сил сектору безпеки і оборони України: правові та організаційні аспекти* : матеріали Міжнародної науково-практичної конференції, 27–28 березня 2025 року. Київ : Алерта, 2025. С. 43 – 46.

3. Використання інструментів та методів OSINT для отримання пошукової інформації: практичний poradnik. 5-те вид., переробл. та до повн. / Д. С. Зоренко, Л. О. Кульчицька, Р. В. Лех, О. І. Червяков. Харків : Видавець: О.А. Мірошніченко, 2024. 80 с.

**Грінченко В. В.,**  
доцент кафедри  
прикордонної служби, доктор філософії  
(*Національна академія державної прикордонної  
служби України імені Богдана Хмельницького*)

**Дегалюк М. А.,**  
здобувач вищої освіти  
(*Національна академія державної прикордонної  
служби України імені Богдана Хмельницького*)

## **OSINT-ДОСЛІДЖЕННЯ ЯК ІНСТРУМЕНТ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ**

Сучасна архітектура національної безпеки України в умовах гібридної агресії вимагає інтеграції новітніх методів збору та аналізу даних, серед яких особливе місце посідає розвідка на основі відкритих джерел (OSINT). Відповідно до стандартів НАТО та практики провідних країн світу, OSINT визначається як розвідувальна інформація, отримана з загальнодоступних даних, що збирається та розповсюджується для задоволення конкретних потреб безпеки. Перевагами цього напрямку є економічна ефективність, доступність широкого спектру даних та можливість підтримки прийняття стратегічних рішень у реальному часі [1].

Ефективність використання OSINT у правоохоронній діяльності залежить від застосування чітких і структурованих підходів до аналізу інформації. Одним із таких підходів є модель «6 W + 2 H» (Who, What, Where, When, Why, Whom + How, How Much), яка допомагає послідовно відтворити події, встановити причини їх виникнення та оцінити можливі наслідки [1]. Водночас процес збору та обробки даних має здійснюватися з дотриманням етичних принципів, зокрема тих, що закладені у підходах PLANE та ALPEN.

PLANE передбачає логічну послідовність дій: від визначення мети дослідження та підбору джерел до аналізу інформації, фіксації результатів і безпосереднього збору даних. Натомість ALPEN орієнтований на організацію роботи аналітика - він допомагає правильно розподілити завдання, оцінити час на їх виконання, визначити пріоритети та проконтролювати отримані результати.

Застосування цих підходів дозволяє зробити процес OSINT-дослідження більш упорядкованим і обґрунтованим, зменшує ризик правових порушень та підвищує довіру до отриманої інформації, що є особливо важливим у разі використання таких матеріалів у судовій практиці [3].

Напрямом забезпечення інформаційної безпеки є виявлення та аналіз демаскувальних ознак об'єктів інформатизації. Сучасна технічна розвідка противника активно використовує радіоелектронні, оптичні та акустичні канали для перехоплення конфіденційної інформації. У цьому контексті значення набуває ідентифікація побічних сигналів, зокрема параметрів побічних електромагнітних випромінювань і наведень, а також акустико-електричних перетворень, які можуть свідчити про витік інформації. Нейтралізація таких загроз досягається шляхом застосування заходів активного маскування, екранування та технічного захисту інформації. Системний моніторинг і контроль зазначених каналів витоку дозволяє підвищити стійкість держави до шпигунства [2].

Пріоритетом є кібергігієна та протидія методам соціальної інженерії, яка часто використовується для маніпуляції персоналом та отримання несанкціонованого доступу до даних. Практичні рекомендації включають суворе розмежування службових та особистих пристроїв, відключення геолокації, використання наскрізного шифрування в месенджерах та налаштування двофакторної автентифікації. Впровадження цих стандартів серед особового складу правоохоронних органів є невід’ємною частиною захисту інформаційного периметра держави [2].

Досвід міжнародних груп, таких як Bellingcat, демонструє, що OSINT стає «народною розвідкою», здатною встановлювати істину у справах міжнародного значення, наприклад, у розслідуванні катастрофи рейсу MH17 [4]. Завдяки геолокації та аналізу метаданих стає можливим відстеження переміщення військової техніки та ідентифікація осіб, причетних до воєнних злочинів. Таким чином, OSINT-дослідження трансформуються з допоміжного інструменту в фундаментальний компонент сучасної системи національної безпеки, що забезпечує прозорість, підзвітність та ефективну протидію дезінформаційним загрозам [4].

### **Список використаних джерел**

1. Про сучасну інформаційну розвідку. Сфери використання Victory Drones. 2024.
2. Гуляєв В. П. Аналіз демаскувальних ознак об’єктів інформатизації та технічних каналів витоку інформації: навч.-метод. комплект, 2014.
3. Практичні рекомендації з кібербезпеки під час ведення бойових дій. Запоріжжя : СБУ, 2023.
4. Гігінз Е. Ми – Bellingcat. Онлайн-розслідування міжнародних злочинів та інформаційна війна з Росією. Київ : Наш Формат, 2022.

**Гром'як С. І.,**  
докторант  
(Львівський національний університет ветеринарної  
медицини та біотехнологій імені С. З. Гжицького)

## **СТРУКТУРНІ ЧИННИКИ ВАРТОСТІ ТА ФІНАНСОВОЇ ЕФЕКТИВНОСТІ OSINT-СИСТЕМИ У СФЕРІ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ**

Інженерна архітектура модуля «Валідатор Стратегій» – верифікаційного шлюзу, що функціонує у складі ширшої аналітичної екосистеми Military Gini. Екосистема призначена для побудови калібрувального ряду Індексу Військового Джині ( $G_{mil} \in [0, 1]$ ) як кількісного – предиктора ендогенних структурних розривів. Її вхідним контуром слугують відкриті джерела – SIPRI, IISS, GlobalFirepower, Soufan Center, RUSI, парламентські звіти, – а також польовий OSINT: скани ворожих документів, фотоматеріали з Telegram та X, геотеговані відеозаписи. Усі ці потоки за замовчуванням вважаються «брудними» та потенційно ворожими. Валідатор виконує функцію Zero-Trust-шлюзу між нестабільним динамічним контекстом мережі та статичним графом прецедентів, розгорнутим у Neo4j (257 вузлів, 366 ребер, 73 історичні епохи, 78 траскторій країн, 76,7 % джерел верифіковано через Wikipedia API).

Типова архітектура «OSINT-агент плюс хмарна велика мовна модель» у військовому контексті має три критичні дефекти. По-перше, вона породжує витoki чутливих даних через API провайдерів юрисдикцій США, Європейського Союзу та Китаю. По-друге, вона страждає від явища context clogging – забивання вікна контексту сирими HTML-, PDF- та OCR-шумами, що деградує якість reasoning та нарощує вартість токенів у п'ять – тридцять разів. По-третє, вона лишається вразливою до непрямих ін'єкцій промптів: дослідження Fogseroint (2026) зафіксувало десять активних пейлоадів у відкритих джерелах, а Schneier зі співавторами (2026) формалізували «Promptware Kill Chain» на семи послідовних стадіях. Окремим ризиком є атака TopicAttack (Shi та ін., EMNLP 2025) з показником успішності понад 90 % навіть проти сучасних захисних механізмів StruQ, SecAlign та Spotlight.

У відповідь запропоновано гібридну інференс-архітектуру, що складається з трьох шарів. Перший шар (L0, Data-Ingestion Python-layer) реалізовано виключно на детермінованих інструментах – регулярних виразах, дедуплікації за SimHash та MinHash, іменованому розпізнаванні сутностей, perplexity-фільтрації; його завдання – зрізати шум ще до того, як дані досягнуть токенизатора великої мовної моделі. Другий шар (L1) – air-gapped локальний LLM-контур на базі Meta Llama 3.3 Instruct 70B, Llava v1.6 Mistral, Qwen3-VL, GPT OSS та Gemma-4, який опрацьовує класифіковані потоки без будь-якого мережевого виходу. Третій шар (L2) – хмарний arbitration-контур на основі Claude 4.7 Opus, GPT-5.5 та Gemini 3.1 Pro Preview, що залучається виключно для високомаржинальних завдань стратегічної валідації та cross-model disagreement detection. Мультимодальний OCR-фронтенд побудовано на сімействі Gemini, яке у внутрішніх бенчмарках легких моделей продемонструвало найкращі показники на розпізнаванні сканів кирилицею та розумінні структури таблиць.

На синтетичному контрольованому датасеті обсягом 200 OSINT-джерел із симетричним розподілом 100 чистих та 100 отруєних повна трирівнева архітектура досягає 89,0 % accuracy та  $F1 = 0,88$ . Робоча точка конфігурації виявляє явний trade-off: чисто локальний режим забезпечує FPR 4,2 % за FNR 18,1 %, натомість гібридний arbitration-шар зсуває баланс до FPR 11,8 % за FNR 9,0 %, що є закономірною платою за підвищену чутливість у агресивному середовищі. Python-фільтрація зменшує обсяг токенів, поданих у модель, у середньому на 78 % – зі 142 тис. до 31 тис. на типову партію з 50 сирих джерел.

Екосистема Military Gini розв'язує вузькоспеціалізовану прикладну задачу – побудову калібрувального ряду Індексу Військового Джині для понад тридцяти держав на основі дезагрегованого розподілу примусового потенціалу серед інституційних акторів: регулярної армії, президентської гвардії, приватних військових компаній, проксі-міліцій, організованої злочинності, регіональних воєначальників. Вхідний матеріал принципово гетерогенний: табличні бюджети SIPRI, прозові звіти RUSI, скани парламентських додатків, фотографії техніки з Telegram та X, геотеговані OSINT-ролики, перехоплені PDF-документи. Жоден з цих потоків не є «чистим» за замовчуванням; кожен розглядається як кандидат на цілеспрямоване отруєння.

Саме в цій точці екосистеми функціонує «Валідатор Стратегій» – не «черговий чатбот», а критичний шлюз, що приймає бінарне рішення: чи має конкретне OSINT-спостереження право потрапити у граф прецедентів і вплинути на значення  $G_{mil}$  конкретної країни. Помилка у цивільному контексті є відносно дешевою; у військовому – навпаки, коштовною: отруєна точка даних здатна зрушити композитний індикатор та спровокувати хибне стратегічне рішення з потенційно незворотними наслідками.

Загальну логіку взаємодії шарів ілюструє рисунок 1. Три обчислювальні контури – детермінований L0, air-gapped L1 та хмарний arbitration L2 – послідовно передають матеріал до верифікаційного шлюзу «Валідатор Стратегій», який зіставляє динамічне спостереження зі статичним графом прецедентів Neo4j і приймає рішення про його включення до калібрувального ряду  $G_{mil}$ .

Валідатор функціонує як багаторівневий верифікаційний шлюз, що перевіряє аксіологічну добросовісність стратегічних даних (на діаграмі нижній блок зліва) через послідовну фільтрацію та дедуплікацію інформаційних потоків (в кінцевому результаті маємо три показники власне Мілітарі Джині, Критичне сповільнення та синтетичний аксіологічної добросовісності). Ключове завдання OSINT підсистеми – захистити розрахунки Індексу Військового Джині від маніпулятивного «отруєння», непрямих ін'єкцій та когнітивних галюцинацій, які можуть викривити оцінку національного багатства. Використання ізольованих локальних контурів та ансамблевого арбітражу дозволяє системі верифікувати автентичність сутностей, гарантуючи, що стратегічні рішення базуються на об'єктивному фундаменті, а не на інспірованих ззовні наративах.

## Strategy Validator Ecosystem (SVE) трикутатурна архітектура

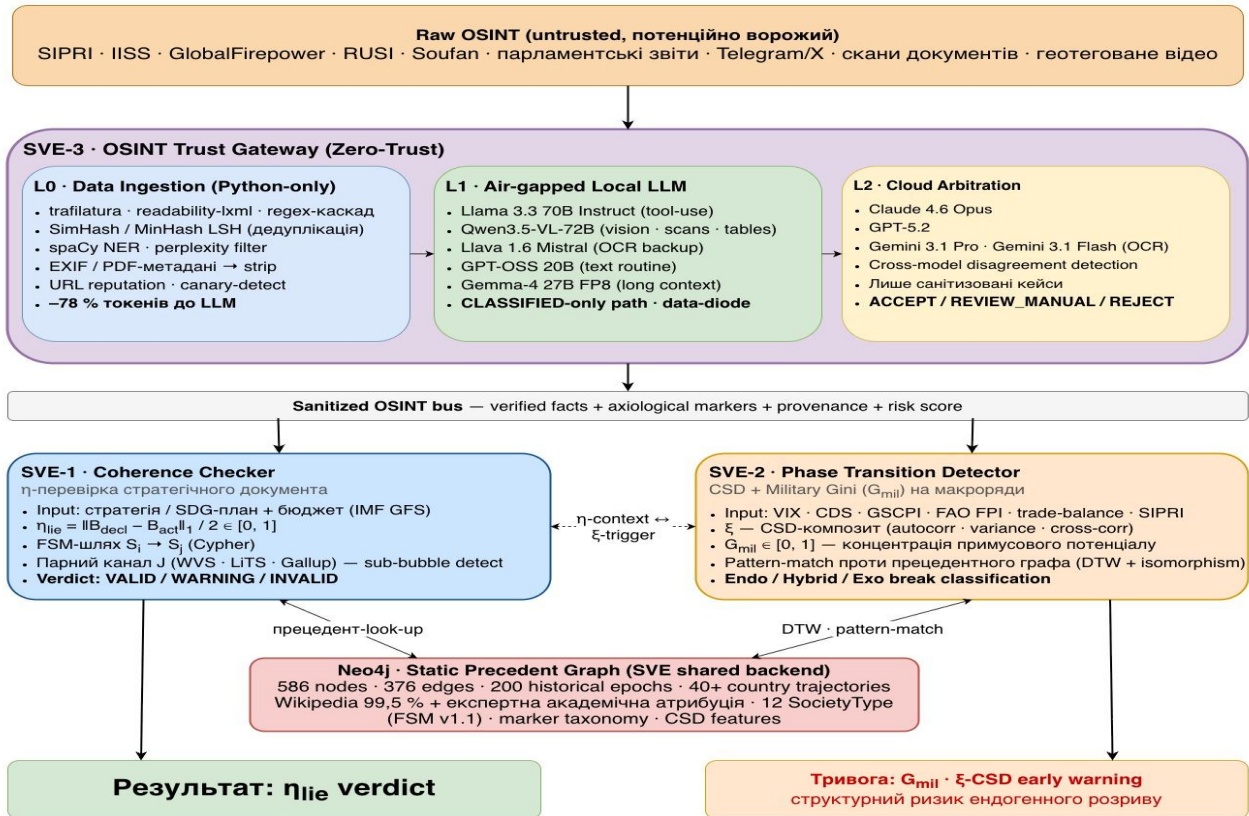


Рис. 1. Трикутатурна гібридна архітектура екосистеми Military Gini з Zero-Trust верифікаційним шлюзом.

У контексті запобігання загрозам фазового зсуву (на схемі нижній блок справа), система виступає детектором критичного сповільнення, ідентифікуючи приховані аномалії в управлінських та фінансових сигналах. Валідатор відстежує розриви між декларативними цінностями та реальними векторами розподілу ресурсів, фіксуючи зростання аксіологічної брехні ще до того, як вона спричинить системний колапс чи неконтрольовану зміну соціального стану. Це дозволяє вчасно виявляти ознаки деградації інституційної стійкості, забезпечуючи можливість превентивної корекції стратегії у точках фазової нестабільності.

### **Список використаних джерел**

1. Forcepoint Research. Researchers Uncover 10 In-the-Wild Indirect Prompt Injection Attacks. Infosecurity Magazine, 23 April 2026.
2. Brodt O., Feldman E., Schneier B., Nassi B. The Promptware Kill Chain: How Prompt Injections Gradually Evolved Into a Multistep Malware Delivery Mechanism. arXiv:2601.09625v2, 2026.
3. Shi C. et al. TopicAttack: An Indirect Prompt Injection Attack via Topic Transition. Findings of EMNLP 2025, pp. 16995–17006.
4. Bassani E., Sanchez I. On Guardrail Models' Robustness to Mutations and Adversarial Attacks. Findings of EMNLP 2025.
5. Flynn J., Terzis A., Sitawarin C., Nasr M. et al. Lessons from Defending Gemini Against Indirect Prompt Injections. arXiv:2505.14534, 2025.
6. Castle Research. Fingerprint harvesting in the bot ecosystem. castle.io/research, 2026.
7. Torchia J. Prove you are a robot: reversed CAPTCHAs for AI agents. DEV Community, 20 April 2026.
8. Any-Depth Alignment (ADA): Inference-Time Safety at Arbitrary Generation Depth. Under review, ICLR 2026.
9. URL: [https://drive.google.com/file/d/1MBLzWUfTyxhoxdBTETR7zXpk7qPQULr/view?usp=drive\\_link](https://drive.google.com/file/d/1MBLzWUfTyxhoxdBTETR7zXpk7qPQULr/view?usp=drive_link)

Гуцуляк Ю. В.,  
доцент кафедри кримінального процесу, доктор філософії  
(Львівський державний університет внутрішніх справ)

**ОСОБЛИВОСТІ ВИКОРИСТАННЯ ФАКТИЧНИХ ДАНИХ,  
ОТРИМАНИХ ЗА ДОПОМОГОЮ OSINT-ТЕХНОЛОГІЙ  
У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ  
(ЗА РЕЗУЛЬТАТАМИ АНАЛІЗУ ВОРОЖИХ TELEGRAM-КАНАЛІВ)**

Україна веде важку, виснажливу війну із агресором, котрий переважає сили оборони у техніці та живій силі. Такі виклики диктують необхідність пошуку нових шляхів протидії агресору. На полі бою це стало можливим, окрім іншого, із запровадженням концепції широкого використання наземних роботизованих комплексів (НРК) та безпілотних авіаційних систем (БАС). Переваги таких засобів як ураження так і розвідки чи логістики стали відчутними настільки, що ворог намагається перехопити ініціативу в даному напрямку.

Ефективність використання залежить від багатьох факторів, в тому числі і від технічного. До елементів його відносять технічні модулі керування, навігації та відео-потоків. Результати відео зйомки (найчастіше з БАС) стають об'єктом детального аналізу, передусім з військовою метою. На них спеціалісти виявляють цілі, сліди пересування ворожих підрозділів, а також фіксуються факти підтвердження ураження живої сили та техніки противника. Поширеними є факти фіксування за допомогою як українських сил під час використання авіаційних комплексів так і ворогом, наслідків вчинення воєнних злочинів, так і безпосередньо самі події вчинення таких. Така інформація зберігається на носіях інформації, накопичується в базах даних.

Окрім переваги на полі бою, результати роботи таких засобів ураження та розвідки використовуються сторонами війни і в інших цілях.

Зокрема, зафіксовані українською стороною факти вчинення кримінальних правопорушень проти миру та людяності, правил ведення війни тощо, стають підставами для початку здійснення кримінальних проваджень, а самі відеозаписи – доказами в кримінальному провадженні.

Також метою використання відеозаписів може бути: пропаганда; психологічний вплив на противника (його деморалізація); проведення інформаційних психологічних операцій чи дезінформація противника.

Одним із шляхів досягнення однієї з мети, зазначеної вище – є оприлюднення в широкому інформаційному просторі відеоматеріалу. Одним з основних способів поширення необхідної інформації, які мають вигляд відео – є його через канали приватних та офіційних засобів масової інформації (ЗМІ). Останніми роками популярними видами яких є інформаційні канали у безкоштовні хмарні месенджери з функціями соціальної мережі (наприклад Telegram). Проведений нами аналіз змісту ворожих телеграм-каналів (Херсонського напрямку ведення бойових дій), зокрема змісту представлених ворогом відеоматеріалів, дозволив зробити висновок, про численні факти вчинення воєнних злочинів на території Херсонської області. Та виокремити певні особливості таких відеоматеріалів.

Першою особливістю матеріалів, які опубліковані відкрито є те, що жоден з них не є цілісним. Тобто таким, який фіксує від початку до кінця, безперервно використання БАС противника. У відеоматеріалах зафіксовані переважно дані щодо вже безпосереднього факту

завдання удару дронами типу fpv (First Person View). Відеоматеріал, які поширюються відкрито є лише частиною отриманого відео-запису, тобто перед оприлюдненням проходять «вирізання» частини, переважно завершальної, що автоматично підтверджує факт «втручання» у цілісність файлу.

Наступною – застосування графічних ефектів, котрі частково змінюють відео зображення (Blur). Застосування таких технологій має на меті приховати інформацію на відео про технічні особливості застосованого дрона, інформація про що відображається на екрані оператора і є повним відображенням відео контенту. Водночас «блюр» частини зображення змінює автентичність даних оригіналу відео.

Такі особливості слід враховувати при оцінці доказів в кримінальному провадженні. Нагадаємо, що докази в кримінальному провадженні оцінюються з позиції їх належності, достовірності, допустимості та достатності. Вплив використання технологій обробки відео зображення, яке отримуємо за допомогою технології OSINT та із застосуванням відповідного процесуального інструментарію (шляхом проведення відповідних процесуальних дій, а саме слідчих (розшукових)), з ворожих Telegram каналів, в окремих випадках може становити загрозу достовірності, як ознаці доказів в кримінальному провадженні. На наш погляд, така слідча ситуація, не є безумовною обставиною визнання доказу недостовірною чи неможливістю використання його в наслідок оперування такими даними як не оригінальним матеріалом. Однак, така ситуація повинна враховуватись як слідчим на стадії досудового розслідування під час перевірки отриманих даних з таких відео, і супроводжуватись його додатковими процесуальними діями з метою спростування окремих сумнівів щодо спотворення, зміни автентичності всієї інформації, котрі отримується зі змісту відео.

Такими процесуальними засобами перевірки доказів на стадії досудового розслідування, з метою забезпечення належного судового розгляду і досягнення завдань кримінального процесуального законодавства, можуть бути: призначення криміналістичних експертиз; отримання та фіксування за допомогою OSINT не лише відеоматеріалів, але й роз'яснень авторів Telegram каналів до відео та супутньої інформації. такою супутньою інформацією, можуть бути коментарі до відео чи посту, ідентифіковані автори коментарів тощо. Таким чином такий об'єм інформації здатен повно і всебічно відобразити обставини зображені на відео, отримати цілісну картину за фрагментом відео, точно локалізувати відео за місцем та часом, підтвердити застосування ударних дронів чи інших обставин вчинення воєнних кримінальних правопорушень.

На наш погляд, зазначені нами особливості та напрямки процесуальної діяльності суб'єктів кримінального провадження є перспективним полем як для наукового так і для правозастосовного пошуку та вирішення в межах кримінальної юстиції та кримінальної процесуальної політики в Україні.

**Гуцуляк Ю. В.,**  
доцент кафедри кримінального процесу, доктор філософії  
*(Львівський державний університет внутрішніх справ)*  
**Гонта С. Ю.,**  
здобувач вищої освіти  
*(Львівський державний університет внутрішніх справ)*

## **ЗАСТОСУВАННЯ МЕТОДУ OSINT ДЛЯ ЗБОРУ ДОКАЗІВ У ВОЄННИХ КОНФЛІКТАХ**

Із 2014 року Україна перебуває в умовах збройного протистояння, яке після 24 лютого 2022 року трансформувалося у повномасштабну збройну агресію з боку російської федерації. Значна частина територій держави залишається тимчасово окупованою ще з початку конфлікту, а на окремих напрямках тривають інтенсивні бойові дії. Це створює суттєві перешкоди для здійснення традиційних процесуальних заходів, зокрема проведення слідчих і негласних слідчих (розшукових) дій, а також отримання інформації через офіційні запити.

В умовах війни особливої актуальності набуває використання даних із відкритих джерел як альтернативного способу отримання відомостей, що мають доказове значення. Сучасний розвиток цифрових та інформаційних технологій суттєво розширює можливості органів досудового розслідування у зборі криміналістично значущої інформації. Водночас важливим аспектом є належна фіксація таких даних, що забезпечує можливість їх подальшого використання як доказів як у національних судах, так і в міжнародних інституціях, зокрема в Міжнародному кримінальному суді.

OSINT у досудовому розслідуванні є допоміжною технікою, яка надає слідчому додаткову інформацію, що має значення у досудовому розслідуванні, та докази, але при цьому не повинно бути їх єдиним джерелом.

OSINT-аналіз охоплює будь-які відкриті джерела інформації: супутникові знімки, книги, аналітичні звіти, газетні публікації тощо. Найчастіше збір даних відбувається через інтернет із використанням інформації із соціальних мереж і месенджерів.

Аналіз практики досудового розслідування дає підстави виокремити кілька основних категорій джерел інформації, що використовуються в межах OSINT.

По-перше, це загальнодоступні джерела, які можуть бути як безкоштовними, так і платними. До них належать нормативно-правові акти держави-агресора, що дозволяють простежити причинно-наслідкові зв'язки між рішеннями військово-політичного керівництва та вчиненими злочинами. Важливу роль також відіграють офіційні вебресурси державних органів і юридичних осіб, де можуть міститися документи, повідомлення та інша значуща інформація, зокрема щодо структури, місцезнаходження, контактних даних і керівництва відповідних суб'єктів. Значний обсяг відомостей надають засоби масової інформації та їхні публікації, які дозволяють встановити наміри, плани (наприклад, мобілізаційні заходи), а також причетність окремих осіб до ведення війни. Окрему групу становлять відкриті державні реєстри та бази даних, що дають змогу отримувати додаткові відомості, зокрема

про юридичних осіб або окремі юридично значущі факти. Разом із цим використовуються агрегатори відкритих даних, хоча доступ до них у державі-агресорі поступово обмежується. Також важливими є інші відкриті інтернет-ресурси, зокрема наукові та публіцистичні матеріали, які формують ідеологічне підґрунтя агресії.

По-друге, суттєве значення мають так звані витoki даних — інформація, доступ до якої спочатку був обмежений, але згодом став відкритим унаслідок несанкціонованого поширення. Такі джерела можуть містити персональні, фінансові та інші дані, що дозволяють встановити базову інформацію про осіб, включаючи їхні анкетні дані, контакти або окремі документи. Водночас ці відомості мають допоміжний характер, потребують обов'язкової перевірки та не можуть розглядатися як самостійні докази.

По-третє, важливим джерелом виступають соціальні медіа, які залежно від налаштувань доступу можуть містити як відкрити, так і обмежену інформацію. Аналіз таких ресурсів дає змогу встановити місце перебування особи, її належність до певних військових формувань, а також соціальні зв'язки — коло спілкування, родинні та службові контакти.

По-четверте, значний потенціал мають геопросторові дані, включаючи цифрові карти, супутникові знімки та інші візуальні матеріали. Їх використання дозволяє, зокрема, відстежувати переміщення військової техніки, аналізувати наслідки руйнувань об'єктів інфраструктури та отримувати іншу важливу інформацію.

Окрему категорію джерел OSINT становить так звана сіра література (Grey literature). Це збірка технічних звітів, попередніх публікацій, патентів, робочих документів, службових матеріалів, неопублікованих робіт та інформаційних бюлетенів. Ці ресурси містять важливу інформацію, що знаходить застосування в багатьох сферах, таких як дослідження безпеки, виявлення слабких місць та аналіз потенційних загроз. Водночас, необхідно використовувати ці джерела відповідно до чинного законодавства та з необхідними дозволами, оскільки незаконне отримання інформації може спричинити серйозні юридичні наслідки.

Використання методів OSINT у сучасних умовах дозволяє ефективно здійснювати онлайн-розслідування та виявляти цифрові сліди кримінальних правопорушень. Значна кількість даних, необхідних як для початку кримінального провадження, так і для подальшого розслідування воєнних злочинів та злочинів проти людяності, уже перебуває у відкритому доступі. Водночас ці відомості часто є розпорошеними та прихованими серед великого інформаційного потоку.

OSINT-аналітики працюють із окремими фрагментами відкритих джерел, поєднуючи їх у цілісну систему для відтворення реальної картини подій. Завдяки цьому можна отримувати відомості про переміщення військових підрозділів РФ, використання озброєння, тактичні рішення противника, а інколи навіть прогнозувати його подальші дії.

Разом із тим використання OSINT у судових процесах супроводжується низкою складних питань. Насамперед важливо довести автентичність цифрових доказів, оскільки суд повинен бути впевненим у відсутності фальсифікації чи будь-яких змін інформації. Не менш важливо забезпечити надійність джерел, із яких отримуються дані, щоб уникнути можливості їх оскарження. Окрему роль відіграє дотримання безперервного ланцюга збереження доказів, адже це підтверджує їхню цілісність і достовірність.

Для підвищення ефективності використання OSINT-доказів у судовій практиці необхідно вдосконалювати процедури збору, перевірки та фіксації інформації, а також розширювати співпрацю між практиками OSINT і слідчо-оперативними підрозділами.

Отже, у сучасних умовах збройної агресії РФ проти України OSINT став одним із ключових інструментів документування воєнних злочинів та порушень прав людини. Його можливості щодо використання відкритих джерел суттєво змінили підходи до розслідування міжнародних злочинів і збору доказової бази.

### **Список використаних джерел**

1. Білобров А. В., Клімушин П. С. Використання технологій OSINT для отримання інформації. *Протидія кіберзлочинності та торгівлі людьми* : матеріали Міжнародної науково-практичної конференції (м. Харків, 27 травня 2020 року). С. 135–137.

2. Сіфоров О., Калугін В. Використання OSINT у встановленні фактів воєнних злочинів та особи воєнних злочинців. *Правове регулювання дотримання прав і свобод людини та громадянина в умовах адміністративно-правового режиму воєнного стану* : колективна монографія / за заг. ред. А. В. Денисової. Одеса : Видавництво «Юридика», 2025. Розд. 20. DOI: <https://doi.org/10.61563/978-617-8574-56-7-20>

3. Комісарчук Ю. А., Черевко В. В. OSINT як один з інструментів для збирання інформації про воєнні злочини Російської Федерації в Україні. *Modern science: innovations and prospects* : Proceedings of the XIV International Scientific and Practical Conference, Stockholm, Sweden, 16–18 October 2022. Stockholm, 2022. С. 451–454.

**Деркач Д.,**  
аспірант кафедри фінансів,  
грошового обігу і кредиту  
(Львівський національний університет імені Івана Франка)  
Науковий керівник: **Підхормний О. М.,**  
професор кафедри фінансів, грошового обігу і кредиту,  
доктор економічних наук  
(Львівський національний університет імені Івана Франка)

## **ІНТЕГРАЦІЯ ІНСТРУМЕНТІВ ШІ ТА OSINT ДЛЯ МІНІМІЗАЦІЇ БЕЗПЕКОВИХ ЗАГРОЗ У СФЕРІ КОРПОРАТИВНИХ ФІНАНСІВ**

В умовах глобалізованої економіки, зокрема в періоди геополітичної турбулентності, збройних конфліктів та масштабних економічних криз, великі корпорації відіграють важливу роль у забезпеченні фінансової, продовольчої та соціальної безпеки на національному та міжнародному рівнях. Управлінські рішення, що приймаються системними підприємствами, безпосередньо впливають на стабільність ринків та добробут мільйонів людей. Зростання кількості кіберзагроз, шахрайства та маніпуляцій з фінансовими даними зумовлює необхідність постійного вдосконалення підходів до своєчасного виявлення та нейтралізації безпекових загроз у сфері корпоративних фінансів. Особливого значення за таких умов набуває корпоративна розвідка (КР) – систематичний, легальний та етичний процес збору, аналізу та інтерпретації інформації про ринкове середовище, конкурентів та потенційні загрози. Перспективним інструментом у цьому контексті стає інтеграція технологій штучного інтелекту (ШІ) та розвідки на основі відкритих джерел (OSINT) [2].

Основними напрямками КР на базі OSINT в системі корпоративного управління ризиками є:

- проведення комплексних перевірок контрагентів (Due Diligence);
- конкурентна та ринкова розвідки;
- внутрішній аудит та розслідування шахрайства;
- санкційний комплаєнс та моніторинг негативних новин.

Проведення комплексних перевірок контрагентів є найбільш актуальним під час угод злиттів та поглинань (M&A), створення спільних підприємств, в процесі інвестування або ж при укладанні стратегічних партнерських угод. Під час Due Diligence відбувається перехресна перевірка корпоративних реєстрів для ідентифікації реальних бенефіціарів, прихованих зобов'язань та потенційних конфліктів інтересів. Аналіз фінансової стійкості контрагента підкріплюється OSINT-дослідженням його ділової репутації, що дозволяє уникнути інвестицій у компанії з фіктивним зростанням [1].

Конкурентна розвідка дозволяє відстежувати стратегії конкурентів, їхні фінансові показники, кадрові змін та ринкові ініціативи для збереження конкурентної переваги. Ринкова розвідка доповнює такі дані аналізом макроекономічних трендів, регуляторних змін та геополітичних ризиків, що можуть вплинути на фінансові результати компанії. Результати даних розвідок іноді інтегруються в комплексне стратегічне дослідження для більш глибокої оцінки життєздатності бізнес-моделі компанії, ймовірності ворожих поглинань чи потенційних суттєвих зрушень регуляторного, політичного, логістичного чи безпекового характеру.

Система оперативного внутрішнього аудиту та розслідування шахрайства допомагає ідентифікувати внутрішні зловживання (неправомірне збагачення, передача конфіденційної інформації конкурентам, навмисне викривлення фінансової звітності та ін.), а також проводить моніторинг у реальному часі операційних ризиків (кібератак та витоків даних). OSINT забезпечує можливість встановлення хронології подій та виявлення можливих фактів змови шляхом дослідження соціальних мереж та інших відкритих даних щодо підозрюваних [3].

КР в сфері санкційного комплаєнсу та відслідковування негативних новин націлена на превентивний моніторинг репутаційних криз партнерів, актуальних кіберзагроз, порушеннях у ланцюгах постачання. Для прикладу, аналіз негативних новин дозволяє виявити участь контрагента в екологічних порушеннях, корупційних скандалах або фінансуванні тероризму ще до порушення кримінальних справ чи включення до санкційних списків.

Сучасні інструменти ШІ дозволяють суттєво розширити можливості КР шляхом:

- масштабування (ШІ здатен оперативно опрацьовувати великі масиви публічних даних);
- автоматизованого моніторингу в реальному часі (зокрема, інформації про зміни в санкційних списках, подачу звітності, запуск нового продукту чи вихід на нові ринки конкурентами, оголошення про тендери, дані зі ЗМІ та соціальних мереж);
- предиктивної аналітики та виявлення аномалій (наприклад, незвичні транзакції, поведінка контрагентів чи нетипові ринкові сигнали);
- побудови візуальних графів для дослідження складних взаємозв'язків (GNN-моделі збирають OSINT-дані та накладають їх на внутрішні транзакційні дані, що дозволяє генерувати візуальні графи взаємозв'язків для виявлення потенційних безпекових загроз);
- інтеграції просторового аналізу (наприклад, алгоритм здатний виявити просторову неможливість чи недоцільність логістичних маршрутів, задекларованих у митних документах, або підозрілу концентрацію підприємств за однією адресою, що може свідчити про мережу фіктивних компаній-оболонки) [5];
- обробки неструктурованих даних (NLP-моделі дозволяють ефективно опрацьовувати текстову інформацію із судових реєстрів, публікацій в ЗМІ та соціальних мережах, митних та податкових базах для формування профілів ризику) [4];
- прискорення циклу розслідування (для більш оперативного прийняття рішень та оптимізації ресурсів).

Разом з тим слід зауважити, що використання ШІ покладає на компанії певні обмеження. Так, інструменти ШІ повинні бути інтегрованими у загальнокорпоративну систему управління ризиками, при чому слід врахувати ймовірну упередженість інструментів ШІ та передбачити контроль з боку кваліфікованих фахівців на основних етапах розвідки. Алгоритми, які блокують транзакції або присвоюють негативні рейтинги контрагентам, повинні надавати чітке та логічне обґрунтування своїх рішень, зрозуміле для аудиторів та регуляторів. Такі заходи також необхідні для забезпечення юридичної підзвітності відповідальними особами.

### **Список використаних джерел**

1. Corporate Intelligence. *PwC US*. URL: <https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/analytics-intelligence/intelligence.html> (дата звернення: 27.04.2026).
2. How OSINT is valuable to threat monitoring and investigations. *EY - Global*. URL: [https://www.ey.com/en\\_us/insights/forensic-integrity-services/value-of-osint-to-threat-monitoring-and-investigations](https://www.ey.com/en_us/insights/forensic-integrity-services/value-of-osint-to-threat-monitoring-and-investigations) (дата звернення: 27.04.2026).
3. How to use Open-Source Intelligence (OSINT) for investigations. *Moody's*. URL: <https://www.moody.com/web/en/us/insights/compliance-tpm/open-source-intelligence-osint-types-tools-and-methods.html> (дата звернення: 25.04.2026).
4. OSINT AI: як оптимізувати своє розслідування у 2025 році. *Molfar*. URL: <https://molfar.com/blog/osint-ai-yak-optymizuvaty-svoe-rozsliduvannya-u-2024-roci> (дата звернення: 26.04.2026).
5. Study Report: Unlocking the Value of Open-Source Intelligence (OSINT) for Customs Enforcement. *World Customs Organization*. URL: [https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/enforcement-and-compliance/activities-and-programmes/security-programme/osint-report\\_final.pdf](https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/enforcement-and-compliance/activities-and-programmes/security-programme/osint-report_final.pdf) (дата звернення: 26.04.2026).

**Дмитрук П. А.,**  
*курсант 2 курсу факультету № 2*  
*(Львівський державний університет внутрішніх справ)*  
**Науковий керівник: Ревак І. О.,**  
завідувач науково-дослідної лабораторії  
OSINT-досліджень та безпекової аналітики ННІУПБ,  
доктор економічних наук, професор  
*(Львівський державний університет внутрішніх справ)*

## **РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ У ВДОСКОНАЛЕННІ OSINT-ІНСТРУМЕНТАРІЮ В СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ**

У сучасних умовах трансформації безпекового середовища, зумовленої цифровізацією та зростанням обсягів відкритих даних, штучний інтелект стає ключовим чинником підвищення ефективності OSINT як інструменту аналітичного забезпечення системи національної безпеки. Інтеграція алгоритмів машинного навчання, обробки природної мови та автоматизованого аналізу великих масивів інформації сприяє не лише оптимізації процесів збору та обробки відкритих джерел, але й формує нові можливості для раннього виявлення загроз, ідентифікації прихованих зв'язків та прогнозування ризиків. У цьому контексті дослідження ролі штучного інтелекту у вдосконаленні OSINT-напрямку набуває особливої актуальності, оскільки дозволяє визначити як потенціал його практичного застосування, так і пов'язані з ним виклики у сфері забезпечення національної безпеки.

Сучасний ландшафт кіберзагроз охоплює сукупність ризиків, з якими зіштовхуються організації в різних сферах діяльності залежно від їхнього функціонального та цифрового контексту. Кіберзагрози характеризуються динамічним розвитком і поступовим проникненням у всі без винятку сфери суспільного та організаційного функціонування, що особливо посилюється в умовах широкої інтернетизації та впровадження цифрових технологій. Зазначені процеси зумовлюють зростання загального рівня кіберризиків і ускладнення їхньої структури. Водночас численні кіберінциденти, що фіксуються у цифровому середовищі, формують постійний фактор загрози для організацій, які здійснюють діяльність у віртуальному просторі [1]. Станом на 2026 рік штучний інтелект трансформувався у системоутворюючий елемент сучасного глобального порядку, виступаючи ключовим інструментом упорядкування та структурування значних обсягів інформації. Водночас, незважаючи на значний функціональний потенціал, ШІ залишається алгоритмічно зумовленою системою, позбавленою інтуїтивного сприйняття та здатності до самостійного критичного осмислення. У цих умовах, особливо в контексті сучасних воєнних викликів, актуалізується дослідження ролі ШІ у вдосконаленні інструментарію OSINT в системі національної безпеки.

Впровадження технологій штучний інтелект зумовило глибинну трансформацію методологічних підходів до OSINT, забезпечивши перехід від лінійних моделей аналізу до комплексного автоматизованого інтелектуального синтезу даних [2]. У межах проведеного дослідження на базі науково-аналітичного гуртка «Цифрові детективи» виокремлено чотири ключові вектори застосування інструментарію ШІ, що відображають основні напрями його інтеграції в аналітичну практику.

Обробка великих масивів даних (Big Data): алгоритми штучний інтелект забезпечують оперативне структурування розрізнених інформаційних потоків шляхом інтеграції даних із систем відеоспостереження, архівних джерел та цифрових слідів. Це створює передумови для автоматизованого формування хронології подій, а також для виявлення латентних

зв'язків, ідентифікація яких у межах традиційного ручного аналізу потребувала б значних часових і ресурсних витрат.

Геопросторова аналітика та Computer Vision: застосування штучний інтелект у поєднанні з технологіями Computer Vision забезпечує можливість детермінації точних геолокацій на основі аналізу візуальних характеристик ландшафту, архітектурних об'єктів і світлотіньових параметрів фотозображень. Водночас системи комп'ютерного зору дозволяють здійснювати ідентифікацію осіб та об'єктів за складними параметризованими запитами, формуючи аналітичне підґрунтя для створення автоматизованих цифрових профілів.

Предиктивна аналітика (метод «Sentientia-Predictor»): зазначений підхід ґрунтується на здатності штучний інтелект здійснювати аналіз патернів попередньої злочинної активності з метою прогнозування ймовірних загроз у перспективі. Його застосування забезпечує перехід від реактивної до превентивної моделі діяльності правоохоронних органів, що має визначальне значення для підвищення ефективності функціонування системи національної безпеки.

«Контр-ШІ» інструментарій: спеціалізовані програмні рішення, орієнтовані на верифікацію цифрового контенту, що із застосуванням штучний інтелект забезпечують оперативну ідентифікацію дідфейків та синтетичних даних, мінімізуючи ризики дезорієнтації аналітичних і слідчих процесів та запобігаючи формуванню хибних висновків у межах розслідування.

Штучний інтелект у системі OSINT виступає об'єктивно необхідним елементом забезпечення національної безпеки в умовах гібридних загроз сучасного безпекового середовища. Водночас визначальним фактором ефективності його застосування є здатність до інтеграції алгоритмічних можливостей із глибинною аналітичною інтерпретацією та належним рівнем оперативної компетентності [3].

Динаміка кількісних показників свідчить про стрімке зростання рівня інтеграції штучний інтелект у практику OSINT: упродовж 2020–2026 років частка його використання зростає орієнтовно з 10–15% до понад 75–85%, що супроводжується скороченням часу аналітичної обробки інформації на 40–70% [4]. У цьому контексті ШІ доцільно розглядати як стратегічний інструмент підвищення ефективності правоохоронної діяльності, застосування якого потребує високого рівня професійної підготовки та відповідальності. Автоматизація процесів і розвиток предиктивної аналітики суттєво розширюють можливості виявлення та розкриття правопорушень, однак ключова роль у прийнятті рішень і надалі належить людині як носію правових та етичних засад. Відтак пріоритетним завданням є формування здатності до компетентного використання зазначеного інструментарію з метою забезпечення правопорядку в умовах цифровізації суспільства.

### **Список використаних джерел**

1. Корпоративна кібербезпека: Роль ШІ у захисті даних. URL: <https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/corporate-cybersecurity-ai-role-in-data-protection>
2. Гбур З. В. Використання штучного інтелекту в інформаційній безпеці України DOI: 10.32702/2307-2156-2022.1.2. URL: [http://www.dy.nayka.com.ua/pdf/1\\_2022/4.pdf](http://www.dy.nayka.com.ua/pdf/1_2022/4.pdf)
3. Василюк М. В., Василюк А. В., Притула М.О. Роль штучного інтелекту в інформаційній безпеці України. URL: <https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/47934/22795.pdf?sequence=3&isAllowed=y>
4. OSINT and AI in 2026: How the Tool Landscape Is Being Rebuilt From the Ground Up. URL: [https://nullsec.news/osint-ai-2026-tool-landscape?utm\\_source=https://shadowdragon.io/blog/osint-year-in-review-report/?utm\\_source](https://nullsec.news/osint-ai-2026-tool-landscape?utm_source=https://shadowdragon.io/blog/osint-year-in-review-report/?utm_source)

**Д'яков А. В.,**  
доцент кафедри інформаційних технологій,  
кандидат технічних наук  
(Львівський державний університет внутрішніх справ)

## **ІНТЕГРАЦІЯ OSINT ТА ГЕОІНФОРМАЦІЙНОГО АНАЛІЗУ У ВЕРИФІКАЦІЇ ВОЄННИХ ЗЛОЧИНІВ**

Сучасні воєнні конфлікти характеризуються цифровізацією бойових дій та широким використанням відкритих інформаційних ресурсів, що зумовлює трансформацію підходів до документування воєнних злочинів. У цих умовах OSINT виступає важливим інструментом формування доказової бази, забезпечуючи оперативне отримання, аналіз і верифікацію цифрових слідів подій.

Методологічна основа застосування OSINT ґрунтується на трьох взаємопов'язаних процесах: зборі, верифікації та інтеграції відкритих даних. Визначальними критеріями якості інформації є достовірність (джерело, авторство, метадані), релевантність (відповідність контексту події) та відтворюваність (можливість повторної перевірки) [1]. Як системний інструмент ситуаційної обізнаності, OSINT поєднує соціальні джерела, медійні ресурси, технічні дані та геопросторові компоненти. Це забезпечує фіксацію фактів, встановлення обставин подій, ідентифікацію причетних осіб та підтвердження наслідків. Застосування OSINT має відповідати міжнародному стандарту *Berkeley Protocol on Digital Open Source Investigations*, який визначає принципи автентичності та стандарти верифікації цифрового контенту [2]. Це створює основу юридично значущого процесу формування доказів та зумовлює необхідність поглибленої просторово-часової верифікації даних.

Геоінформаційний аналіз забезпечує встановлення просторових і часових параметрів подій, що є критичним для перетворення OSINT-даних на доказову інформацію. На цьому етапі геопросторова складова інтегрує текстові, візуальні та технічні дані в єдину аналітичну модель. Ключовими методичними інструментами виступають геолокація (співставлення візуальних орієнтирів із картографічними даними) та хронолокація (аналіз метаданих, погодних умов та непрямих ознак). Застосування цих методів дозволяє уточнювати параметри подій навіть за умов інформаційної невизначеності. Подальший просторовий аналіз передбачає кореляцію даних у геоінформаційному середовищі для виявлення взаємозв'язків між місцями ураження, переміщенням техніки та об'єктами інфраструктури [3]. Відповідно до вимог Протоколу Берклі, результати такого аналізу підлягають документуванню та підтвердженню незалежними джерелами.

Застосування вказаного методу у верифікації воєнних злочинів є одним із найбільш перспективних напрямів сучасної цифрової криміналістики, оскільки саме просторовий компонент дозволяє перетворити фрагментарні відкриті дані на логічно узгоджену доказову конструкцію. Якщо OSINT забезпечує отримання фото-, відео-, текстових та технічних матеріалів, то геоінформаційний аналіз надає інструменти для встановлення місця, часу, масштабу та взаємозв'язків між подіями [1; 4]. Практично це реалізується у кількох взаємопов'язаних напрямках.

Передусім геоінформаційні технології застосовуються для точної геолокації місця події. Ідеться про співставлення зображень або відеозаписів із супутниковими знімками, картографічними сервісами та тривимірними моделями місцевості. Наявність характерних

орієнтирів — дорожніх розв'язок, конфігурації будівель, лісосмуг, мостів, ліній електропередач, рельєфу місцевості — дозволяє з високою точністю визначити координати місця обстрілу, руйнування чи переміщення військової техніки. Це особливо важливо у випадках, коли сторони конфлікту заперечують сам факт події або поширюють дезінформацію.

Другим важливим напрямом є хронологія подій, тобто встановлення часу їх виникнення через просторово-часові ознаки. Геоінформаційне середовище дозволяє поєднувати координати із часовими метаданими, напрямком тіней, погодними умовами, сезонними змінами рослинності, станом дорожнього покриття чи освітлення. Наприклад, аналіз довжини тіней на відео разом із сонячною моделлю місцевості може допомогти визначити приблизний час зйомки. Це має доказове значення при перевірці заяв про алібі, часу нанесення удару або послідовності бойових епізодів.

Окреме значення має аналіз траєкторій та напрямків ураження. За допомогою ГІС можливо моделювати напрям польоту снарядів, розміщення вогневих позицій, радіуси ураження артилерії, можливі маршрути пересування техніки. Поєднання даних про воронки, пошкодження будівель та координати місцевості дозволяє встановити ймовірний сектор обстрілу, а відтак і потенційне джерело вогню. Геоінформаційний аналіз також використовується для фіксації наслідків воєнних злочинів у динаміці. Порівняння супутникових знімків за різні дати дає змогу документувати руйнування житлових кварталів, знищення лікарень, шкіл, об'єктів енергетики, зміну ландшафту після підривів дамб або мінування територій. Такі матеріали мають високу доказову цінність, оскільки формуються незалежними джерелами дистанційного зондування Землі.

Ще одним напрямом є виявлення системності та повторюваності атак. Просторове групування епізодів у ГІС дозволяє побачити закономірності: концентрацію ударів по цивільних районах, регулярні обстріли об'єктів критичної інфраструктури, збіг атак із гуманітарними маршрутами чи евакуаційними коридорами. Якщо окремий інцидент може трактуватися як випадковий, то серія однотипних подій у просторі та часі свідчить про можливий умисний характер дій. У практичній площині важливою є інтеграція геоінформаційного аналізу з базами доказів, коли кожен цифровий артефакт — фото, відео, свідчення очевидця, телекомунікаційні дані, супутниковий кадр — прив'язується до координат і часу. У результаті формується єдина карта доказів, де слідчий або аналітик бачить цілісну картину події.

Не менш важливим є використання ГІС для гуманітарно-правової оцінки цілей ураження. Накладання шару військових об'єктів, цивільної забудови, медичних закладів, шкіл, культових споруд, зон евакуації дозволяє оцінити, чи перебував об'єкт під особливим захистом міжнародного гуманітарного права. Це суттєво підсилює юридичну аргументацію у справах щодо атак на цивільне населення.

Інтеграція OSINT та геоінформаційних технологій забезпечує узгоджений аналіз різнорідних цифрових даних у межах єдиного середовища, поєднуючи контентний аналіз із просторово-часовою інтерпретацією. У межах інтеграційного підходу дані проходять послідовні етапи: збір, первинну верифікацію, структурування, геокодування та аналітичну обробку. Практична цінність такої синергії полягає у зіставленні інформаційних фрагментів у спільному просторовому контексті, що підвищує обґрунтованість висновків. Узгодження візуальних, текстових і технічних даних за принципом множинної верифікації гарантує цілісність аналітичної моделі. На цій основі здійснюється перехід від аналізу окремих цифрових свідчень до комплексного відтворення подій у ГІС-середовищі [4].

Таким чином, геоінформаційний аналіз у верифікації воєнних злочинів виконує не допоміжну, а системоутворюючу функцію. Саме він забезпечує просторову точність, часову узгодженість, логічну повноту та відтворюваність доказів, що є критично важливим для національних розслідувань і міжнародного правосуддя. Подальший розвиток галузі пов'язаний із системною інтеграцією OSINT в інформаційно-аналітичні процеси правоохоронних органів та уніфікацією методичних підходів відповідно до міжнародних стандартів. Перспективним напрямом є автоматизація аналітичних процесів із застосуванням штучного інтелекту для обробки великих масивів даних, розвиток міжплатформної інтеграції для об'єднання різних джерел у єдині аналітичні системи, а також адаптація національного законодавства до вимог Протоколу Берклі.

Крім того, актуальною залишається інституціоналізація OSINT, що включає підготовку фахівців та створення спеціалізованих підрозділів, які сприятимуть підвищенню ефективності документування воєнних злочинів.

### **Список використаних джерел**

1. Д'яков А. В., Дядюшкін О. В. OSINT-технології як інструмент підвищення ситуаційної обізнаності в умовах гібридних загроз. *Національні інтереси України : науково-практичний журнал*. 2025. № 12(17). С. 154–169. DOI: 10.52058/3041-1793-2025-12(17)-154-169.

2. Berkeley Protocol on Digital Open Source Investigations : a practical guide on the effective use of digital open source information in investigating violations of international criminal, human rights and humanitarian law / Office of the United Nations High Commissioner for Human Rights. Geneva ; New York : United Nations, 2022. URL: [https://www.ohchr.org/sites/default/files/2024-01/OHCHR\\_BerkeleyProtocol.pdf](https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf) (дата звернення: 12.04.2026).

3. Д'яков А. В. Просторовий аналіз у кібер- та інформаційній безпеці: синергія ГІС та OSINT-методів. *Актуальні проблеми діяльності складових сектору безпеки і оборони України : тези II Всеукраїнської науково-практичної конференції (м. Золочів, 30 жовтня 2025 р.)*. Харків: Вид-во Національної академії Національної гвардії України, 2025. С. 155–157.

4. Д'яков А. В., Дядюшкін О. В. Просторово-часове моделювання подій на основі відкритих даних у геоінформаційних системах для підтримки прийняття рішень. *Національні інтереси України : науково-практичний журнал*. 2026. № 4(21). С. 298–310. DOI: 10.52058/3041-1793-2026-4(21)-298-310.

**Зоренко Д. С.,**  
співробітник Інституту Служби безпеки України  
(Національний юридичний університет  
імені Ярослава Мудрого)

## **ВИКОРИСТАННЯ РЕКЛАМНИХ ІДЕНТИФІКАТОРІВ У КОНТЕКСТІ РОЗВІДКИ З ВІДКРИТИХ ДЖЕРЕЛ**

Еволюція екосистеми цифрової реклами призвела до створення однієї з найбільш деталізованих інфраструктур профілювання в історії людства. В її основі лежить мобільний рекламний ідентифікатор (Mobile Advertising Identifiers, MAID), що спочатку розроблявся як інструмент для псевдонімного відстеження поведінки користувачів з метою персоналізації маркетингу. Однак публічні розслідування The New York Times (датасет із понад 50 мільярдів геолокаційних пінгів від 12 мільйонів американських смартфонів, 2019 р.) [1] та Vice/Motherboard (про продукт Locate X компанії Babel Street, 2020 р.) [2] наочно продемонстрували, що вказані відомості дозволяють з точністю до метрів відтворити повсякденне життя конкретної особи, встановити місце її роботи, проживання, релігійні практики та соціальні зв'язки.

Особливої гостроти ця проблематика набула у 2024-2026 рр. після серії розслідувань медіа-структур WIRED, Bayerischer Rundfunk та Netzpolitik.org про відкритий продаж 3,6 мільярда геолокаційних координат 11 мільйонів пристроїв у Німеччині (зокрема на авіабазах Бюхель, Рамштайн та полігоні Графенвюр, де тренувалися українські військові) за 14 000 доларів США на місяць [3].

Загалом під рекламним ідентифікатором слід розуміти унікальний чи умовно-унікальний маркер, який встановлюється, керується або зчитується на пристрої кінцевого користувача з метою ідентифікації гаджету для цілей маркетингової аналітики та таргетованої реклами. Його слід відрізнити від апаратних ідентифікаторів, таких як IMEI, серійний номер або MAC-адреса.

MAID дозволяє розробникам монетизувати свої програмні продукти, надаючи рекламодавцям стандартизовану систему для відстеження активності особи шляхом: 1) персонального вибору – можливості ідентифікувати користувача як частини конкретного сегмента аудиторії (наприклад, «любителі кави» або «в пошуку нового автомобіля») на основі його попередньої поведінки в різних додатках; 2) управління частотою та актуальністю – людина не побачить одне й те саме оголошення занадто багато разів для запобігання втомі від реклами; 3) конкретизації – визначення того, який саме рекламний «контакт» призвів до покупки або встановлення застосунку.

Сучасне середовище мобільних гаджетів спирається на два основні типи таких ідентифікаторів: Apple Identifier for Advertisers (IDFA) для екосистеми iOS та Google Advertising ID (AAID або GAID) для пристроїв на базі Android. Ці маркери є унікальними рядками з 32 символів, розділених дефісами, що за замовчанням генеруються операційною системою пристрою та надаються стороннім додатками через спеціалізовані набори засобів розробки програмного забезпечення (Software Development Kit, SDK). За необхідності MAID може бути скинутий або видалений користувачем у будь-який час. Крім того, з випуском iOS 14.5 у 2021 році та впровадженням фреймворку App Tracking Transparency компанія Apple змінила механізм доступу до цього ідентифікатора на модель явного дозволу (opt-in) – у разі

незгоди особи з відстеженням, значення IDFA замінюється рядком нулів. На відміну від цього підходу, Google тривалий час дотримується моделі відмови (opt-out), де цей маркер передається за замовчуванням, поки користувач самостійно не обмежить персоналізацію реклами в налаштуваннях гаджета.

Ключовим місцем, де зазначені ідентифікатори «кристалізуються» та стають товаром, є інфраструктура системи автоматизованої купівлі-продажу інтернет-реклами через аукціон у реальному часі (Real-Time Bidding, RTB). Його цикл займає менше секунди, що робить процес непомітним для пересічної людини. Ефективність RTB базується на здатності оцінювати кожен показ індивідуально, а не купувати рекламу пакетами на тисячі показів.

Зокрема, у момент звернення користувача до вебресурсу або застосунку з рекламною підтримкою клієнтське середовище (браузер або мобільний SDK) автоматично фіксує контекстні метадані – рекламний ідентифікатор, геолокацію, тип пристрою та операційну систему, оператор мобільного зв'язку, мітки часу (всього близько 150 позицій). На їх основі платформа формує запит на ставку, який одночасно розсилається потенційним покупцям (учасникам аукціону) через рекламну біржу. При цьому, без MAID рекламодавці бачать лише контекст (наприклад, «запит з додатка про погоду»), але не знають, хто стоїть за ним, що робить неможливим ретаргетинг або його детальну сегментацію.

Кожен з покупців протягом встановленого таймауту (як правило 80-400 мс) зіставляє рекламний ідентифікатор із власними базами даних поведінкових профілів для оцінки релевантності конкретного користувача цілям власних рекламних кампаній та формує відповідь із розміром ставки. Рекламна біржа агрегує ставки, визначає переможця за правилом аукціону першої ціни й ініціює доставку рекламного контенту, який починає відтворюватися в клієнтському середовищі паралельно із завантаженням основного ресурсу. Після показу реклами система відстеження передає відомості про взаємодію з користувачем назад до платформ управління даними, де рекламний ідентифікатор збагачується новими поведінковими атрибутами. Цей процес відбувається мільярди разів на добу, створюючи безперервний потік телеметрії, що фіксує кожен крок людини.

Принципово важливим є те, що запит на ставку отримують усі запрошені учасники торгів незалежно від результатів аукціону. Таким чином, кожен з них одержує пакет метаданих з пристрою користувача майже без будь-яких правових зобов'язань щодо їх використання виключно в рекламних цілях. Зазначена особливість архітектури RTB є підставою для розгляду подібних відомостей як потенційного інструменту масового збору чутливої для людини інформації. Дійсно, спеціалізовані платформи, приміром Babel Street, Venntel, Anomaly Six, Fog Data Science, AppGoblin, агрегують величезну кількість цих метаданих та в подальшому надають державним і корпоративним клієнтам доступ до них у вигляді готових інформаційно-аналітичних продуктів.

Хоча MAID безпосередньо не містять персональних даних, таких як ім'я чи номер телефону, їх цінність у контексті OSINT-досліджень реалізується через аналіз всієї сукупності відомостей, оскільки рекламні ідентифікатори можуть залишатися незмінними протягом місяців або навіть років, дозволяючи формувати довгострокові патерни поведінки об'єкта зацікавленості. Для цього зазвичай використовують дві основні методології: 1) детерміноване зіставлення, що базується на використанні точних ідентифікаторів (наприклад, якщо користувач реєструється в додатку за допомогою особистої електронної пошти, а система одночасно фіксує MAID його пристрою); 2) імовірнісне зіставлення, яке має місце у разі відсутності прямих зв'язків і відбувається шляхом аналізу збігів за IP-адресами, типами

пристроїв, історією переглядів та регулярними географічними перетинами (приміром, якщо смартфон і ноутбук щовечора з'являються в одній житловій мережі Wi-Fi, а вдень – в одній офісній мережі, їх з великою долею ймовірності можна віднести до одного власника).

З огляду на це, одним із найпотужніших застосувань MAID є дослідження патернів повсякденної життєдіяльності людини, оскільки агрегування історичних геосигналів дозволяє визначати:

- місця проживання та роботи – розташування (координати), де пристрій найчастіше перебуває між 23:00 та 06:00 або в робочі години відповідно;

- коло спілкування – періодична присутність гаджету протягом тривалого часу в конкретних локаціях як вдень, так і ввечері, на вихідних або під час відпочинку у поєднанні з виявленням інших пристроїв, які часто з'являються поруч із цільовим об'єктом, що може свідчити про соціальні чи професійні зв'язки між їхніми власниками;

- поведінкові аномалії – будь-які відхилення від звичайного розпорядку особи, наприклад, виїзд за кордон або до іншого регіону, зміна маршрутів пересування чи участь у масових заходах тощо;

- перелік потенційних працівників (відвідувачів) організації – отримання списку усіх рекламних ідентифікаторів, які з'являлися в певній області на місцевості (будівлі) протягом визначеного проміжку часу;

- ланцюгів постачання та руху активів – відстеження переміщення пристроїв уздовж логістичних маршрутів з метою виявлення санкційних порушень, відстеження контрабанди, місць дислокації командних пунктів або складів боєприпасів та ін.;

- специфічні мобільні застосунки, якими користується особа – наявність додатків для знайомств, криптогаманців або професійного софту.

При цьому, результати аналізу MAID необхідно корелювати з іншими джерелами OSINT для створення цілісного профілю об'єкта зацікавленості.

На завершення варто підкреслити, що рекламна інфраструктура, створена для стимулювання споживання, мимоволі перетворилася на глобальну систему сенсорів. Для дослідника MAID – це унікальне вікно в життя конкретного користувача мобільного пристрою, а для людини – цифровий автограф, який майже неможливо стерти в умовах сучасного цифрового світу.

### **Список використаних джерел**

1. Thompson, S. A., & Warzel, C. (2019, December 19). Twelve million phones, one dataset, zero privacy. The New York Times. <https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html> (дата звернення 30.04.2026).

2. Cox, J. (2020, August 17). Secret Service bought phone location data from apps, contract confirms. Vice Motherboard. <https://www.vice.com/en/article/secret-service-phone-location-data-babel-street/> (дата звернення 30.04.2026).

3. Cox, J., & Mehrotra, D. (2024, November 19). Anyone can buy data tracking US soldiers and spies to nuclear vaults and brothels in Germany. WIRED. <https://www.wired.com/story/phone-data-us-soldiers-spies-nuclear-germany/> (дата звернення 30.04.2026).

**Іванишин М. І.,**  
молодший науковий співробітник  
(Національна академія сухопутних військ  
імені гетьмана Петра Сагайдачного)  
**Ленівий О. Ю.,**  
старший науковий співробітник  
(Національна академія сухопутних військ  
імені гетьмана Петра Сагайдачного)

## **ЗАСТОСУВАННЯ OSINT У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ ТА ЗАБЕЗПЕЧЕННІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ**

Трансформація безпекового середовища в умовах повномасштабної збройної агресії російської федерації проти України актуалізувала потребу в переосмисленні методологічного апарату правоохоронної діяльності та розвідувально-аналітичної роботи в інтересах національної безпеки. Серед новітніх підходів до збору та аналізу інформації особливе місце посідає розвідка на основі відкритих джерел – OSINT (Open Source Intelligence), яка завдяки своїй доступності, оперативності та широті охоплення перетворилась на один із базових інструментів сучасної правоохоронної практики.

OSINT у правоохоронному контексті охоплює систематичний збір та аналіз публічно доступної інформації з метою попередження, виявлення та документування правопорушень, встановлення особи підозрюваних, відстеження злочинних мереж та підтримки оперативно-розшукової діяльності. Відповідно до сучасної аналітичної доктрини, OSINT включає дані соціальних мереж, відкриті бази даних державних реєстрів, відомості засобів масової інформації, матеріали з публічних веб-ресурсів, а також дані геопросторових сервісів та супутникових знімків [1]. Комплексне використання цих джерел дозволяє правоохоронним органам держави формувати повну оперативну картину без залучення засобів негласного збору інформації.

В умовах воєнного стану в Україні OSINT набуває особливого значення в декількох критично важливих напрямках правоохоронної діяльності. По-перше, у сфері протидії диверсійно-розвідувальній діяльності противника. Аналіз відкритих джерел дозволяє виявляти ознаки агентурних мереж, встановлювати підозрілі патерни поведінки осіб, які можуть бути пов'язані з ворожими структурами, а також відстежувати канали передачі розвідувальних даних через публічні комунікаційні платформи. Так, Служба безпеки України активно використовує OSINT-методи для нейтралізації агентури противника на підконтрольній території [2].

По-друге, OSINT застосовується в боротьбі з кіберзлочинністю та злочинністю у сфері інформаційних технологій. Технічний аналіз відкритих даних – IP-адрес, доменних імен, цифрових сертифікатів, метаданих публікацій – дозволяє ефективно відстежувати інфраструктуру кіберзлочинців, атрибутувати хакерські атаки та збирати цифрові докази для кримінального переслідування. Особливої актуальності це набуває в контексті зростання кількості кібератак на об'єкти критичної інфраструктури України, здійснюваних угрупованнями, пов'язаними із спецслужбами росії.

По-третє, у розслідуванні економічних злочинів та корупції OSINT забезпечує можливість аналізу майнового стану підозрюваних осіб шляхом моніторингу відкритих реєстрів нерухомості, даних корпоративного реєстру, відомостей про державні закупівлі та декларацій публічних службовців. Національне антикорупційне бюро України (НАБУ) та

Спеціалізована антикорупційна прокуратура (САП) використовують OSINT-аналіз як допоміжний метод у розслідуванні корупційних схем, особливо в частині встановлення прихованих активів та зв'язків між фігурантами справ [3].

По-четверте, OSINT відіграє важливу роль у системі забезпечення публічної безпеки та охорони громадського порядку. Моніторинг відкритих комунікаційних каналів дозволяє завчасно виявляти плановані протиправні акції, відстежувати діяльність екстремістських угруповань та попереджати масові заворушення. В умовах підвищеної загрози тероризму та диверсій аналіз відкритих джерел стає невід'ємним елементом систем раннього попередження загроз.

Важливим аспектом є питання правового регулювання використання OSINT у правоохоронній діяльності. Попри те, що йдеться про публічно доступну інформацію, збір і обробка персональних даних громадян, навіть із відкритих джерел, має здійснюватись з дотриманням вимог законодавства про захист персональних даних та конституційних гарантій права на приватність. В Україні це питання залишається недостатньо врегульованим: чинна нормативна база не містить спеціальних положень щодо OSINT-діяльності правоохоронних органів, що створює правову невизначеність та потенційні ризики зловживань [4]. Необхідним є розроблення відповідного законодавства, яке б забезпечило баланс між ефективністю оперативно-розшукової роботи та захистом прав і свобод громадян.

Перспективним напрямом розвитку OSINT у правоохоронній сфері є інтеграція методів штучного інтелекту та машинного навчання для автоматизованої обробки великих масивів відкритих даних. Застосування NLP-технологій для моніторингу соціальних мереж, комп'ютерного зору для аналізу відеоконтенту та алгоритмів виявлення аномалій для ідентифікації підозрілих патернів здатне суттєво підвищити ефективність роботи правоохоронних органів. Водночас запровадження таких систем потребує чіткого законодавчого регулювання та механізмів незалежного нагляду задля недопущення надмірного стеження та порушень громадянських свобод [5].

Таким чином, OSINT є потужним і перспективним інструментом правоохоронної діяльності та забезпечення національної безпеки України. Ефективне впровадження цього методу потребує комплексного підходу, що включає: формування нормативно-правової бази, яка регулює збір та використання відкритих даних у правоохоронній практиці; розбудову спеціалізованих підрозділів OSINT-аналізу в структурі правоохоронних органів та спецслужб; системну підготовку фахівців із цифрової розвідки; налагодження міжвідомчої та міжнародної взаємодії в обміні OSINT-даними. Реалізація вищезазначених заходів дозволить суттєво підвищити оперативні можливості правоохоронної системи України в умовах тривалого гібридного протистояння.

### **Список використаних джерел**

1. Lowenthal M.M. *Intelligence: From Secrets to Policy*. 8th ed. CQ Press, 2022. 448 p.
2. Грищенко І. В. Використання розвідки на основі відкритих джерел у діяльності органів безпеки: зарубіжний досвід та перспективи для України. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2023. № 2. С. 112–119.
3. Transparency International Ukraine. *Відкриті дані як інструмент антикорупційних розслідувань : практичний посібник*. Київ, 2022. 64 с.
4. Задорожній О. В. Правове регулювання збору розвідувальної інформації з відкритих джерел: порівняльно-правовий аналіз. *Право України*. 2023. № 4. С. 67-81.
5. Završnik A. *Criminal Justice, Artificial Intelligence Systems, and Human Rights*. ERA Forum. 2020. Vol. 20. Is. 4. P. 567–583.

**Іванченко А. О.,**  
начальник кафедри розвідки – начальник розвідки,  
кандидат технічних наук, доцент  
(Київський інститут Національної гвардії України)

## **ІНТЕГРАЦІЯ OSINT У СИСТЕМУ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ**

У сучасних умовах гібридних загроз, інформаційного протиборства та повномасштабної збройної агресії проти України особливого значення набуває ефективне використання відкритих джерел інформації (OSINT) у системі забезпечення національної безпеки. Зростання обсягів доступних даних, розвиток цифрових технологій та поширення соціальних мереж створюють нові можливості для збору, аналізу та використання інформації в інтересах держави.

OSINT (Open Source Intelligence) розглядається як систематизований процес пошуку, відбору, обробки та аналізу інформації з відкритих джерел з метою отримання розвідувальних даних. Основними джерелами OSINT є мережа Інтернет, соціальні мережі, засоби масової інформації, супутникові знімки, геопросторові дані, відкриті бази даних та інші доступні інформаційні ресурси.

Інтеграція OSINT у систему національної безпеки передбачає включення відповідних методів і технологій у діяльність сектору безпеки і оборони, правоохоронних органів, аналітичних центрів та органів державного управління. Одним із ключових напрямів є використання OSINT для підвищення рівня ситуаційної обізнаності, що дозволяє оперативно виявляти загрози, прогнозувати розвиток обстановки та приймати обґрунтовані управлінські рішення.

Важливим аспектом є застосування OSINT у військовій сфері, зокрема для аналізу місцевості, виявлення демаскувальних ознак діяльності противника, оцінки інфраструктури та логістичних маршрутів. Використання супутникових знімків і аерофотоматеріалів у поєднанні з іншими відкритими джерелами дозволяє значно підвищити ефективність розвідки без залучення додаткових ресурсів.

Разом із тим, інтеграція OSINT супроводжується низкою викликів, серед яких: необхідність перевірки достовірності інформації, протидія дезінформації, забезпечення кібербезпеки, а також підготовка кваліфікованих фахівців. Важливою є розробка єдиних методичних підходів, стандартів обробки інформації та впровадження сучасних інструментів автоматизації аналітичної діяльності.

Перспективним напрямом розвитку є поєднання OSINT із технологіями штучного інтелекту, що дозволяє автоматизувати процеси аналізу великих масивів даних, виявляти закономірності та підвищувати швидкість прийняття рішень. Це створює передумови для формування інтегрованих систем безпекової аналітики.

Таким чином, інтеграція OSINT у систему забезпечення національної безпеки є необхідною умовою підвищення ефективності діяльності державних інституцій в умовах сучасних загроз. Подальший розвиток цього напрямку потребує комплексного підходу, що включає вдосконалення нормативно-правової бази, розвиток технологічної інфраструктури та підготовку висококваліфікованих кадрів.

#### **Список використаних джерел**

1. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII.
2. Стратегія національної безпеки України «Безпека людини – безпека країни» : Указ Президента України від 14.09.2020 № 392/2020.
3. Доктрина інформаційної безпеки України : Указ Президента України від 25.02.2017 № 47/2017.
4. Про інформацію : Закон України від 02.10.1992 № 2657-XII.
5. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI.
6. Дубов Д. В. Інформаційна безпека України: сучасні виклики та загрози. Київ : НІСД, 2016.
7. Горбулін В.П. Світова гібридна війна: український фронт. К.: НІСД, 2017.

**Ігнат'єв Б. М.,**  
доцент кафедри управління та інформаційно-аналітичного  
забезпечення оперативно-службової діяльності  
(Національна академія Служби безпеки України)

## **ВПЛИВ ЦИФРОВОГО ВІДБИТКУ ПРОФІЛЮ ВЕБОГЛЯДАЧА НА КОНФІДЕНЦІЙНІСТЬ ОСІНТ-АНАЛІТИКА**

У сучасному світі цифрових технологій анонімність є критично важливою умовою безпечної роботи в мережі, особливо під час виконання ОСІНТ-завдань із використанням сумнівних, ворожих або спеціально контрольованих ресурсів. Одним із ключових ризиків у цьому контексті є цифровий відбиток вебоглядача – сукупність технічних сигнатур програмного середовища користувача, зокрема браузера, операційної системи, пристрою та його налаштувань, які сайт може збирати під час відвідування сторінки. До таких маркерів належать рядок ідентифікації вебоглядача, мова й часова зона, параметри екрана, набір шрифтів, особливості відтворення графіки через Canvas і WebGL, обробка звуку через AudioContext, доступні програмні інтерфейси, встановлені розширення та поведінка JavaScript. На відміну від cookie-файлів, такий відбиток не обов'язково зберігається на пристрої: сайт може щоразу відтворювати його заново на основі спостережуваних параметрів, тому в науковій літературі його розглядають як прихований ідентифікатор, здатний працювати навіть після очищення cookie або в приватному режимі [1; 4].

Для ОСІНТ-аналітика, який працює з відкритими джерелами, цифровий відбиток профілю вебоглядача безпосередньо стосується операційної безпеки. Під час відвідування форумів, пропагандистських ресурсів, витоків даних, сайтів державних структур і платформ, що опосередковано контролюються державою або є з нею афілійованими, а також пов'язаних із ворожою інфраструктурою, осінтер може залишати сталі технічні сліди. Навіть якщо ресурс не знає справжнього імені користувача, він потенційно здатен пов'язувати повторні візити, різні акаунти, пошукові легенди, роботу з кількох доменів або часову періодичність мережевої активності. VPN у такому випадку приховує IP-адресу, але не усуває відмінності у шрифтах, графічному стеку, часовій зоні, розмірі вікна чи поведінці браузерних інтерфейсів.

Актуальність цієї загрози підтверджена емпіричними дослідженнями. Зокрема, у науковому проєкті Raportclick, присвяченому ідентифікації браузерів за допомогою цифрових відбитків, було показано, що значна частина відбитків вебоглядача має унікальний характер, а у масштабному аналізі Нампоїни Андріаміланто та співавторів понад 4,1 млн відбитків із 216 атрибутів продемонстрували високу розрізнюваність і стабільність у часі: понад 81% відбитків у часових вибірках належали лише одному вебоглядачу, а більшість атрибутів залишалася незмінною навіть через місяці [2; 3]. Узагальнюючи наведені результати, можна стверджувати, що цифровий відбиток не є абсолютним «паспортом» пристрою, проте у поєднанні з IP-діапазоном, поведінкою користувача, сталими циклами активності, вмістом файлів cookie або акаунтами може бути вагомим чинником для ймовірнісної кореляції сеансів. З позиції ОСІНТ цього достатньо: якщо противник здатен пов'язати розділені акаунти, сеанси або легенди – сегментація діяльності втрачає надійність.

Отже, цифровий відбиток профілю вебоглядача не обмежується лише базовими параметрами, адже сучасні технології відстеження дають змогу фіксувати особливості відтворення графіки й звуку, роботи драйверів, набору шрифтів та програмного середовища загалом [1]. Тому проста зміна рядка ідентифікації вебоглядача або використання приватного режиму не забезпечує достатнього рівня захисту. Науково обґрунтовані підходи до мінімізації цифрового відбитку можна звести до двох стратегій. Перша полягає у зміні, нормалізації, додаванні шуму або блокуванні окремих параметрів: наприклад, зашумленні Canvas, повідомленні стандартної часової зони, обмеженні шрифтів, зменшенні точності таймерів або блокуванні WebGL. За такою логікою працює Resist Fingerprinting у Firefox та похідних рішеннях [5]. Його перевага – баланс між приватністю і сумісністю з вебсайтами; недолік – ризик аномальної унікальності, коли надмірні ручні зміни, розширення або винятки самі стають демаскуючою ознакою. Проект LibreWolf є прикладом такого підходу: він вмикає RFP, використовує uBlock Origin, захист cookie, вимикає телеметрію і WebGL, тому його доцільно використовувати коли завдання вимагає тривалої та стабільної роботи з інтернет-ресурсами, а ризик активного контр-ОСІНТ є помірним [6].

Друга стратегія – маскування у множині схожих користувачів. Її суть полягає не в тому, щоб щоразу виглядати інакше, а навпаки – бути максимально схожим на інших користувачів того самого захищеного вебоглядача. Такий підхід характерний для Tor Browser і Mullvad Browser: вони стандартизують значну частину параметрів, обмежують варіативність шрифтів, мови, розміру вікна, доступу до графічних функцій та інших сигнатур [1; 7]. В свою чергу Mullvad Browser призначений для роботи з VPN або без нього, а не через мережу Tor. Його головна перевага для ОСІНТ полягає у тому, що користувачеві не потрібно самостійно збирати «ідеальну» конфігурацію: правильна стратегія зазвичай полягає у збереженні стандартних налаштувань. Основний недолік – менша гнучкість і потенційна впізнаваність самого класу інструмента: сайт може не відрізнити одного користувача Mullvad Browser від іншого, але може зрозуміти, що перед ним вебоглядач, орієнтований на приватність. Для деяких ресурсів це не має значення, а для систем виявлення автоматизованої поведінки або протидії шахрайству може впливати на доступність сервісу, появу капчі чи підозрілість сеансу.

Тому вибір між підходами має визначатися не абстрактним рейтингом вебоглядачів, а моделлю загроз. Для повсякденної роботи ОСІНТ-аналітика –перегляду великої кількості відкритих джерел, читання медіа, перевірки посилань, роботи з неворожими платформами або виконання завдань, де важлива сумісність, доцільно використовувати посилено налаштований вебоглядач, наприклад LibreWolf або Firefox із RFP та розширеним захистом від стеження, за умови, що користувач не перетворює його на унікальний набір розширень. Для коротких або середніх сеансів на сумнівних ресурсах, де головна мета не виділитися технічно і не накопичувати міжсеансовий стан – доцільнішим є використання Mullvad Browser у стандартній конфігурації, бажано з окремим мережевим профілем і без додаткового налаштування. Для найризикованіших сценаріїв, де потрібно приховати не лише браузерний профіль, а й мережеву адресу та маршрут доступу, логічним вибором є Tor Browser, однак із розумінням його операційної ціни: Тор-трафік часто може бути впізнаний, заблокований або позначений як підстава для додаткових перевірок, а сам факт використання Тор у певному контексті може виступати окремою демаскуючою ознакою.

Отже, мінімізація цифрового відбитку вебглядача не є прагненням до абсолютної невидимості. Її реальна мета – зменшити кількість стабільних і взаємопов’язаних технічних сигнатур, за якими противник може корелювати сеанси, ролі й легенди. Практично це означає управління ризиками деанонізації через сегментацію середовищ, окремі профілі або вебглядачі для різних завдань, відмову від зайвих розширень, збереження стандартних параметрів, контроль витоків WebRTC та IP-адреси і регулярну перевірку цифрового відбитку після оновлень. Під час роботи з ворожими, зокрема російськими та китайськими, сумнівними або спеціально контрольованими ресурсами пріоритет має переходити до маскуванню у множині схожих користувачів, ізоляції середовища та мінімізації персональної варіативності.

### Список використаних джерел

1. Browser fingerprinting: a survey / P. Laperdrix та ін. *ACM Transactions on the Web*. 2020. Т. 14. № 2. 8. URL: <https://dl.acm.org/doi/10.1145/3386040> (дата звернення: 28.04.2026);
2. Eckersley P. How unique is your web browser? *Privacy Enhancing Technologies : PETS 2010* / ed. M. J. Atallah, N. J. Hopper. Berlin ; Heidelberg : Springer, 2010. Vol. 6205. P. 1–18. (Lecture Notes in Computer Science). DOI: [https://doi.org/10.1007/978-3-642-14527-8\\_1](https://doi.org/10.1007/978-3-642-14527-8_1) (дата звернення: 28.04.2026);
3. A large-scale empirical analysis of browser fingerprints properties for web authentication / N. Andriamilanto та ін. *ACM transactions on the web*. 2021. Т. 16, № 1. С. 1–62. URL: <https://doi.org/10.1145/3478026> (дата звернення: 28.04.2026).
4. Mitigating browser fingerprinting in web specifications. *World Wide Web Consortium*. URL: <https://www.w3.org/TR/fingerprinting-guidance/> (дата звернення: 28.04.2026).
5. Resist fingerprinting. *Mozilla Support*. URL: <https://support.mozilla.org/en-US/kb/resist-fingerprinting> (дата звернення: 28.04.2026).
6. Features. *LibreWolf Docs*. URL: <https://librewolf.net/docs/features/> (дата звернення: 28.04.2026).
7. The Mullvad Browser hard facts: list of settings and modifications. *Mullvad Browser*. URL: <https://mullvad.net/en/browser/hard-facts> (дата звернення: 28.04.2026).

**Кіреєва О. С.,**  
доцент кафедри спеціальних дисциплін,  
кандидат психологічних наук, доцент  
*(Національна академія Державної прикордонної  
служби України імені Богдана Хмельницького)*

## **ТРАНСФОРМАЦІЯ OSINT-ДОСЛІДЖЕНЬ У ПАРАДИГМІ INTELLIGENCE-LED POLICING ДЛЯ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ**

Специфіка безпекового середовища прикордонного відомства вимагає не лише моніторингу глобальних кіберзагроз, а й постійного аналізу локальних диверсійних мереж та міграційних потоків, що мають ознаки керованого інформаційно-психологічного впливу. Традиційні реактивні підходи до збору інформації в умовах повномасштабної агресії втрачають актуальність, оскільки ворог використовує прикордонні зони як полігон для випробування нових методів гібридної війни. У цьому контексті OSINT (Open Source Intelligence) поступово трансформується з допоміжного технічного інструменту на автономну стратегічну спроможність аналітичного забезпечення, що дозволяє формувати цілісну картину безпекової ситуації через синтез великих масивів даних [1].

Концептуальна зміна моделей правоохоронної діяльності та перехід до Intelligence-led Policing (ILP) означає фундаментальний відхід від простого реагування на правопорушення до проактивного управління ризиками, що ґрунтується на випереджальній аналітичній розвідці та точному прогнозуванні. В межах цієї парадигми інформація перестає бути пасивним ресурсом і стає фундаментом для прийняття управлінських рішень, що обумовлює нагальну потребу повної інтеграції OSINT у систему кримінального аналізу та стратегічного управління національною безпекою.

Тому OSINT доцільно розглядати не просто як екосистему, а як інтелектуальний інструментарій, що формує принципово нову логіку реагування на асиметричні виклики. Концепція ILP при цьому виступає як управлінська філософія, що забезпечує трансформацію сирих даних у конкретну правоохоронну політику, орієнтовану на превенцію та раціональний розподіл ресурсів [2]. Вибір методологічного апарату обумовлений потребою комплексного бачення проблеми: системний метод дозволяє нам ідентифікувати OSINT як невід'ємну ланку державної аналітичної інфраструктури, тоді як структурно-функціональний аналіз дає змогу чітко розмежувати ролі підрозділів у моделі ILP, забезпечуючи перехід від накопичення даних до їхньої глибокої інтерпретації як ключового показника якості. Важливим елементом є впровадження концепції «OSINT як повного аналітичного циклу», що передбачає неперервний шлях від визначення потреб замовника до фінальної підтримки прийняття рішень, де головним ознакою якості є не обсяг накопиченої інформації, а глибина її інтерпретації.

У парадигмі ILP дослідження відкритих джерел виконують комплекс взаємопов'язаних функцій, серед яких інформаційна забезпечує доступ до цифрового сліду в соціальних мережах, державних реєстрах та Deep Web, а аналітична - дозволяє формувати достовірні висновки на основі верифікації та синтезу цих даних. Прогностична функція стає ключовою для виявлення латентних закономірностей розвитку загроз, тоді як управлінська - створює умови для точного спрямування зусиль правоохоронних органів на стратегічному та тактичному рівнях. Ефективність такої діяльності впирається у необхідність

реалізації принципу «need to share», який, попри свою теоретичну довершеність, на практиці часто гальмується «відомчим парканізмом» та застарілими протоколами доступу до даних. Подолання цієї психологічної та інституційної ізоляції є критичною умовою для успішного функціонування системи кримінального аналізу.

Трансформація OSINT у структурі ІЛР має системний багаторівневий характер, що на інституційному рівні виявляється у створенні спеціалізованих центрів кримінального аналізу та оновлення нормативної бази, здатної легалізувати цифрові докази [3].

Для чіткої систематизації цих процесів доцільно виокремити ключові вектори інтеграції, які представлені у таблиці 1.

*Таблиця 1*

### **Рівні інтеграції OSINT у парадигму ІЛР**

<b>Рівень трансформації</b>	<b>Ключовий фокус</b>	<b>Результат для системи ІЛР</b>
<b>Інституційний</b>	Створення аналітичних центрів, нормативне врегулювання	Легалізація цифрових доказів та формування єдиного аналітичного поля.
<b>Технологічний</b>	Використання Big Data, ІІІ, графового аналізу	Здатність деанонімізувати об'єкти та виявляти закономірності в Dark Web.
<b>Процесуальний</b>	Стандартизація процедур збору даних	Забезпечення цілісності ланцюга передачі доказів та доказової бази.
<b>Аналітичний</b>	Побудова динамічних моделей загроз	Проактивне управління ризиками та точне прогнозування.

Представлена матриця інтеграції дозволяє констатувати, що успішність переходу до парадигми ІЛР залежить не від окремих технологічних рішень, а від синхронності розвитку всіх зазначених рівнів, де аналітичний компонент виступає інтегруючим чинником.

Практичне значення OSINT для національної безпеки України набуває особливої гостроти в умовах воєнного стану, оскільки дозволяє не лише документувати воєнні злочини та ідентифікувати комбатантів, а й ефективно виявляти диверсійні мережі, аналізувати ворожі інформаційні кампанії та здійснювати моніторинг обходу санкцій. Зокрема, впровадження інноваційних технологій у діяльність аналітиків прикордонного відомства стає вирішальним інструментом для викриття латентних проявів колабораційної діяльності, де цифрові сліди у прикордонних зонах формують доказову базу для викриття протиправних зв'язків. Таким чином, інтеграція OSINT-технологій у кримінальний аналіз дозволяє перевести розслідування злочинів проти основ національної безпеки на якісно новий рівень, забезпечуючи випереджальну протидію ворожим впливам [4].

Головною перевагою OSINT залишається його висока оперативність та здатність адаптуватися до змін безпекового середовища швидше за традиційні методи розвідки. Водночас повноцінна інтеграція OSINT у систему ІЛР стикається з викликами, такими як відсутність єдиних методологічних стандартів, складність легального обміну даними та дефіцит аналітиків зі специфічними компетенціями.

Вирішення виявлених проблем, зокрема дефіциту аналітиків із вузькоспеціалізованими компетенціями, вбачається у впровадженні нових освітніх стандартів, які розробляються на базі Національної академії Державної прикордонної служби України. Це дозволить виховати нову генерацію аналітиків, здатних оперувати як відкритими, так і конфіденційними джерелами у єдиному аналітичному полі.

### **Список використаних джерел**

1. OSINT Open Source Intelligence. Теорія та методологія: монографія / О. Користін, С. Демедюк, О. Барановський, Д. Ланде та ін. ; за заг. ред. О. Є. Користіна, С. В. Демедюка. Київ : 7БЦ, 2025. 304 с.
2. Реалізація філософії «Intelligence-led Policing» в системі кримінального аналізу Національної поліції України: О. Користін, Д. Швець, Б. Бутко, Б. Денисенко та ін. ; за заг. ред. О. Є. Користіна. Київ : ВАІТЕ, 2024. 444 с.
3. OSINT Open Source Intelligence. Інструменти та методи: навч. посіб. / О. Користін, С. Демедюк, К. Ісмайлов, Д. Ланде та ін. ; за заг. ред. О. Є. Користіна, С. В. Демедюка. Київ : 7БЦ, 2025. 460 с.
4. Кіреєва О. С. Використання кримінальними аналітиками інноваційних технологій для виявлення проявів колабораційної діяльності. *Успіхи і досягнення у науці (Серія «Право»)*. 2024. № 3 (3). С. 46–58.

**Кісіль З. Р.,**

заступник директора навчально-наукового інституту управління, психології та безпеки, доктор юридичних наук, професор, заслужений діяч науки і техніки України  
(Львівський державний університет внутрішніх справ)

## **ІНСТРУМЕНТАРІЙ OSINT ЯК ЧИННИК ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ОПЕРАТИВНО-СЛУЖБОВОЇ ДІЯЛЬНОСТІ ПОЛІЦІЇ**

Сучасна парадигма правоохоронної діяльності в умовах глобальної цифровізації вимагає від оперативних підрозділів Національної поліції України впровадження новітніх інструментів збору та аналізу даних, серед яких особливе місце дає розвідку на основі відкритих джерел (Open Source Intelligence – OSINT). Перспективи застосування інформації, отриманої шляхом із соціальних мереж та відкритих сегментів мережі Інтернет, в оперативних цілях є надзвичайно широкими, що зумовлено трансформацією злочинності та її переходом у кіберпростір. Існує низка продуктивних алгоритмів збору й аналітики цієї інформації, які необхідно інтегрувати в повсюдну практику працівників поліції. Для ефективного реалізації завдань, поставлених перед оперативними підрозділами, необ'єктивна потреба не лише в підвищеному рівні комп'ютерної грамотності діючих співробітників та вдосконаленні тактики одержання інформації, а й у створеному спеціалізованому програмному забезпеченні. Такий інструментарій повинен дозволити проводити глибокий аналіз даних шляхом їх агрегації з наявними оперативними базами органів внутрішніх справ, що забезпечує комплексний підхід до інсталюваної об'єктивної істини.

Концептуально OSINT збільшується як сукупність заходів із пошуку, вибору та збору розвідувальної інформації з офіційно доступних джерел з її подальшим аналізом для прийняття управлінських чи тактичних рішень. Теоретичні підмурівки OSINT базуються на двох фундаментальних поняттях: відкритому джерелі та загальнодоступній інформації. Ефективність планування та ведення такої розвідки залежить від низки факторів, серед яких чисельне місце дає релевантність даних, їх доступність, обсяг, якість та ясність. Важливою перевагою методів OSINT є легкість використання та мінімальна вартість із традиційними методами агентурної розвідки чи застосуванням складних технічних засобів негласного зняття інформації. Досвід західних демократій демонструє високу ефективність спеціалізованих структур, таких як 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.

Правова регламентація застосування методів OSINT в Україні спирається на засади законності та утримання прав людини. відповідно до статті 34 Конституції України кожен має право вільно збирати, зберігати та використовувати інформацію у будь-який спосіб на власний розсуд, що створює первинну правову базу для збору даних із відкритих джерел. Разом із тим, застосування OSINT-інструментарію в межах правоохоронної діяльності вимагає неухильного дотримання норм кримінального процесуального законодавства. Аналіз відкритих даних часто межує з процедурами, передбаченими главою 21 Кримінального процесуального кодексу України, зокрема в частині зняття інформації з електронних інформаційних систем. Слід пам'ятати, що відповідно до частини 3 статті 214 КПК України

проведення слідчих дій до внесення відомостей до ЄРДР не допускається (крім огляду місця події). Крім того, Закон України «Про оперативно-розшукову діяльність» встановлює чіткі межі проведення заходів лише після відкриття відповідної оперативно-розшукової справи. Це зумовлює повністю чіткої верифікації кожного етапу збору інформації для забезпечення її допустимості як доказу в суді.

Для забезпечення об'єктивності та легітимності використання OSINT у діяльності поліції необхідно диференціювати одержання інформації на загально-правові, що стосуються принципів усіх суб'єктів суспільних відносин, та інформування, характерні для суб'єктів оперативно-розшукової діяльності. В європейській поліцейській практиці OSINT розглядається як невід'ємний елемент стандартних операційних процедур. Сучасні програмно-технологічні рішення дозволяють автоматизувати збір даних із соціальних мереж (Facebook, Twitter/X, YouTube, Instagram), проводити інтелектуальний аналіз тексту, оцінювати достовірність та проводити моніторинг ідентичності користувачів. Надається можливість роботи з геоданими в особливій вазі, що дозволяє реконструювати маршрути пересування осіб та встановлювати місця їх фактичного перебування. Крім того, професійний OSINT передбачає роботу з «невидимим вебом» – Dark Web та Deep Web, де часто міститься інформація про протиправну діяльність, торгівлю нелегальними товарами або координацію злочинних угруповань.

Аналітичний потенціал відкритих джерел є надзвичайно потужним, оскільки вони охоплюють значні масиви даних, необхідні для розуміння як об'єктивних ознак вчинення правопорушення, так і суб'єктивних характеристик особи злочинця. Найбільша ефективність досягається при комплексному використанні відкритої інформації з конфіденційними даними, отриманими з оперативних джерел. Застосовуючи ці методи, поліцейські підрозділи забезпечують можливість оперативно ідентифікувати делінквенту за випадковими фотографіями в мережі, встановлювати коло його зв'язків, професійні інтереси, політичне уподобання та активність до вчинення певних видів злочинів. Переваги такого підходу полягають у вільних потребах у значних фінансових вливаннях та можливості діяти дистанційно, що мінімізує ризики для співробітників поліції.

Розвиток технологій штучного інтелекту та машинного навчання відкриває нові горизонти для OSINT, дозволяючи автоматично розпізнавати обличчя на великих масивах відеоданих, аналізувати тональність повідомлень у месенджерах та виявляти аномалії в поведінці користувачів, які можуть свідчити про підготовку до вчинення злочину. Водночас це ставить перед правоохоронною системою виклики щодо захисту персональних даних та дотримання етичних стандартів. Впровадження OSINT-технологій у діяльність Національної поліції України має супроводжуватися створенням відповідних методичних рекомендацій та навчальних програм для підготовки фахівців-аналітиків. У підсумку, інтеграція методів розвідки на основі відкритих джерел у практику оперативних підрозділів є стратегічним кроком, що сприяє модернізації правоохоронної системи, посиленню протидії злочинності та забезпеченню безпечного середовища для громадян у цифровому просторі, що є запорукою стійкості держави в умовах сучасних гібридних загроз.

**Кісіль Р.-В. В.,**  
науковий співробітник  
науково-дослідної лабораторії OSINT-досліджень  
та безпекової аналітики навчально-наукового  
інституту управління, психології та безпеки, кандидат юридичних наук  
*(Львівський державний університет внутрішніх справ)*

## **СТРАТЕГІЧНІ ТА ПРИКЛАДНІ АСПЕКТИ ЗАСТОСУВАННЯ ІНСТРУМЕНТАРІЮ OSINT У ПРОЦЕСУАЛЬНІЙ ДІЯЛЬНОСТІ НА ЕТАПІ ДОСУДОВОГО РОЗСЛІДУВАННЯ**

Трансформація сучасного злочинного середовища та перехід значної частини соціальних комунікацій у цифровий простір зумовлюють об'єктивну необхідність перегляду традиційних підходів до збирання доказової бази у кримінальному провадженні. В умовах інформаційного суспільства Open Source Intelligence (OSINT) – розвідка на основі відкритих джерел – перетворюється з допоміжного аналітичного методу на базовий елемент стратегії досудового розслідування. Поширення концепції «цифрового сліду» особистості дозволяє правоохоронним органам отримувати критично важливу інформацію без безпосереднього фізичного контакту з об'єктом, що мінімізує ризик розголошення таємниці слідства та забезпечує високу оперативність дій. Ефективність OSINT у межах кримінального процесу базується на принципі інформаційної надмірності сучасних мереж, де громадяни добровільно оприлюднюють масиви персональних даних: анкетні відомості, біографічні факти, відомості про коло спілкування та матеріальний стан. З погляду криміналістики, такі дані є об'єктивною реальністю, зафіксованою у цифровому форматі, що може бути використана для ідентифікації особи за антропометричними ознаками зовнішності та поведінковими патернами. Аналітична розвідка на етапі досудового розслідування класифікується за джерелами походження інформації, охоплюючи загальний моніторинг інтернет-ресурсів, роботу з автоматизованими банками даних різних форм власності та вивчення медіа-дискурсу як засобу фіксації подій.

Соціальні платформи, такі як Facebook, Instagram та LinkedIn, виступають основними донорами інформації про суб'єкта, дозволяючи слідчим органам здійснювати моніторинг у реальному часі. Це є критичним для запобігання злочинам, які лише готуються, або для оперативної атрибуції вчинених правопорушень. Зокрема, аналіз публічного профілю в Instagram дає змогу реконструювати щоденний графік особи, встановити місця її постійного перебування через геопозиціонування та ідентифікувати найближче коло зв'язків. Особливого значення набуває аналіз професійних мереж, що надають структуровану інформацію про кар'єрний шлях та корпоративні зв'язки, що стає фундаментальною базою для розслідування економічних злочинів та правопорушень у сфері інтелектуальної власності. Водночас, використання месенджерів та локальних територіальних чатів дозволяє отримувати первинні свідчення від очевидців у вигляді фото- та відеофіксації, що часто випереджає офіційні звіти та повідомлення про злочини.

Технологічний базис сучасного OSINT обґрунтовується на використанні складних пошукових алгоритмів та спеціалізованих сервісів реверсивного пошуку зображення. Центральне місце в цьому процесі займається біометричною ідентифікацією на основі нейронних мереж. Це статичний метод розпізнавання, що базується на унікальних геометричних характеристиках обличчя та форми черепа. Використання автоматизованих інструментів дозволяє здійснювати безконтактний пошук суб'єктів у глобальних масивах даних, встановлюючи особу з високим ступенем вірогідності. Програмне забезпечення нового покоління порівнює завантажені видимі матеріали з мільйонами зображень у відкритих джерелах, надаючи аналітичний звіт із показниками схожості, що значно прискорює процес встановлення особи оцінюваного. У науковій практиці виділяють декілька методів такого розпізнавання: автоматичну обробку контурів, статистичний аналіз піксельних масивів за методом «власних граней», аналіз ключових точок геометрії обличчя та нейромережевої моделі, яка демонструє високу точність навіть у складних умовах візуалізації.

Процес технічної реалізації OSINT-заходів вимагає підтримки суворих правил кібербезпеки та використання засобів криптографічного захисту трафіку, таких як VPN-сервіси, для доступу до географічно обмежених ресурсів або збереження слідчої активності. Системна інтеграція цих інструментів у ході досудового розслідування відкриває нові можливості для отримання доказової інформації без застосування обмежувальних заходів, які могли б значно порушити приватність. Це дозволяє лише встановити особу за випадковим кадром чи реконструювати маршрути пересування за допомогою метаданих, а й виявити закриті зв'язки між учасниками злочинних угруповань. Таким чином, розвиток OSINT-технологій у системі криміналістики є закономірним етапом модернізації правоохоронної діяльності, що забезпечує ефективне реагування на виклики цифрової епохи та гарантує невідворотність покарання за вчинені правопорушення через проактивний аналіз відкритого інформаційного середовища. Консолідація методологічних стандартів та технологічного потенціалу стає запорукою підвищення якості досудового розслідування та визнання інноваційної істини у кримінальних провадженнях будь-якої складності.

**Колесников М. Є.,**  
здобувач вищої освіти  
(Національний юридичний університет  
імені Ярослава Мудрого)

## **ВИЯВЛЕННЯ ОЗНАК ОБХОДУ САНКЦІЙ ІЗ ВИКОРИСТАННЯМ ВІРТУАЛЬНИХ АКТИВІВ ЗАСОБАМИ OSINT: ВІДКРИТІ ДЖЕРЕЛА ТА БЛОКЧЕЙН-ОГЛЯДАЧІ**

Повномасштабна агресія РФ проти України та запроваджені у відповідь обмежувальні заходи загострили проблематику використання віртуальних активів для обходу санкцій і переміщення коштів поза традиційними механізмами аудиту – фінансовим моніторингом, валютним наглядом, податковим контролем та державним фінансовим контролем. 24 лютого 2023 року FATF (*Financial Action Task Force*; з англ. – Група з розробки фінансових заходів з відмивання грошей) призупинила членство в організації для країни-агресора та закликала усі юрисдикції звернути увагу на ризики обходу заходів, запроваджених у зв'язку з війною проти України [1]. Проте відсутність РФ у «чорному списку» FATF досі дозволяє її резидентам використовувати прогалини в глобальному регулюванні віртуальних активів. Зокрема, у липні 2024 року зазначена структура констатувала, що значна частина юрисдикцій досі не забезпечила належного застосування стандартів щодо віртуальних активів і постачальників відповідних послуг, тоді як сам сектор і далі зберігає ризики відмивання коштів, фінансування тероризму та фінансування розповсюдження зброї масового знищення [2]. До того ж, 4 грудня 2024 року Міністерство фінансів США повідомило, що TGR Group (міжнародна мережа з відмивання коштів та обходу санкцій) активно використовує цифрові активи, зокрема стейблкоїни, в інтересах російських еліт [3].

Проблематика використання віртуальних активів для обходу санкцій зафіксована в офіційних міжнародних документах. Зокрема, у рекомендаціях FATF віртуальні активи прямо розглядаються в контексті санкцій та інших заходів примусового впливу [4, с. 4]. 25 березня 2024 року OFAC (*Office of Foreign Assets Control*; з англ. – Управління з контролю за іноземними активами) запровадило санкції проти російських компаній, які розробляли або надавали послуги у сфері віртуальних активів і сприяли потенційному обходу обмежувальних заходів [5]. Зокрема, компанія B-Crypto співпрацювала з підсанкційним Rosbank для здійснення транскордонних розрахунків із використанням віртуальних активів. Компанія ТООР (Tsentr Obrabotki Elektronnykh Platezhey), що діяла під комерційними найменуваннями «Netexchange» та «Netex24», забезпечувала цифрові платежі у рублях та з використанням віртуальних активів для підсанкційних Sberbank, Alfa-Bank і Hydra Market. Окрім використання популярних стейблкоїнів, підсанкційні суб'єкти РФ намагаються вибудувати власну тіньову інфраструктуру, наприклад, через створення підконтрольних криптобірж у лояльних юрисдикціях або розробку цифрових активів, прив'язаних до фіатних валют держави-агресора.

Наведені факти дають підстави визначити предмет OSINT-аналізу у контексті санкцій як сукупність зв'язків між фігурантами обмежувальних списків, афілійованими компаніями, платіжною інфраструктурою та повторюваними моделями транзакцій. З огляду на задокументовані випадки застосування віртуальних активів підсанкційними особами або підконтрольними їм структурами, розвідка з відкритих джерел набуває безпосереднього практичного значення. У центрі уваги перебувають цифрові сліди та організаційні зв'язки,

які вказують на використання криптоактивів підсанкційними юридичними особами або їхніми тіншовими посередниками.

У науковій літературі OSINT розглядається як пошук інформації у відкритих джерелах, її аналітичне опрацювання та подальше використання результатів такого аналізу [6]. Зазначений підхід є універсальним інструментом аналітичної перевірки та зіставлення відкритих даних. У контексті санкційного дослідження релевантними є такі категорії джерел: блокчейн-дані (історія транзакцій, адреси гаманців, сервісні адреси бірж і міксерів); санкційні списки (OFAC SDN List, EU Consolidated List, списки РНБО України); корпоративні реєстри та відомості про юрисдикції реєстрації; публічні повідомлення компаній і профільні медіа; сайти бірж і платіжних сервісів; повідомлення у соціальних мережах і месенджерах.

Практичним проявом даного підходу є дослідження випадків, коли цифрові активи використовуються для розрахунків в інтересах санкційних або пов'язаних із ними суб'єктів. Показовим є повідомлення Міністерства фінансів США про мережу TGR Group, у якому стейблкоїни фігурують як інструмент обходу обмежувальних заходів у поєднанні з посередниками, транснаціональними розрахунками та складною мережею пов'язаних суб'єктів [3].

Для OSINT-аналізу критично важливо встановити: хто саме використовує певний токен; через які платформи здійснюються операції; з якими компаніями або структурами ці платформи пов'язані; які повторювані транзакційні та корпоративні моделі простежуються. Відкриті публікації, повідомлення у месенджерах, сайти компаній, сторінки бірж або адреси гаманців у відкритому доступі є початковими точками такого дослідження. Самі по собі ці дані не доводять факту обходу санкцій, однак у поєднанні з іншими відкритими відомостями вони можуть вказувати на наявність зв'язків, релевантних для санкційного аналізу. Виявлення у відкритому джерелі адреси гаманця, згадки про стейблкоїн, цифровий сервіс або спосіб розрахунку може бути підставою для подальшої перевірки – аналізу історії транзакцій, кола контрагентів, сервісних адрес і повторюваних моделей переказів у блокчейн-оглядачах та інших відкритих ресурсах. Навіть за відсутності встановлення кінцевого адресата сукупність повторюваних моделей транзакцій може мати самостійне значення для виявлення потенційної схеми обходу санкцій.

Мінімально необхідний алгоритм виявлення ознак обходу санкцій із використанням віртуальних активів охоплює шість послідовних етапів. На першому етапі здійснюється встановлення підсанкційного суб'єкта – насамперед юридичної особи – або пов'язаної з ним структури. Другий етап передбачає збір відкритих даних про корпоративні зв'язки, юрисдикції реєстрації, контрагентів, цифрові активи, біржі та адреси гаманців. На третьому етапі ідентифікується віртуальний актив, блокчейн-мережа або сервіс, які фігурують у відкритих джерелах. Четвертий етап полягає в аналізі повторюваних моделей транзакцій у блокчейн-оглядачі. П'ятий етап – зіставлення отриманих блокчейн-даних із санкційними списками, корпоративними реєстрами, публічними повідомленнями та медійними матеріалами. Шостий етап – формулювання висновку про наявність/відсутність відкритих ознак можливої санкційної схеми.

У межах зазначеного підходу найбільше значення мають не окремі транзакції, а сукупність аналітичних індикаторів: повторюваність контрагентів, концентрація операцій у певні часові проміжки, зв'язок із сервісними або біржовими адресами, сталість використання тих самих платформ чи посередників, а також збіг повторюваних моделей транзакцій із відомостями про перебування суб'єкта у санкційних списках. Саме аналіз таких поведінкових

патернів за допомогою спеціалізованих аналітичних платформ (Chainalysis, Elliptic, Crystal Blockchain та ін.) дозволяє виявляти мережі обходу санкцій навіть за умови повної анонімності кінцевих бенефіціарів. Сукупність зазначених ознак дає підстави стверджувати про можливу інфраструктуру обходу санкцій, що потребує подальшої, більш глибокої перевірки.

Водночас межі OSINT-аналізу у сфері санкційного контролю за віртуальними активами мають бути чітко окреслені. Відкрита аналітика дозволяє виявляти зв'язки між суб'єктами, цифровими активами, сервісами та маршрутами руху коштів, проте не завжди забезпечує остаточне встановлення всіх учасників схеми або її кінцевих бенефіціарів. Використання сервісів-посередників (міксерів, кросчейн-мостів), багаторівневих корпоративних структур та іноземних юрисдикцій із непрозорим регулюванням може істотно ускладнювати інтерпретацію відкритих даних. Відповідно, OSINT у цій сфері є інструментом виявлення та аналітичної перевірки ознак, проте не самодостатнім способом остаточного встановлення всіх елементів схеми: результати такого аналізу потребують верифікації засобами фінансового моніторингу, слідчих дій або міждержавного правового співробітництва.

Отже, поєднання відкритих джерел і блокчейн-оглядачів дає змогу виявляти ознаки використання віртуальних активів у схемах обходу санкцій. Найбільшу аналітичну цінність зазначеного підходу становить зіставлення факту перебування суб'єкта у санкційних списках, його корпоративних зв'язків, доступної платіжної інфраструктури та повторюваних моделей транзакцій. Систематичне застосування запропонованого алгоритму дозволяє трансформувати розрізнені відкриті дані у структуровану аналітичну інформацію, придатну для подальшого використання як органами фінансового контролю, так і суб'єктами приватного сектору в рамках процедур комплаєнсу.

#### **Список використаних джерел**

1. FATF Statement on the Russian Federation. FATF. 24 February 2023. URL: <https://www.fatf-gafi.org/en/publications/Fatfgeneral/fatf-statement-russian-federation.html> (дата звернення: 30.04.2026).
2. Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs. FATF. 9 July 2024. URL: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html> (дата звернення: 30.04.2026).
3. Treasury Exposes Money Laundering Network Using Digital Assets to Evade Sanctions. U.S. Department of the Treasury. 4 December 2024. URL: <https://home.treasury.gov/news/press-releases/jy2735> (дата звернення: 30.04.2026).
4. FATF. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Paris : FATF, 2021. URL: <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf> (дата звернення: 30.04.2026).
5. Treasury Designates Russian Companies Supporting Sanctions Evasion Through Virtual Asset Services and Technology Procurement. U.S. Department of the Treasury. 25 March 2024. URL: <https://home.treasury.gov/news/press-releases/jy2204> (дата звернення: 30.04.2026).
6. Дикий О. В., Сидорчук В. В. Поняття OSINT та суміжні категорії. Юридичний науковий електронний журнал. 2024. № 9. С. 332–335. DOI: <https://doi.org/10.32782/2524-0374/2024-9/78>. URL: [https://lsej.org.ua/9\\_2024/80.pdf](https://lsej.org.ua/9_2024/80.pdf) (дата звернення: 30.04.2026).

**Коляда А. О.,**  
курсант 2 курсу ФПФКП НПУ  
Науковий керівник: **Прокопов С. О.,**  
старший викладач кафедри  
інформаційних технологій  
(Дніпровський державний університет  
внутрішніх справ)

## **ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ІДЕНТИФІКАЦІЇ ТА РОЗШУКУ ОСІБ В УМОВАХ ВОЄННОГО СТАНУ МЕТОДАМИ OSINT-ТЕХНОЛОГІЙ**

У межах навчального процесу курсанти Дніпровського державного університету внутрішніх справ були залучені до діяльності відділу кримінального аналізу Головного управління Національної поліції в Луганській області. Основним завданням було здійснення пошуку інформації щодо безвісти зниклих українських військовослужбовців із використанням відкритих джерел інформації з метою встановлення їх можливого статусу, зокрема перебування у полоні, загибелі, або іншого місцезнаходження.

Виконання зазначених завдань здійснювалося із застосуванням методів аналізу відкритих джерел інформації (OSINT), що передбачає роботу з різними типами інформаційних ресурсів, включаючи офіційні державні реєстри, міжнародні бази даних, іноземні інформаційні ресурси, соціальні мережі, новинні платформи, відеохостинги та Telegram-канали. Особливістю даної діяльності є необхідність обробки великого обсягу неструктурованої інформації, яка потребує систематизації, перевірки та аналітичної оцінки.

Важливим елементом виконання завдань був багатомовний пошук інформації. Зокрема, аналіз здійснювався українською, російською та англійською мовами, а також із використанням різних варіантів написання імені та прізвища особи, включаючи транслітерацію. Це дозволяло значно розширити інформаційне поле пошуку та підвищити ймовірність виявлення релевантних даних [1].

У процесі виконання поставлених завдань було встановлено, що традиційні методи пошуку інформації є недостатньо ефективними в умовах великого обсягу даних. У зв'язку з цим доцільним стало використання технологій штучного інтелекту як інструменту інформаційно-аналітичної діяльності.

Ключовим аспектом застосування штучного інтелекту у даному процесі є правильне формулювання запиту. У цьому контексті запит виступає не просто текстовим зверненням до системи, а фактично виконує функцію алгоритму, який визначає логіку роботи штучного інтелекту. Саме структура запиту визначає, які джерела будуть аналізуватися, яким чином здійснюватиметься пошук інформації та у якому вигляді буде сформовано результат. Для виконання завдань було сформовано наступний аналітичний запит (рис. 1):

Якщо тобі треба саме текст для вставки в курсову як відповідь шп, тоді можу далі оформити результат одразу в науковому стилі.

🗨️ 📄 📁 📧 📧 📧

Лунин Ігор Ярославович 18.11.1985 р.н.

Думал на протязі 175

Ось структурований результат за твоїм шаблоном.

#### 1) Знайдені згадки про особу

За запитом щодо Лунина Ігора Ярославовича, 18.11.1985 р. н. знайдено кілька збігів у відкритих джерелах. Найбільш змістовні згадки є на сторінці Книги пам'яті Шептицької міської ради та на сайті «Книга пам'яті полеглих за Україну». На сторінці Шептицької міської ради вказано, що це Лунин Ігор Ярославович (18.11.1985 — 05.05.2022).

#### 2) Можливі ознаки полону

У знайдених відкритих джерелах я не знайшов підтвержень, що йдеться про перебування в полоні. У доступних матеріалах, навпаки, особа фігурує як загиблий військовослужбовець, а не як полонений.

#### 3) Можливі ознаки загибелі

Є кілька незалежних збігів на користь того, що йдеться саме про загибель. Шептицька міська рада вказує дату смерті 05.05.2022. Сайт heroportal.ua уточнює, що Ігор Лунин загинув 5 травня 2022 року під час виконання бойового завдання у Рубіжному Луганської області поблизу заводу «Зоря», отримавши вогнепальне кульове поранення. Додатково у відкритих джерелах є згадки про посмертне нагородження орденом «За мужність» III ступеня.

#### 4) Можливі ознаки перебування у лікарні, евакуації або тимчасового зникнення зв'язку

У знайдених джерелах я не виявив ознак госпіталізації, евакуації чи тимчасової втрати зв'язку. Відкриті матеріали, які вдалося знайти, послідовно описують саме загибель, а не поранення з подальшим лікуванням чи статус «зник безвісти».

#### 5) Пов'язані особи, події, місця та підрозділи

Із відкритих джерел пов'язуються такі дані:

- місце походження — Червоноград / нині Шептицький район, Львівщина;
- дата народження — 18.11.1985;
- дата загибелі — 05.05.2022;
- місце загибелі — Рубіжне, Луганська область, поблизу заводу «Зоря». Водночас у знайдених мною джерелах підрозділ прямо не вказаний, тому цей елемент потребує окремої перевірки.

#### 6) Оцінка достовірності кожного знайденого джерела

- Шептицька міська рада — висока достовірність, бо це офіційний ресурс органу місцевого самоврядування.
- Книга пам'яті полеглих за Україну — середня/висока достовірність як меморіальний ресурс, корисний для підтвердження збігу ПІБ і дати, але бажано звертати з офіційними актами.
- heroportal.ua — середня достовірність; містить важливі біографічні й обставинні деталі, але краще підтвердити факти іншими надійніми джерелами чи звітами.

+ Спробуйте ChatGPT

ChatGPT можемо добувати особлив. Рекомендуємо перевіряти наявність інформації.

Рис. 1. Запит штучному інтелекту на пошук інформації.

Допоможи у пошуку інформації щодо безвісти зниклого військовослужбовця [ПІБ], [дата народження], з метою встановлення його можливого статусу: перебування у полоні, загибель або інше можливе місцезнаходження. Здійснюй аналіз виключно відкритих джерел інформації, включаючи офіційні українські реєстри, міжнародні бази даних, іноземні інформаційні ресурси, соціальні мережі, новинні публікації, відеохостинги, форуми та Telegram-канали. Виконуй пошук різними мовами: українською, російською та англійською, використовуючи можливі варіанти написання імені та прізвища, у тому числі транслітерацію. Аналізуй текстові, фото- та відеоматеріали, встановлюй можливі зв'язки та надавай результати у структурованому вигляді з оцінкою достовірності.

Застосування такого запиту дозволило забезпечити комплексний підхід до аналізу інформації. У процесі його виконання штучний інтелект здійснює послідовні етапи обробки даних. На першому етапі відбувається пошук інформації у різних джерелах із використанням заданих параметрів. На другому етапі здійснюється аналіз знайдених даних, включаючи текстові згадки, фото- та відеоматеріали. На третьому етапі відбувається встановлення зв'язків між окремими елементами інформації, що дозволяє сформуванню узагальненої інформаційної картини (рис.2):

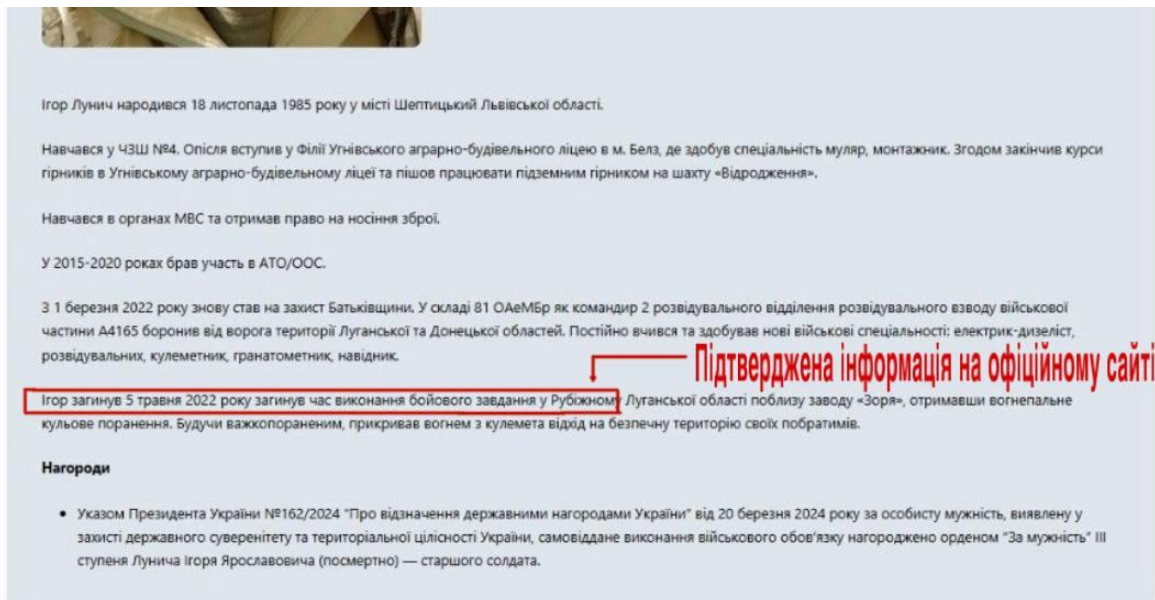


Рис. 2. Знайдена штучним інтелектом інформація відповідно запиту.

Результатом роботи штучного інтелекту є структурована інформація, яка включає можливі згадки про особу, ознаки перебування у полоні або загибелі, а також оцінку достовірності джерел [2]. Важливо зазначити, що отримані результати не є остаточними та потребують обов'язкової перевірки працівниками правоохоронних органів.

Таким чином, у процесі виконання завдань було встановлено, що штучний інтелект не є самостійним інструментом прийняття рішень, а виступає як допоміжний засіб інформаційно-аналітичної діяльності. Його ефективність безпосередньо залежить від правильності сформованого запиту, який фактично визначає алгоритм його роботи.

Узагальнюючи викладене, слід зазначити, що використання штучного інтелекту у поєднанні з правильно сформованими аналітичними запитом дозволяє значно підвищити ефективність пошуку та аналізу інформації у відкритих джерелах. Це особливо актуально в умовах воєнного стану, коли швидкість обробки інформації має критичне значення. Отже, штучний інтелект доцільно розглядати як ефективний інструмент правоохоронної діяльності, який набуває практичного значення лише за умови правильного визначення алгоритму його використання.

### Список використаних джерел

1. Гребенюк А. М., Прокопов С. О., Рибальченко Л. В. Використання технологій розпізнавання обличчя на відео- та фотозображеннях : метод. рекомендації. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2023. 48 с.

URI: [https://er.dduvs.edu.ua/bitstream/123456789/13273/5/%D0%BC%D0%B0%D0%BA%D0%B5%D1%82\\_%D1%80%D0%BE%D0%B7%D0%BF%D1%96%D0%B7%D0%BD%D0%B0%D0%B2\\_%D0%B2%D1%96%D0%B4%D0%B5%D0%BE\\_%D0%9C%D0%B5%D1%82%D0%BE%D0%B4.%20%D1%80%D0%B5%D0%BA%D0%BE%D0%BC%D0%B5%D0%BD%D0%B4.pdf](https://er.dduvs.edu.ua/bitstream/123456789/13273/5/%D0%BC%D0%B0%D0%BA%D0%B5%D1%82_%D1%80%D0%BE%D0%B7%D0%BF%D1%96%D0%B7%D0%BD%D0%B0%D0%B2_%D0%B2%D1%96%D0%B4%D0%B5%D0%BE_%D0%9C%D0%B5%D1%82%D0%BE%D0%B4.%20%D1%80%D0%B5%D0%BA%D0%BE%D0%BC%D0%B5%D0%BD%D0%B4.pdf)

2. Чат GPT.

URL: [https://chatgpt.com/?utm\\_source=google&utm\\_medium=paid\\_search&utm\\_campaign=G\\_OOG\\_C\\_SEM\\_GBR\\_Core\\_CHT\\_BAU\\_ACQ\\_PER\\_MIX\\_ALL\\_EMEA\\_UA\\_UK\\_050825&c\\_id=22525797771&c\\_agid=181335141493&c\\_crid=788442738636&c\\_kwid=kwd-1927051708782&c\\_ims=&c\\_pms=9197775&c\\_nw=g&c\\_dvc=c&gad\\_source=1&gad\\_campaignid=22525797771&gclid=CjwKCAjwteHPBhADEiWAWo3sJstcXPIB8ZZ7mdC\\_cbo2I\\_\\_1PdyXsh-GNdZQga\\_5--okHV5kzBkZxoCEN8QAvD\\_BwE](https://chatgpt.com/?utm_source=google&utm_medium=paid_search&utm_campaign=G_OOG_C_SEM_GBR_Core_CHT_BAU_ACQ_PER_MIX_ALL_EMEA_UA_UK_050825&c_id=22525797771&c_agid=181335141493&c_crid=788442738636&c_kwid=kwd-1927051708782&c_ims=&c_pms=9197775&c_nw=g&c_dvc=c&gad_source=1&gad_campaignid=22525797771&gclid=CjwKCAjwteHPBhADEiWAWo3sJstcXPIB8ZZ7mdC_cbo2I__1PdyXsh-GNdZQga_5--okHV5kzBkZxoCEN8QAvD_BwE)

**Копитко М. І.,**  
завідувач кафедри  
менеджменту та економічної безпеки,  
доктор економічних наук, професор  
(Львівський державний університет внутрішніх справ)

**Мойса Т. В.,**  
старший викладач кафедри  
менеджменту та економічної безпеки  
(Львівський державний університет внутрішніх справ)

## **OSINT-ДОСЛІДЖЕННЯ У СИСТЕМІ КОМПЛАЄНС-КОНТРОЛЮ НА ПІДПРИЄМСТВАХ**

Актуальність теми обумовлена посиленням ролі комплаєнс-контролю в умовах цифрової трансформації економіки, глобалізації бізнес-середовища та інтеграції України до європейського економічного простору. Сучасні підприємства функціонують у складному та динамічному середовищі, яке характеризується високим рівнем невизначеності, інформаційною асиметрією, зростанням кіберзагроз, а також посиленням регуляторного тиску. У таких умовах зростає потреба у використанні інноваційних інструментів забезпечення прозорості, доброчесності та відповідності діяльності підприємств встановленим нормам і стандартам. Одним із таких інструментів є OSINT-дослідження (Open Source Intelligence), які набувають все більшого поширення у системах комплаєнс-контролю.

OSINT-дослідження являють собою процес системного збору, обробки, аналізу та інтерпретації інформації з відкритих джерел. До таких джерел належать державні реєстри, офіційні бази даних, судові рішення, інформаційні портали, засоби масової інформації, соціальні мережі, корпоративні вебсайти, аналітичні платформи та інші публічні ресурси. Важливою перевагою OSINT є легальність отримання інформації, її доступність та можливість швидкої актуалізації, що робить цей інструмент особливо ефективним у сфері комплаєнсу [1].

Метою дослідження є обґрунтування теоретико-прикладних засад використання OSINT-досліджень у системі комплаєнс-контролю підприємств, визначення їх функціональних можливостей, а також оцінка впливу на рівень економічної безпеки та ефективність управління ризиками.

У системі комплаєнс-контролю ключовими завданнями є забезпечення дотримання законодавства, внутрішніх політик і процедур, а також запобігання порушенням, що можуть призвести до фінансових втрат або репутаційних ризиків. Використання OSINT дозволяє значно підвищити якість виконання цих завдань шляхом розширення інформаційної бази для аналізу. Зокрема, OSINT-дослідження забезпечують:

- проведення комплексної перевірки контрагентів (due diligence) перед укладанням угод;
- виявлення кінцевих бенефіціарних власників та аналіз корпоративної структури;
- ідентифікацію афілійованих осіб і компаній, що можуть становити конфлікт інтересів;
- моніторинг репутаційних ризиків шляхом аналізу інформаційного поля;
- виявлення фактів участі суб'єктів господарювання у судових спорах, фінансових махінаціях або корупційних правопорушеннях;
- перевірку відповідності діяльності підприємства вимогам законодавства та міжнародних стандартів [2].

Особливого значення OSINT набуває в умовах євроінтеграції, коли українські підприємства змушені адаптуватися до стандартів ЄС у сфері комплаєнсу, антикорупційної політики, боротьби з відмиванням коштів (AML) та фінансуванням тероризму (CFT) [3]. Європейська практика передбачає впровадження комплексних систем контролю, що базуються на принципах прозорості, підзвітності та належної перевірки партнерів. У цьому контексті OSINT виступає як ефективний інструмент забезпечення відповідності таким вимогам.

Інтеграція OSINT у систему комплаєнс-контролю підприємства потребує формування відповідної організаційної інфраструктури. Це включає створення спеціалізованих підрозділів або визначення відповідальних осіб, розроблення внутрішніх регламентів, політик і процедур, а також впровадження сучасних інформаційно-аналітичних систем. Важливим є також забезпечення взаємодії між підрозділами комплаєнсу, внутрішнього аудиту, безпеки та управління ризиками.

Суттєвим аспектом є використання сучасних цифрових технологій для автоматизації OSINT-досліджень. Йдеться про застосування спеціалізованого програмного забезпечення, алгоритмів обробки великих даних (Big Data), машинного навчання та штучного інтелекту [4]. Це дозволяє значно підвищити швидкість і точність аналізу, а також виявляти приховані закономірності та ризики, які неможливо ідентифікувати традиційними методами.

Водночас використання OSINT супроводжується низкою викликів. По-перше, це проблема перевірки достовірності інформації, оскільки відкриті джерела можуть містити неповні або викривлені дані. По-друге, важливим є дотримання правових та етичних норм, зокрема щодо захисту персональних даних та конфіденційної інформації. По-третє, ефективне використання OSINT потребує високого рівня професійної підготовки фахівців, які володіють навичками аналітичного мислення, критичного оцінювання інформації та роботи з цифровими інструментами.

З метою підвищення ефективності використання OSINT у системі комплаєнс-контролю доцільно реалізувати комплекс заходів, серед яких:

- розроблення методичних рекомендацій щодо проведення OSINT-досліджень;
- стандартизація процедур збору та аналізу інформації;
- впровадження систем навчання та підвищення кваліфікації персоналу;
- інтеграція OSINT з іншими інструментами управління ризиками та внутрішнього контролю;
- використання міжнародного досвіду та кращих практик у сфері комплаєнсу [5].

Крім того, важливо враховувати галузеву специфіку підприємств, оскільки рівень ризиків, характер інформаційних потоків та вимоги до комплаєнсу можуть суттєво відрізнятися залежно від сфери діяльності. Наприклад, у фінансовому секторі особлива увага приділяється перевірці клієнтів і транзакцій, тоді як у сфері ІТ-захисту даних і кібербезпеці.

Таким чином, OSINT-дослідження є важливим інструментом підвищення ефективності комплаєнс-контролю на підприємствах. Їх використання сприяє своєчасному виявленню ризиків, забезпеченню прозорості бізнес-процесів, зміцненню репутації підприємства та підвищенню довіри з боку партнерів, інвесторів і регуляторних органів. У сучасних умовах вони стають невід'ємною складовою системи економічної безпеки підприємств.

### Список використаних джерел

1. Кобелєва Т. О. Дослідження взаємозв'язку комплаєнс-контролю з внутрішнім аудитом та внутрішнім контролем на промисловому підприємстві. *Наукові праці Донецького національного технічного університету. Серія: Економічна*. Покровськ: ДонНТУ, 2019. № 2 (21). С. 81–91. [http://doi.org/10.31474/1680-0044-2019-2\(21\)-81-91](http://doi.org/10.31474/1680-0044-2019-2(21)-81-91)
2. Копитко М. І., Шевченко Н. В. Корпоративна культура і комплаєнс-контроль як елементи корпоративного управління та економічної безпеки українських акціонерних товариств в умовах євроінтеграції. *Вчені записки Університету «КРОК»*. 2026. № 1. С. 200–208. URL: <https://doi.org/10.31732/2663-2209-2026-81-200-208>
3. Пальцун І. М. Compliance-політика як складова корпоративної культури підприємства. *Торгівля і ринок України*. 2013. Вип. 35. С. 134–141.
4. Ревак І. О., Підхомний О. М. Відкриті джерела інформації в управлінні корпоративним санкційним комплаєнсом логістичних підприємств. *Науковий вісник Львівського державного університету внутрішніх справ. Серія економічна*. 2025. № 2. С. 48–54. DOI: <https://doi.org/10.32782/2311-844X/2025-2-6>
5. Копитко М. І., Вінчук М. В. Комплаєнс-контроль у системі публічного управління та контролінгу безпеки підприємств критичної інфраструктури. *Вісник Львівського державного університету внутрішніх справ. Серія економічна*. 2025. № 2. С. 3–11. DOI: <https://doi.org/10.32782/2311-844X/2025-2-1>

**Косяченко Є. О.,**  
здобувач вищої освіти  
*(Дніпровський державний університет внутрішніх справ)*  
Науковий керівник: **Рижков Е. В.,**  
професор кафедри інформаційних технологій,  
кандидат юридичних наук, професор  
*(Дніпровський державний університет внутрішніх справ)*

## **АНАЛІТИЧНА ПІДТРИМКА ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ У СФЕРІ ПРОТИДІЇ ОРГАНІЗОВАНИЙ ЗЛОЧИННОСТІ ПІД ЧАС ВОЄННОГО СТАНУ**

Аналіз ситуації зі злочинністю за період 2022–2025 років показує, що кримінальні угруповання сильно змінилися. Повномасштабне вторгнення спочатку призвело до розпаду та розпорошення звичних банд. Частина злочинців була змушена перенести свою діяльність за кордон або в більш безпечні області України. Проте вже у 2023 році злочинці знову активізувалися. Їх стало менше, але вони змінили підходи до вчинення злочинів та стали діяти значно хитріше [1].

Сучасні організовані злочинні групи дедалі частіше відмовляються від старої суворой підпорядкованості (де головними були «злодії в законі» чи «авторитети»). Тепер вони працюють як гнучкі мережі, які можуть дуже швидко підлаштовуватися під нові маршрути перевезення контрабанди та потреби чорного ринку.

Робота аналітиків в оперативно-розшуковій діяльності (ОРД) під час війни – це вже не просто паперова допомога оперативнику, а міцний фундамент, без якого побороти мафію неможливо. Сьогодні злочинці миттєво пристосовуються до війни: маскуються під волонтерів, незаконно переправляють ухилянтів за кордон або торгують нелегальною зброєю. Тому аналітика має бути швидкою та точною. Закон прямо визначає, що «завданням оперативно-розшукової діяльності є пошук і фіксація фактичних даних про протиправні діяння окремих осіб та груп» [2]. Під час воєнного стану шукати ці дані набагато складніше через масові переїзди людей та те, що ворог спеціально використовує кримінал для розхитування ситуації всередині нашої країни.

Сучасна аналітика в ОРД дуже відрізняється від тієї, що була до 2022 року. Зараз головна увага приділяється кримінальному аналізу, який допомагає скласти загальну картину з розкиданих шматочків інформації. Якщо раніше поліція більше спиралася на опитування та роботу з агентурою, то сьогодні головною стає робота з великими масивами даних (Big Data) та пошук цифрових слідів. Як зазначають фахівці, в умовах війни успішне виявлення організованих груп напряму залежить від розвідки на основі відкритих джерел (OSINT) та правильного поєднання відкритих даних із відомчими та міжвідомчими поліцейськими базами [3]. Тобто сучасний аналітик має бути трохи «хакером» і розвідником, щоб знаходити зв'язки, які злочинці намагаються сховати в Даркнеті чи переказах криптовалюти.

Національна поліція України, зокрема підрозділи стратегічних розслідувань, стратегічно переходить на сучасну модель ІІР (поліцейська діяльність, керована розвідкою). Це дозволяє відмовитися від застарілої моделі «відбувся злочин – поліція відреагувала» на користь сучасної моделі роботи на випередження – «проаналізували – запобігли» [4]. Аналітика тут виступає не просто як збір та обробка інформації, а як основа для того, щоб

керівництво приймало правильні рішення у боротьбі зі злочинністю. Головним інструментом при цьому є модель SARA (Сканування, Аналіз, Реагування, Оцінка), яку адаптували до умов бойових дій та протидії організованій злочинності [5].

Організована злочинність стала міжнародною загрозою для України, тому боротися з нею треба спільно з іншими державами. Наша країна активно інтегрується в європейську систему безпеки. Наприклад, ми беремо участь у програмі SOCTA (Оцінка загроз від серйозної та організованої злочинності в ЄС), де спершу вивчаються ризики на основі даних усіх країн-партнерів. Співпраця з Європолем дає нашим аналітикам доступ до інформації про те, куди ховають незаконні гроші в межах Європи. Водночас Інтерпол підтримує розслідування воєнних злочинів та допомагає шукати втікачів за кордоном. А структура ООН розробляє для України стратегію до 2029 року, щоб краще боротися з наркоторгівлею в умовах війни [6].

Особливість сьогоднішньої роботи полягає в тому, що правоохоронці працюють під шаленим тиском: часу обмаль, а ресурсів не вистачає. Експерти підкреслюють, що аналітика сьогодні має прогнозувати, як злочинці будуть співпрацювати з окупантами, адже це пряма загроза безпеці держави [7]. Завдяки такому підходу можна працювати на випередження: наприклад, блокувати фінансові рахунки злочинців ще до того, як ці гроші підуть на організацію нових злочинів.

За останні роки відбувся справжній прорив у використанні відкритої розвідки (OSINT) для потреб поліції. З'явилося багато приватних та державних команд (як-от компанія Molfar), які допомагають поліцейським знаходити майно злочинців та встановлювати особи хакерів. Сучасний пошук інформації стосовно організованої злочинності неможливий без великих даних та використання технологій штучного інтелекту [8].

Особливо важливою стає робота підрозділів кримінального аналізу. Вони збирають інформацію з поліцейських баз, матеріалів кримінальних справ та інтернету. Використовуючи спеціальні програми, наприклад IBM i2 Analyst's Notebook, аналітики малюють наочні схеми зв'язків між IP-адресами, грошовими переказами та самими злочинцями. Це дозволяє оперативнику та слідчому побачити приховані схеми та вийти на справжніх організаторів злочину.

Якщо коротко, то проста фіксація злочинів уже не працює. Щоб перемогти організовану злочинність сьогодні, потрібна глибока інтелектуальна аналітика. Старі методи, коли оперативники просто «відпрацьовували» територію, об'єкти чи особу (осіб), йдуть у минуле [9]. Їх замінюють точкові удари, які ретельно планують аналітики спільно з оперативниками та слідчими. Інтеграція аналітиків у роботу оперативників — це ключ до знищення міжнародних банд під час війни. Таким чином, аналітика працює як фільтр: вона відкидає зайве і дозволяє поліції бити точно в ціль, реально захищаючи країну.

Підсумовуючи вищевикладене, можна констатувати, що:

1. Організована злочинність в Україні сильно змінилася, швидко пристосувалася до умов війни і становить пряму загрозу державі.
2. Наш організований кримінал вийшов на міжнародний рівень, тому для його знищення потрібна тісна співпраця з Європолем, Інтерполом, ФБР та іншими правоохоронними структурами.
3. Поліція України переходить на роботу на випередження (модель ILP), тому аналітика стає фундаментом оперативної роботи, а не просто додатком до неї.
4. Сучасний оперативник обов'язково має бути трохи аналітиком: вміти шукати цифрові сліди та користуватися інструментами OSINT.

Отже, головний висновок для сучасного правоохоронця полягає в тому, що боротьба зі злочинністю сьогодні вимагає роботи розумом. Сучасне програмне забезпечення та аналітичні здібності є такою ж важливою зброєю, як і класичні знання та навички оперативника.

### Список використаних джерел

1. Ukraine: Organized Crime Dynamics in the Context of War. URL: [https://www.unodc.org/documents/data-and-analysis/Ukraine/Ukraine\\_OC\\_Study.pdf](https://www.unodc.org/documents/data-and-analysis/Ukraine/Ukraine_OC_Study.pdf).
2. Про оперативно-розшукову діяльність : Закон України від 18 лют. 1992 р. № 2135-ХІІ. Дата оновлення: 01.01.2026. URL: <https://zakon.rada.gov.ua/laws/show/2135-12#Text>.
3. Рижков Е. В. Методика «OSINT+»: синергія відкритих та відомчих інформаційних ресурсів у діяльності оперативних підрозділів Національної поліції України. *Роль OSINT-досліджень у підвищенні рівня національної безпеки України* : матеріали кругл. Столу (м. Львів, 07 трав. 2025 р.) / упоряд. І. О. Ревак. Львів : ЛьвДУВС, 2025. С. 192–199.
4. Рижков Е.В. «Загрози» впровадження методології ІЛР та Європолу СОСТА в діяльності підрозділів кримінальної поліції. *Актуальні питання діяльності підрозділів кримінальної поліції* : матеріали Всеукр. наук.-практ. конф. (м. Кропивницький, 14 квіт. 2023 р.). Кропивницький : ДонДУВС, 2023. С. 49–51.
5. The SARA Model // ASU Center for Problem-Oriented Policing. URL: <https://porcenter.asu.edu/content/sara-model>.
6. Уряд України та ООН підписали Рамкову програму співробітництва в галузі сталого розвитку між Україною та ООН на 2025–2029 роки // UN Ukraine. 2025. URL: [https://www.unodc.org/poukr/en/webstory\\_organized\\_crime\\_strategy\\_2025.html](https://www.unodc.org/poukr/en/webstory_organized_crime_strategy_2025.html).
7. Рижков Е. В. Використання інформаційних технологій для встановлення колаборантів. *Інформаційні технології в освіті та практиці* : матеріали Всеукраїнської науково-практичної конференції (м. Львів, 16 грудня 2022) / упорядник: Т. В. Магеровська. Львів : ЛьвДУВС, 2023. С. 58–62.
8. Виноградова К. В., Рижков Е. В. Використання штучного інтелекту підрозділами стратегічних розслідувань Національної поліції України. *Штучний інтелект і безпека* : матеріали наук.-практ. конф. (м. Київ, 19–21 листоп. 2024 р.). Київ : ІПМЕ ім. Г. Є. Пухова НАН України, 2024. С. 95–97.
9. Організація діяльності правоохоронних органів у сфері боротьби з організованою злочинністю : навч. посіб. / О. І. Козаченко, Е. В. Рижков, В. О. Черков, О.М. Чистолінов та ін. Луганськ : РВВ ЛДУВС, 2011. 184 с.

**Кудимов С. М.,**  
заступник начальника науково-дослідного відділу  
розвитку підготовки військ  
(*Національна академія сухопутних військ  
імені гетьмана Петра Сагайдачного*)

**Жук О. В.,**  
викладач кафедри тактики факультету  
бойового застосування військ  
(*Національна академія сухопутних військ  
імені гетьмана Петра Сагайдачного*)

**Гулько Л. В.,**  
доцент кафедри поведінкових наук  
та військового лідерства,  
доктор філософії  
(*Національна академія сухопутних військ  
імені гетьмана Петра Сагайдачного*)

## **OSINT ЯК СКЛАДОВА ПРОТИДІЇ НЕЛЕГАЛЬНІЙ ТОРГІВЛІ ТА ОБХОДУ САНКЦІЙ**

Нелегальна торгівля та обхід міжнародних санкцій є одними з найбільш латентних та економічно шкідливих видів злочинної діяльності, що становлять серйозну загрозу як для національної безпеки держав, так і для стабільності міжнародного порядку, в цілому. В умовах повномасштабної збройної агресії росії проти України ці проблеми набули нового виміру: санкційний тиск на державу-агресора супроводжується безпрецедентними зусиллями щодо його пошуку шляхів обходу через підставні компанії, треті країни та тіньові фінансові мережі, тоді як воєнний конфлікт генерує нові потоки незаконного обігу наркотиків та масове розкрадання культурних цінностей з окупованих територій. Виходячи з вищезазначеного, методи OSINT виступають ефективним інструментом виявлення та документування всіх зазначених видів протиправної діяльності.

У сфері протидії наркотрафіку OSINT-методи застосовуються на кількох рівнях. На оперативному рівні аналіз відкритих джерел дозволяє виявляти ринки збуту наркотичних речовин у даркнеті, відстежувати криптовалютні транзакції, пов'язані з незаконним обігом наркотиків, а також встановлювати логістичні маршрути їх переміщення через моніторинг транспортних та митних операцій, баз даних. Специфіка сучасного наркоринку полягає в активному використанні публічних месенджерів та соціальних мереж для організації збуту, що відкриває значні можливості для OSINT-моніторингу [1]. На стратегічному рівні аналіз відкритих фінансових звітів, корпоративних реєстрів та угод із нерухомістю дозволяє виявляти схеми легалізації доходів від наркоторгівлі.

Незаконний обіг культурних цінностей є проблемою, що різко загострилась після початку повномасштабного вторгнення російської федерації в Україну. За різними оцінками UNESCO та міжнародних правозахисних організацій, з окупованих українських територій

було викрадено тисячі предметів культурної та історичної спадщини [2]. І саме OSINT відіграє ключову роль у відстеженні шляхів переміщення викрадених об'єктів через аналіз аукціонних каталогів, баз даних антикварних ринків, публікацій у соціальних мережах та пропозицій на платформах електронної комерції. Бази даних викрадених об'єктів культурної спадщини – зокрема платформа INTERPOL Works of Art та Єдиний реєстр культурних цінностей України – у поєднанні з OSINT-моніторингом міжнародних арт-ринків забезпечують підґрунтя для ідентифікації та юридичного витребування викрадених цінностей.

Моніторинг виконання санкційних режимів є, мабуть, найбільш масштабним напрямом застосування OSINT у протидії нелегальній торгівлі. Після введення безпрецедентного пакету санкцій відносно росії у 2022 році фахівці з фінансового моніторингу, журналісти-розслідувачі та аналітики міжнародних організацій активно застосовують відкриті джерела для виявлення схем їх обходу. Аналіз корпоративних реєстрів юрисдикцій-транзитерів (ОАЕ, Туреччина, Казахстан, Вірменія), відстеження суднових маршрутів через AIS-дані, моніторинг митної статистики суміжних держав та аналіз ланцюгів поставок дозволяють виявляти реекспортні схеми та підставні компанії, що використовуються для постачання підсанкційних товарів подвійного призначення до росії [3].

Особливо ефективним виявився аналіз даних торговельного судноплавства у контексті санкцій. Публічні AIS-трекери (MarineTraffic, VesselFinder) у поєднанні з методами OSINT-атрибуції суден дозволили виявити так званий «тіньовий флот» – сотні танкерів, що здійснюють перевезення підсанкційної російської нафти, приховуючи свою ідентичність через вимикання транспондерів, зміни прапорів та складні схеми власності. Дослідження таких організацій, як CREA (Centre for Research on Energy and Clean Air), Kyiv School of Economics та Windward, що ґрунтуються виключно на відкритих даних, стали основою для впровадження нових санкційних механізмів [4].

Важливим методологічним інструментом OSINT-розслідувань у сфері санкційного комплаєнсу є аналіз корпоративної власності та ланцюгів бенефіціарів. Публічні реєстри компаній, бази даних витоків (Panama Papers, Pandora Papers), дані про державні закупівлі та відкриті фінансові звіти у поєднанні дозволяють встановлювати кінцевих бенефіціарів підставних структур, що використовуються для обходу санкцій. Міжнародні організації OCCRP (Organized Crime and Corruption Reporting Project) та Transparency International неодноразово публікували розслідування, засновані виключно на OSINT-методах, що призвели до введення нових санкцій та порушення кримінальних проваджень у різних юрисдикціях [5].

Разом із тим, OSINT-розслідування у сфері нелегальної торгівлі та санкційного моніторингу стикаються з низкою системних викликів. По-перше, стрімке розповсюдження складних корпоративних структур у непрозорих юрисдикціях суттєво ускладнює встановлення реальних бенефіціарів. По-друге, використання криптовалют та децентралізованих фінансових інструментів створюють нові виклики для аналізу фінансових потоків, хоча публічність блокчейну водночас відкриває нові можливості для OSINT-аналізу. По-третє, фрагментарність і неуніфікованість відкритих реєстрів різних юрисдикцій знижує ефективність крос-юрисдикційних розслідувань. Подолання цих обмежень потребує розбудови міжнародної аналітичної інфраструктури та гармонізації вимог до прозорості корпоративної власності.

Отже, OSINT є незамінним інструментом у протидії нелегальній торгівлі та обходу санкцій, що охоплює наркотрафік, незаконний обіг культурних цінностей та моніторинг виконання санкційних режимів. Комплексне застосування аналізу корпоративних реєстрів, відстеження торговельних і транспортних потоків, моніторингу криптовалютних транзакцій та аналізу арт-ринків дозволяє виявляти та задокументувати витончені схеми протиправної діяльності. Для підвищення ефективності цього напрямку в Україні необхідне: розроблення відомчих методичних стандартів OSINT-аналізу у сфері санкційного моніторингу; налагодження партнерства між державними органами та незалежними аналітичними організаціями; забезпечення участі українських фахівців у міжнародних санкційних розслідуваннях.

### **Список використаних джерел**

1. Décary-Héту D., Quessy-Doré O. Are Police Crackdowns Disrupting Internet Drug Cryptomarkets? A Longitudinal Analysis of the Effects of Operation Onymous. *Crime, Law and Social Change*. 2017. Vol. 67. Issue 1. P. 55–75.
2. UNESCO. Report on the Situation of Ukraine’s Cultural Heritage (March 2022 – March 2024). Paris: UNESCO, 2024. 48 p.
3. Bērziņš M., Kovaļovs G. Sanctions Circumvention Networks: OSINT Approaches to Detecting Third-Country Transit Schemes. *Baltic Journal of Law & Politics*. 2023. Vol. 16. Issue 2. P. 1–28.
4. Centre for Research on Energy and Clean Air (CREA). Shadow Fleet and Russian Oil: Tracking Violations Through Open Source Data. Helsinki, 2023. URL: <https://energyandcleanair.org/shadow-fleet> (дата звернення: 14.04.2025).
5. OCCRP. Pandora Papers: How the World’s Rich and Powerful Hide Their Money Offshore. Organized Crime and Corruption Reporting Project. 2021. URL: <https://www.occrp.org/en/the-pandora-papers> (дата звернення: 14.04.2025).

**Кудінов В. А.,**  
завідувач кафедри інформаційних технологій,  
кандидат фізико-математичних наук, доцент  
(Національна академія внутрішніх справ)

**Пакриш О. Є.,**  
доцент кафедри інформаційних технологій,  
кандидат технічних наук, доцент  
(Національна академія внутрішніх справ)

## **ІНТЕГРАЦІЯ МОЖЛИВОСТЕЙ OSINT У СИСТЕМУ ОПЕРАТИВНОГО ІНФОРМУВАННЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ**

В органах (підрозділах) Національної поліції України (далі – НПУ) для організації реагування на заяви і повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування створена та ефективно використовується інтегрована інформаційна система оперативного інформування. Відповідно до пункту 2 розділу I наказу Міністерства внутрішніх справ № 357 від 27 квітня 2020 року (далі – наказ) «оперативне інформування – єдина система збирання, опрацювання та подання до чергової служби вищого рівня інформації про правопорушення або подію з метою організації контролю за встановленням і затриманням осіб, які вчинили кримінальні правопорушення, а також оперативного реагування на надзвичайні ситуації» [1].

Заяви і повідомлення про правопорушення або події працівниками чергової служби органів (підрозділів) поліції реєструються в інформаційних ресурсах системи інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» (пункт 2 розділу II наказу) [1, 2]. З метою встановлення необхідної інформації про правопорушення або подію, забезпечення своєчасного та якісного реагування нарядами поліції за фактом їх учинення (виникнення) працівники чергової служби керуються Алгоритмом орієнтовних невідкладних дій (пункт 4 розділу II наказу) [1].

Зазначений Алгоритм передбачає з'ясування працівником чергової служби первинної інформації про обставини вчинення кримінального правопорушення та реєстрацію повідомлення в установленому порядку, негайне вжиття у разі необхідності відповідних заходів щодо організації реагування поліції на повідомлення, негайне інформування керівництва органу (підрозділу) поліції та чергової служби вищого рівня. В залежності від категорії повідомлення (наприклад, отримана інформація про резонансні кримінальні правопорушення або надзвичайні події) вона може негайно доповідатися керівництву НПУ, МВС, інших державних органів. Оперативний черговий Департаменту організаційно-аналітичного забезпечення та оперативного реагування НПУ опрацьовує отриману під час чергування інформацію про такі правопорушення та події, звертаючи особливу увагу на її повноту та за необхідності витребує додаткові відомості, готує добове зведення, яке подає керівництву поліції, заінтересованим структурним підрозділам центрального органу управління поліцією, відповідним органам державної влади.

Національна поліція України останніми роками з метою підвищення ефективності функціонування системи оперативного інформування впроваджує в її діяльність Ситуаційні

центри (далі – СЦ) [3, 4, 5]. СЦ – це сучасна форма організації аналітичної діяльності, яка базується на синтезі інформаційно-комунікаційних технологій, засобів накопичення і представлення інформації, комп'ютерних засобів підтримки прийняття рішень. Аналітики СЦ НПУ постійно збирають і обробляють відповідну інформацію, групують і передають її Голові НПУ для своєчасного прийняття відповідних управлінських рішень. Вони використовують три види аналізу [6]: 1) стратегічний – це аналіз злочинності, її рівня, поширеності, динаміки, структури загалом; 2) тактичний – це ситуація впродовж доби, тижня щодо конкретних регіонів, конкретних видів злочинів; 3) практичний – це оперативний кримінальний аналіз по кожному конкретному тяжкому та особливо тяжкому злочину. Необхідно відмітити, що аналітики СЦ НПУ, крім щоденного зведення за добу, також готують звіти за тиждень і за місяць.

На наш погляд, в умовах гібридних загроз та стрімкої цифровізації суспільства традиційні методи збору оперативної інформації працівниками чергових служб та аналітиками Ситуаційного центру потребують якісного доповнення інструментами OSINT, що зумовлено наступними факторами:

1. Первинне повідомлення про правопорушення часто містить фрагментарні або неточні дані. Використання OSINT дозволить працівнику чергової служби подолати «інформаційний вакуум» на початковому етапі (наприклад, швидко верифікувати подію через моніторинг локальних Telegram-каналів, стрімів у соцмережах та систем відеоспостереження з відкритим доступом).

2. Аналітики Ситуаційного центру використовуючи OSINT можуть швидко побудувати профіль правопорушника та отримати ідентифікацію ризиків ще до приїзду слідчо-оперативної групи на місце події. Наприклад, встановити: а) зв'язки підозрюваних осіб та їх належність до різних угруповань; б) наявність у правопорушників навичок поведінки зі зброєю шляхом аналізу контенту соцмереж; в) автотранспорт, на якому пересуваються особи.

3. За допомогою інструментів OSINT аналітик шляхом аналізу соціальних мереж може спрогнозувати динаміку розвитку надзвичайних ситуацій, що надзвичайно важливо для своєчасного маневрування силами та засобами поліції.

4. OSINT дозволяє миттєво отримати важливі дані (геолокацію, метадані, фото) на відміну від тривалих процедур отримання інформації через офіційні запити, що суттєво підвищує ефективність системи оперативного інформування, оскільки перші години після злочину є вирішальними для його розкриття.

5. Аналітики Ситуаційного центру через OSINT-моніторинг можуть протидіяти дезінформації та ПСО у ситуаціях, коли правопорушення використовується ворогом для розхитування стабільності в державі.

**Висновок:** інтеграція OSINT у систему оперативного інформування Національної поліції України перетворює Ситуаційний центр з органу фіксації на центр випереджальної аналітики. Це дозволить керівництву поліції приймати управлінські рішення, спираючись на повну інформаційну картину, що підвищує рівень публічної безпеки та мінімізує ризики для особового складу.

### Список використаних джерел

1. Про затвердження Інструкції з організації реагування на заяви і повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції України : Наказ МВС України від 27 квіт. 2020 р. № 357. *Верховна Рада України*: вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/z0443-20#Text> (дата звернення: 30.04.2026).
2. Про затвердження Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України» : Наказ МВС України від 03 серп. 2017 р. № 676. *Верховна Рада України*: вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/z1059-17#Text> (дата звернення: 30.04.2026).
3. Кудінов В. А. Удосконалення функціонування системи оперативного інформування Національної поліції України шляхом створення Ситуаційних центрів. *Використання сучасних інформаційних технологій в діяльності Національної поліції України*: матеріали Всеукр. наук.-практ. семінару (м. Дніпро, 23 листоп. 2018 р.). Дніпро : Дніпропетровський держ. ун-т внутр. справ, 2018. С. 44–46.
4. Кудінов В. А. Можливості Ситуаційних центрів Національної поліції України щодо виявлення та розкриття злочинів. *Актуальні питання виявлення та розкриття злочинів Національною поліцією: вітчизняний та зарубіжний досвід* : матеріали Міжнар. наук.-практ. круглого столу (м. Київ, 19 лют. 2020 р.). Київ : Нац. акад. внутр. справ, 2020. С. 106–109.
5. Кудінов В. А., Грищенко О. І., Швець М. М. Удосконалення правового забезпечення діяльності Ситуаційних центрів Національної поліції України. *Міхновські юридичні читання*: матеріали наук.-практ. конф. (м. Хмельницький, 31 берез. 2025 р.). Хмельницький : Нац. акад. держ. прикорд. служби України ім. Б. Хмельницького (військова частина 9960), 2025. С. 491–495.
6. Основні завдання та функції Ситуаційних центрів органів Національної поліції. *Prezi*: вебсайт. URL: <https://prezi.com/p/zhigbbcnpwj5/presentation/> (дата звернення: 30.04.2026).

**Кузьменко В. В.,**  
курсант 1 курсу навчально-наукового інституту підготовки фахівців  
для підрозділів кримінальної поліції імені Е. О. Дідоренка  
(*Донецький державний університет внутрішніх справ*)  
Науковий керівник: **Кісіль М. Л.,**  
викладач кафедри адміністративно-правових дисциплін  
(*Донецький державний університет внутрішніх справ*)

## **ВИКОРИСТАННЯ OSINT-ТЕХНОЛОГІЙ У ПРОТИДІ КІБЕРЗАГРОЗАМ: ДОСВІД ПРАВООХОРОННИХ ОРГАНІВ УКРАЇНИ**

Сучасний безпековий простір України характеризується надзвичайно високою інтенсивністю гібридних загроз, де кіберопераційна складова набуває дедалі більшого значення. Повномасштабне вторгнення Російської Федерації у 2022 році актуалізувало питання своєчасного виявлення, атрибуції та нейтралізації кіберзагроз, а відтак обумовило необхідність впровадження новітніх методів збору та аналізу розвідувальної інформації з відкритих джерел (Open Source Intelligence, OSINT). Метою цих тез є висвітлення практичних аспектів застосування OSINT-методології правоохоронними органами України в умовах триваючого збройного конфлікту.

OSINT як дисципліна розвідки охоплює сукупність методів і засобів збору, верифікації та аналізу загальнодоступної інформації з відкритих джерел: соціальних мереж, веб-сайтів, форумів у мережі darknet, телеграм-каналів, публічних баз даних, супутникових знімків, а також метаданих цифрових файлів [1, с. 205-210]. На відміну від класичних агентурних методів, OSINT-технології дозволяють оперативно отримувати значні масиви даних без порушення норм законодавства про збір інформації, що є критично важливим для забезпечення допустимості доказів у кримінальному провадженні.

У правоохоронній практиці України OSINT застосовується за кількома основними напрямками. По-перше, це ідентифікація суб'єктів кіберзлочинів. Фахівці Кіберполіції Національної поліції України та Департаменту кіберрозвідки СБУ систематично використовують інструменти аналізу цифрових слідів: Maltego, Shodan, Censys, SpiderFoot для встановлення реальних особистостей операторів хакерських угруповань за їхніми псевдонімами, IP-адресами, криптогаманцями та цифровими артефактами [2]. По-друге, у сфері моніторингу загроз правоохоронці відстежують активність АРТ-угруповань (Advanced Persistent Threat), пов'язаних із державними структурами РФ, зокрема Sandworm, Gamaredon (UAC-0010), FANCY BEAR, аналізуючи їхні публічні комунікаційні канали, технічні індикатори компрометації (IoC) та патерни поведінки.

Значний практичний потенціал має використання OSINT у процесі розслідування воєнних злочинів, пов'язаних із кібернетичними операціями. Інструментарій геолокації (геокодування зображень через Google Earth Pro, сервіс SunCalc для визначення часу зйомки за тінями), аналіз EXIF-метаданих, верифікація через крос-референсні джерела дозволяють документувати кібератаки на критичну інфраструктуру відповідно до вимог міжнародного гуманітарного права [3, с. 273-277]. Такий підхід вже апробовано у рамках взаємодії Офісу Генерального прокурора України з Міжнародним кримінальним судом.

Водночас імплементація OSINT-технологій у діяльність правоохоронних органів стикається з низкою проблем. Ключовою є верифікація достовірності отриманих даних,

оскільки противник активно застосовує дезінформацію та технології deepfake для компрометації OSINT-аналізу. Не менш важливою є проблема правового статусу OSINT-доказів у кримінальному процесі України: чинний КПК України не містить спеціальних норм щодо порядку збору та фіксації цифрових доказів з відкритих джерел, що породжує процесуальні ризики при їх використанні в суді [4, с. 294-303]. Окремої уваги потребує кадрове забезпечення: підготовка OSINT-аналітиків для потреб правоохоронних органів залишається фрагментарною та не відповідає сучасним оперативним потребам.

Перспективним напрямом удосконалення OSINT-практики у правоохоронній діяльності є інтеграція методів штучного інтелекту та машинного навчання для автоматизованої обробки великих масивів відкритих даних. Зокрема, моделі NLP (Natural Language Processing) демонструють високу ефективність при аналізі україно- та російськомовного контенту соціальних мереж з метою виявлення скоординованих інформаційних операцій. Паралельно актуальним є розвиток міжнародного співробітництва у сфері обміну OSINT-інформацією в рамках механізмів Інтерполу, Євроюсту та двосторонніх угод про правову допомогу [5, с. 431-437].

Таким чином, OSINT-технології становлять важливу інструментарій сучасної правоохоронної діяльності та забезпечення національної безпеки України. Їх ефективне впровадження потребує комплексного підходу: законодавчого врегулювання процесуального статусу OSINT-доказів, системної підготовки спеціалістів, розвитку відомчої інфраструктури аналізу відкритих даних та поглиблення міжнародного співробітництва у цій сфері. Подальші наукові розвідки мають бути спрямовані на розробку уніфікованих методологічних стандартів збору та оцінки OSINT-інформації, придатних для застосування у кримінальному провадженні.

### Список використаних джерел

1. OSINT у правоохоронній діяльності: міжнародний досвід та українські перспективи / К. Борисова, К. Жмуровська, Є. Кришталь, О. Деревягін. *UNIVERSUM*. 2025. № 25. С. 205–210. URL: <https://archive.liga.science/index.php/universum/article/view/2155> (дата звернення: 09.04.2026).
2. Використання інструментів та методів OSINT для отримання пошукової інформації: практ. порадник / Д. С. Зоренко, Л. О. Кульчицька, Р. В. Лех, О. І. Червяков. 5-те вид., переробл. та доповн. Харків : Видавець О. А. Мірошніченко, 2024. 36 с. URL: <https://dspace.nlu.edu.ua/handle/123456789/19712> (дата звернення: 09.04.2026).
3. Відкрита розвідка (OSINT) у протидії інформаційним війнам: аналітичні інструменти та правові межі. *Аналітично-порівняльне правознавство*. 2025. С. 273–277. URL: <https://journal-app.uzhnu.edu.ua/article/view/346448> (дата звернення: 10.04.2026).
4. Небезпека інструментів OSINT та способи пом'якшення наслідків їх використання для організації / С. Легомінова, Ю. Щавінський, Д. Рабчун та ін. *Кібербезпека: освіта, наука, техніка*. 2024. Т. 1. № 25. С. 294–303. DOI: <https://doi.org/10.28925/2663-4023.2024.25.294303> (дата звернення: 09.04.2026)..
5. OSINT у забезпеченні національної безпеки. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. С. 431–437. URL: <https://visnyk-pravo.uzhnu.edu.ua/article/view/344308> (дата звернення: 10.04.2026).

**Ленівий О. Ю.,**  
старший науковий співробітник  
(*Національна академія сухопутних військ  
імені гетьмана Петра Сагайдачного*)

**Матала І. В.,**  
науковий співробітник  
(*Національна академія сухопутних військ  
імені гетьмана Петра Сагайдачного*)

## **OSINT-ДОСЛІДЖЕННЯ ЯК НАПРЯМ РОЗСЛІДУВАННЯ ВОЄННИХ ЗЛОЧИНІВ, СКОЄНИХ АРМІЄЮ АГРЕСОРА**

Починаючи з 24 лютого 2022 року, повномасштабне збройне вторгнення російської федерації на територію України висвітило перед міжнародною спільнотою гостру проблему документування та притягнення до відповідальності осіб, винних у скоєнні воєнних злочинів. В умовах активних бойових дій традиційні методи збору доказів суттєво ускладнені, що зумовлює зростання ролі відкритих джерел розвідки (Open Source Intelligence, OSINT) як інструменту розслідування міжнародних злочинів.

Так, OSINT-дослідження охоплюють систематичний збір, верифікацію та аналіз інформації з публічно доступних джерел: соціальних мереж, відеохостингів, супутникових знімків, офіційних реєстрів, ЗМІ та інших відкритих баз даних. У контексті розслідування воєнних злочинів зазначений метод набуває особливої актуальності, оскільки дозволяє фіксувати докази в режимі реального часу, незважаючи на відсутність фізичного доступу до місця скоєння злочину.

Серед ключових напрямів застосування фахівцями OSINT у розслідуванні воєнних злочинів виділяють: геолокацію та верифікацію відеоматеріалів з місць ударів по цивільній інфраструктурі; ідентифікацію військової техніки та підрозділів збройних сил за ідентифікованими ознаками; аналіз супутникових знімків для фіксації знищення населених пунктів, масових поховань, переміщення військ; моніторинг офіційних заяв та публікацій у соціальних мережах для встановлення ланцюга командування.

Сьогодні практика застосування OSINT у розслідуванні злочинів, вчинених під час збройних конфліктів, вже має позитивні прецеденти. Зокрема, організація Bellingcat активно використовувала відкриті джерела для встановлення причетності підрозділів збройних сил росії до катастрофи MH17 над Донбасом у 2014 році [1]. Сформована доказова база на основі OSINT-досліджень була врахована Спільною слідчою групою та стала важливим елементом кримінального розслідування. Цей досвід заклав підґрунтя для подальшого розвитку цифрової криміналістики в умовах збройних конфліктів.

Також з початком повномасштабного вторгнення 2022 року OSINT-спільнота консолідувала зусилля навколо документування злочинів проти мирного населення. Низка організацій – Mnemonic, WITNESS, Truth Hounds, українські правозахисні структури – розгорнули масштабні проекти зі збору та архівування цифрових доказів. Водночас Офіс Прокурора Міжнародного кримінального суду (МКС) активно взаємодіє з OSINT-аналітиками в рамках власних розслідувань [2]. Видача ордерів на арешт потенційних злочинців пугіна та львової-білової у березні 2023 року стала значною мірою результатом такої роботи.

Проте, попри очевидні переваги, OSINT-методи розслідування воєнних злочинів зіштовхуються з низкою суттєвих обмежень. По-перше, проблема допустимості доказів: більшість правових систем висувають суворі вимоги до ланцюга зберігання доказів (chain of custody), яких складно дотриматись у разі використання матеріалів із соціальних мереж. По-друге, ризик цифрових фальсифікацій – дипфейків та маніпульованих зображень – суттєво ускладнює верифікацію отриманих матеріалів. По-третє, масштаб конфлікту генерує надзвичайно великий обсяг інформації, що ускладнює її систематизацію та оцінку [3].

Для подолання зазначених обмежень міжнародна спільнота виробляє спеціалізовані стандарти поводження з цифровими доказами. Berkeley Protocol on Digital Open Source Investigations (2020) став першим міжнародно визнаним документом, що регламентує методологію OSINT-розслідувань у сфері прав людини та міжнародного гуманітарного права [4]. Протокол визначає вимоги до збору, збереження та аналізу цифрових матеріалів з огляду на їх потенційне використання в судових провадженнях.

В Україні формується власна інституційна база для OSINT-розслідувань воєнних злочинів. Офіс Генерального прокурора України створив спеціалізований підрозділ з документування воєнних злочинів, який активно співпрацює з цифровими дослідниками. Крім того, ряд університетів та науково-дослідних установ розпочали підготовку фахівців у галузі цифрової криміналістики та OSINT-аналізу [5]. Водночас залишається нагальна потреба у законодавчому врегулюванні порядку збору та використання цифрових доказів у кримінальних провадженнях, пов'язаних із воєнними злочинами.

Таким чином, OSINT-дослідження є невід'ємним та перспективним напрямом розслідування воєнних злочинів в умовах сучасних збройних конфліктів. Ефективне використання цього інструменту потребує: розробки та імплементації стандартизованих методологій верифікації цифрових доказів; налагодження системної взаємодії між OSINT-дослідниками, правоохоронними органами та міжнародними інституціями; законодавчого закріплення статусу цифрових доказів у національному кримінально-процесуальному законодавстві. Реалізація цих заходів дозволить значно підвищити ефективність притягнення до відповідальності осіб, винних у вчиненні воєнних злочинів на території суверенної України.

#### **Список використаних джерел**

1. Higgins E. *We Are Bellingcat: An Intelligence Agency for the People*. Bloomsbury Publishing, 2021. 304 p.
2. Kersten M. *Justice in Conflict: The Effects of the International Criminal Court's Interventions on Ending Wars and Building Peace*. Oxford University Press, 2016. 272 p.
3. Scott-Railton J., Marczak B., McKune S. Closing the Net: How OSINT Evidence Is Transforming International Justice. *Journal of International Criminal Justice*. 2023. Vol. 21. Issue 2. P. 345–368.
4. Berkeley Protocol on Digital Open Source Investigations. A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law. United Nations Human Rights Office of the High Commissioner, New York and Geneva, 2022. 186 p.
5. Потєбенько М. О. Цифрова криміналістика в розслідуванні воєнних злочинів: проблеми теорії та практики. *Науковий вісник Національної академії внутрішніх справ*. 2023. № 3 (128). С. 45–53.

**Лисенко Б. О.,**  
курсант 3 курсу навчально-наукового  
інституту поліцейської діяльності  
(*Національна академія внутрішніх справ*)  
Науковий керівник: **Шаповаленко Є. В.,**  
професор кафедри оперативно-розшукової  
діяльності та національної безпеки,  
кандидат юридичних наук, доцент  
(*Національна академія внутрішніх справ*)

## **АСПЕКТИ ФІКСАЦІЇ ШАХРАЙСТВ, ВЧИНЕНИХ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЙ DEERFAKE ТА СИНТЕЗУ ГОЛОСУ ШТУЧНИМ ІНТЕЛЕКТОМ**

Стрімкий розвиток генеративних нейромереж докорінно кіберзлочинність, перетворивши технології синтезу зображення (Deerfake) та клонування голосу на потужні інструменти для вчинення корисливих кримінальних правопорушень. Якщо класичне шахрайство спиралося на психологічні маніпуляції через текст або звичайний дзвінок, то сьогодні злочинці використовують штучний інтелект для створення біометрично достовірної ілюзії спілкування з близькими родичами або керівництвом. Сучасні дослідники справедливо відзначають, що головна небезпека дїпфейків полягає у їхній здатності змусити людей повірити в реальність того, чого ніколи не існувало, що має колосальний вплив на сприйняття чесності людини та маніпулювання її фінансами [4, с. 376].

Технологія Deerfake остаточно перейшла межу від розважального контенту до інструменту реальної загрози майновій безпеці. В умовах воєнного стану кібершахраї масово експлуатують вразливість населення: спостерігається стрімке зростання заяв громадян щодо вимагання коштів від імені військовослужбовців або полонених, чиї голоси були автоматизовано синтезовані на основі коротких відео з соціальних мереж. ШІ наразі виступає потужним інструментом для створення складних схем обману, де успішність атак сягає критично високих показників саме через стресовий стан потерпілих [5]. Відповідно, перед правоохоронними підрозділами постає нагальна потреба в негайній адаптації криміналістичних методик до умов, де головним слідом злочину є синтезований і вкрай нестабільний електронний файл.

Ключова процесуальна проблема розслідування таких злочинів полягає в тому, що чинний Кримінальний процесуальний кодекс України (КПК) не містить вичерпної та спеціалізованої дефініції поняття «електронний доказ», найчастіше ототожнюючи його зі звичайними документами згідно зі ст. 99 КПК України [1]. На практиці це створює безпрецедентні труднощі під час первинної фіксації.

Згенеровані ШІ голосові повідомлення чи відеодзвінки в месенджерах (Telegram, WhatsApp) є вкрай нестабільними: злочинці використовують функції автовидалення, а самі пристрої потерпілих часто не зберігають кеш-файли дзвінків. Коли слідчий проводить огляд смартфона в порядку ст. 237 КПК України, він зазвичай просто переписує текст повідомлення або робить фотографію екрана (скріншот). Проте візуальна фіксація екрана повністю знищує

метадані файлу, його хеш-суму та цифрові артефакти алгоритму генерації, що унеможливує подальше проведення комп'ютерно-технічної чи фоноскопичної експертизи [3, с. 45]. Наприклад, під час розслідування так званого "CEO Fraud" (шахрайства з піддробкою голосу керівника компанії) або обходу біометричної ідентифікації банківських додатків (KYC) за допомогою дипфейк-масок, слідчий часто стикається з тим, що оригінального медіафайлу на сервері вже немає через його відкриття зловмисником. У результаті суд згодом справедливо може визнати такі докази недопустимими через сумніви в їх автентичності, оскільки захист легко доведе неможливість перевірки джерела походження файлу.

Поряд із процесуальними складнощами первинної фіксації, виникає не менш серйозна проблема матеріального права щодо правильної та справедливої кваліфікації таких діянь. Хоча стаття 190 Кримінального кодексу України передбачає кримінальну відповідальність за заволодіння майном шляхом обману або зловживання довірою, ця норма створювалася задовго до появи нейромереж і зовсім не враховує специфіки «цифрової імітації» особистості як окремої, більш тяжкої кваліфікуючої ознаки [2].

Використання генеративного штучного інтелекту для синтезу голосу чи відеозображення є не просто класичним «обманом», а глибоким, високотехнологічним втручанням, яке потребує ретельної підготовки, цілеспрямованого збору біометричних даних жертви та використання спеціалізованого програмного забезпечення. Це суттєво підвищує рівень суспільної небезпечності діяння, утворюючи нові склади злочинів, однак наразі правоохоронці змушені кваліфікувати ці високотехнологічні злочини за загальними частинами статті 190 КК України. Такий підхід часто не відповідає реальному масштабу заподіяної шкоди та технологічній складності вчиненого кіберзлочину.

Для комплексного вирішення проблеми фіксації електронних слідів та ефективної протидії таким злочинам правоохоронцям України варто імплементувати міжнародний досвід, зокрема ключові положення Протоколу Берклі. Цей документ встановлює жорсткі, але дієві стандарти роботи з цифровими доказами, акцентуючи увагу на збереженні їхньої початкової цілісності, обов'язковому криптографічному хешуванню та унеможливленню будь-якої модифікації з боку третіх осіб [3, с. 12]. Щоб адаптувати ці високі стандарти під реалії чинної системи досудового розслідування, необхідно на законодавчому рівні внести зміни до КПК України та ККУ [1, 2], доповнивши процесуальний закон спеціалізованими нормами щодо вилучення віртуальних активів, а кримінальний кодекс – новою кваліфікуючою ознакою «з використанням технологій штучного інтелекту».

Водночас, на відомчому рівні необхідно терміново зобов'язати слідчо-оперативні групи відмовитися від застарілої практики простого фотографування екранів пристроїв. Замість цього має бути запроваджений обов'язковий і безальтернативний алгоритм: здійснювати процесуальне експортування оригінального медіафайлу через системні функції застосунків на захищений носій поліції із застосуванням програм для підрахунку хеш-суми (наприклад, за алгоритмом SHA-256) безпосередньо на місці огляду [5]. Лише симбіоз оновленої нормативної бази та неухильного дотримання сучасних процесуальних алгоритмів вилучення метаданих дозволить формувати належну доказову базу та ефективно притягувати кіберзлочинців до відповідальності.

### Список використаних джерел

1. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI. *Верховна Рада України*. URL: <https://zakon.rada.gov.ua/laws/show/4651-17#Text> (дата звернення: 10.04.2026).
2. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III. *Верховна Рада України*. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (дата звернення: 10.04.2026).
3. Використання електронних доказів під час досудового розслідування злочинів проти миру, безпеки людства та міжнародного правопорядку (Протокол Берклі) : наук.-практ. порадник / Л. В. Гаврилюк, І. В. Басиста, Д. С. Афонін та ін. Львів : Політехніка, 2024. 196 с. URL: [https://www.researchgate.net/publication/385514719\\_Vikoristanna\\_elektronnih\\_dokaziv\\_pid\\_cas\\_dosudovogo\\_rozsliduvanna\\_zlociniv\\_proti\\_miru\\_bezpeki\\_ludstva\\_ta\\_miznarodnogo\\_pravoporadku\\_Protokol\\_Berkli\\_naukovo-prakticnij\\_poradnik](https://www.researchgate.net/publication/385514719_Vikoristanna_elektronnih_dokaziv_pid_cas_dosudovogo_rozsliduvanna_zlociniv_proti_miru_bezpeki_ludstva_ta_miznarodnogo_pravoporadku_Protokol_Berkli_naukovo-prakticnij_poradnik) (дата звернення: 10.04.2026).
4. Діпфейк в контексті Декларації про майбутнє Інтернету. *Юридичний науковий електронний журнал*. 2022. № 5. С. 375–378. URL: <https://dspace.onua.edu.ua/bitstreams/6555a817-3832-492e-b340-b832c1d2dbef/download> (дата звернення: 10.04.2026).
5. Штучний інтелект у правовій практиці: межі та можливості : матеріали наук.-практ. конф. (м. Івано-Франківськ, 14 берез. 2025 р.). Івано-Франківськ : Університет Короля Данила, 2025. URL: [https://if.uu.edu.ua/wp-content/uploads/2025/05/14\\_03\\_2025.pdf](https://if.uu.edu.ua/wp-content/uploads/2025/05/14_03_2025.pdf) (дата звернення: 10.04.2026).

Ліва С. О.

курсантка 2 курсу навчально-наукового інституту з  
підготовки фахівців для підрозділів кримінальної поліції  
(Львівський державний університет внутрішніх справ)

Огірко О. І.

кандидат технічних наук,  
професор кафедри інформаційних технологій  
(Львівський державний університет внутрішніх справ)

## OSINT: ЯК ОДНА ФОТОГРАФІЯ МОЖЕ РОЗКРИТИ ВСЮ ІНФОРМАЦІЮ ПРО ЛЮДИНУ

OSINT упорядковує розрізнені відкриті дані, перетворюючи їх на чіткі висновки, придатні для практичного застосування, зокрема у правоохоронній діяльності. Розвідка з відкритих джерел є системним процесом збору й аналізу інформації, що перебуває у вільному доступі та не потребує порушення законодавства. Йдеться не про несанкціонований доступ, а про роботу з публічними джерелами: соціальними мережами, новинами, державними реєстрами, супутниковими знімками, а також метаданими фото- і відеоматеріалів [1].

«Один селфі з відпустки може розкрити точні координати завдяки відображенню в очах або положенню тіні» [1], а в поєднанні з OSINT-інструментами таке зображення може стати джерелом значного обсягу додаткової інформації, що виходить за межі самого фото.

Зокрема, засоби OSINT дозволяють здійснювати пошук схожих зображень у мережі, визначати першоджерело та відстежувати подальше поширення фотографії. Важливе значення має також аналіз метаданих, які можуть містити інформацію про пристрій зйомки, час створення файлу та геолокацію. Наприклад, сервіси *GeoSpy* та *EarthKit* забезпечують визначення місця зйомки та фактичну географічну прив'язку зображення. Платформи *Immerse.zone* та *Aperisolve* розширюють можливості аналізу візуальних даних, допомагаючи виявляти на фотографії додаткові, неочевидні елементи [2].

Фотозображення є важливим джерелом доказової інформації, яке дозволяє відтворювати перебіг подій. Їх аналіз дає змогу встановити, що саме відбулося, визначити час і обставини події, а також уточнити окремі деталі, зокрема кількість учасників, характер їхніх дій, емоційний стан, наявність техніки чи зброї [3, с. 15].

Отримана інформація може використовуватися для ідентифікації особи, встановлення її зв'язків, визначення місця перебування та відтворення обставин події, що має безпосереднє значення для формування доказової бази у кримінальних провадженнях. Комплексне застосування різних OSINT-інструментів дозволяє зіставляти фрагменти інформації та формувати більш повну аналітичну картину [4, с. 92].

Використання OSINT-розпізнавання обличь у поєднанні з іншими методами аналізу відкритих джерел підвищує ефективність первинної перевірки даних, сприяє оперативнішому встановленню осіб та підвищує якість аналітичної роботи правоохоронних органів.

Подібні підходи застосовуються в сучасній практиці правоохоронних органів. Зокрема, у Національній поліції України встановлення особи починається саме з аналізу окремого фото. Далі здійснюється пошук у соціальних мережах, зіставлення зовнішніх ознак, аналіз оточення та інших цифрових слідів, що дозволяє поступово ідентифікувати особу та встановити її зв'язки [3, с. 13].

Практичним прикладом є ситуації, коли поліція оприлюднює фотографії підозрюваних або осіб, причетних до злочинів, після чого їх ідентифікація та встановлення місцеперебування здійснюється шляхом залучення відкритих джерел та інформації від громадськості. Зокрема, у справі про вбивство в Одесі оприлюднене правоохоронцями фото підозрюваного сприяло подальшому збору інформації та його розшуку [5].

Разом з тим, науковці звертають увагу на те, що використання OSINT пов'язане з необхідністю забезпечення балансу між ефективністю правоохоронної діяльності та дотриманням фундаментальних прав людини. З огляду на це особливого значення набувають етичні, правові та соціальні аспекти обробки відкритої інформації, насамперед персональних даних, а також дотримання меж допустимого втручання у приватне життя [4, с. 115].

Для України ці питання є особливо актуальними, оскільки розвиток OSINT відбувається в умовах євроінтеграційних процесів, які передбачають наближення до європейських підходів у сфері захисту інформації та прав людини. У зв'язку з цим врахування досвіду провідних держав світу дозволяє більш чітко визначати правові та організаційні підходи до використання відкритих джерел у правоохоронній діяльності [4, с. 116].

Таким чином, можливості OSINT у роботі з фотозображеннями підтверджують його практичну цінність як інструменту аналізу відкритої інформації у правоохоронній діяльності. Водночас його використання має здійснюватися з урахуванням законності та необхідного балансу між ефективністю розслідувань і захистом прав людини.

#### **Список використаних джерел**

1. Кальник М. OSINT це розвідка відкритих джерел: повний посібник для новачків і профі. *Nfront*. URL: <https://lnk.ua/6oeiXUDk4> (дата звернення: 29.04.2026).
2. Інструменти OSINT для роботи з зображеннями. *HackYourMom*. URL: <https://lnk.ua/j8FKNSgM8> (дата звернення: 29.04.2026).
3. Пошук інформації з відкритих джерел (OSINT) працівниками кримінальної поліції: навчал.-метод. рекомендації / уклад. Форос Г. В., Калугін В. Ю. Одеса, ОДУВС, 2026. 37 с. URL: <https://lnk.ua/nB8Kke2j3> (дата звернення: 29.04.2026).
4. OSINT Open Source Intelligence. Теорія та методологія : монографія / Користін О. Є. та ін., за заг. ред. Користіна О. Є., Демедюка С. В. Київ: 7БЦ, 2025. 304 с. URL: <https://lnk.ua/IagZJSfgr> (дата звернення: 29.04.2026).
5. Поліція опублікувала фото підозрюваного у вбивстві в Одесі: його розшуковують. *Українська правда*. URL: <https://lnk.ua/RlywQPxUo> (дата звернення: 29.04.2026).

**Ліліченко Є. С.,**  
здобувач вищої освіти  
(Національна академія Служби безпеки України )  
**Зайченко В. В.,**  
старший викладач, кандидат технічних наук  
(Національна академія Служби безпеки України )

## ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ ВІДКРИТОЇ РОЗВІДКИ У КНР

Технологія OSINT прорвала інформаційний туман війни та відкрила кричущі факти злочинів, які здійснила росія проти України. Існує безліч прикладів, коли за допомогою методів OSINT, таких як геолокація та аналіз супутникових зображень, військові злочини росії поширювалися на Заході через соціальні мережі. Крім того, ця технологія використовувалася і потім, для протидії безглуздим російським виправданням своїх незаконних дій.

OSINT (Open Source Intelligence – розвідка з відкритих джерел) у Китайській Народній Республіці (КНР) – це масштабна, державно-орієнтована діяльність, яка відіграє ключову роль у стратегії національної безпеки, економіки та військового розвитку.

Ключові особливості OSINT у КНР:

- Масштаб та ресурси: За оцінками дослідників, Китай приділяє колосальну увагу розвідці з відкритих джерел. У КНР налічується близько 100 000 аналітиків, які займаються збиранням та аналізом відкритої інформації.

- ШІ та цифровізація: Китай активно впроваджує генеративні моделі штучного інтелекту (ШІ) у військову розвідку, що дозволяє створювати «цифрових аналітиків», які працюють цілодобово. Китай активно використовує ШІ для OSINT, що дозволяє в реальному часі аналізувати величезні масиви даних із соцмереж для отримання критичної розвідінформації, наприклад, про переміщення військ.

- Військове застосування: У Білій книзі оборони КНР 2019 року наголошується, що сучасна війна вимагає проривів в інформаційному та інтелектуальному забезпеченні, що робить OSINT пріоритетом для армії.

- ГЕО-OSINT: Геопросторова розвідка (ГЕО-OSINT) застосовується для моніторингу об'єктів, відстеження переміщень, а також у правоохоронній діяльності для ідентифікації місць правопорушень та аналізу ризиків.

- Інтеграція в правоохоронну діяльність: Китайські правоохоронні органи інтегрують OSINT-інструменти для розслідування злочинів, включаючи використання передових технологій, таких як ШІ-окуляри.

- Специфіка джерел: Через «Великого китайського фаєрвола» (Great Firewall) та обмежень, OSINT у Китаї спирається на унікальну екосистему місцевих платформ:

- Пошук: Baidu (близько 70% ринку).

- Соцмережі/Месенджери: WeChat (1,34 млрд користувачів), Weibo (598 млн), Douyin (752 млн).

- Корпоративні/Робочі платформи: DingTalk, Lark.

- «Цифровий слід» та соціальний рейтинг: У країні активно функціонує система соціального рейтингу, що збирає дані про громадян та компаній.

Основні напрямки використання OSINT у Китаї:

- Пошук наукових талантів: Збір інформації про досягнення вчених.

- Економічна розвідка: Аналіз ринків, конкурентів та виявлення витоків технологій.

Історично OSINT у КНР також використовувався для аналізу ринків та економічних процесів.

- Військовий моніторинг: Аналіз супутникових знімків виявлення будівництва військових об'єктів (наприклад, нових командних центрів).

- Відстеження міжнародних відносин: Аналіз публікацій прикордонних зон та зовнішньої політики.

- Інформаційна безпека: OSINT розглядається як інструмент для підвищення національної безпеки, що включає моніторинг терористичної активності та боротьбу з незаконною діяльністю.

Китай розглядає OSINT як «дешевий» та ефективний спосіб отримати критично важливу інформацію, часто випереджаючи західні країни за обсягом даних, що обробляються.

Використання методів OSINT (розвідки на основі відкритих джерел) у Китайській Народній Республіці (КНР) є складовою загальної стратегії інформаційної безпеки та національної розвідки, що поєднує класичні методи збирання даних із передовими технологіями штучного інтелекту (ШІ).

Основними джерелами даних є соціальні мережі, супутникові знімки, відкриті урядові звіти та інші загальнодоступні джерела, обробка яких здійснюється за допомогою автоматизованих систем.

Використання методів розвідки на основі відкритих джерел (OSINT) у Китайській Народній Республіці (КНР) має специфічний характер, поєднуючи передові технології, державний контроль та масштабний збір даних для різних цілей, від національної безпеки до кібершпигунства.

Основні аспекти використання OSINT у КНР:

- Інтеграція в державні системи контролю: Аналітичні технології OSINT інтегровані в національну систему соціального контролю та профілактики правопорушень.

- «Усе суспільство» для збору даних: КНР використовує підхід «усе суспільство» для збору та аналізу відкритих даних, що часто пов'язують із крадіжкою західних технологій, при цьому ФБР відзначає високу активність китайського шпигунства.

- Військове та розвідувальне використання: Національний університет оборонних технологій КНР (NUDT) активно розробляє інструменти штучного інтелекту для OSINT-розвідки, що підсилює можливості армії.

- Кібершпигунство: Китайські групи, такі як ті, що пов'язані з PRC-Nexus (наприклад, UNC6384 або Mustang Panda), використовують OSINT для викрадення веб-трафіку та проведення атак.

- Контроль за технологіями: У КНР посилюється контроль над інформацією та технологіями, зокрема, забороняється використання західного програмного забезпечення (ПЗ) для кібербезпеки.

- Використання ШІ-окулярів: Поліцію в Китаї оснащують ШІ-окулярами для розширення можливостей збору даних у реальному часі.

- Моніторинг інфраструктури: Проекти, такі як китайське LEO сузір'я зв'язку (GuoWang/XingWang), аналізуються з використанням OSINT-даних.

Крім того, Китай веде активну діяльність у сфері кібербезпеки та кібершпигунства, часто використовуючи OSINT як частину ширших операцій, що призводить до конкуренції з США та ЄС.

Запроваджені в китайській розвідці ШІ-моделі беруть на себе рутинну роботу аналітиків, автоматизуючи обробку величезних масивів даних. З відкритих джерел (OSINT) вони моніторять соціальні мережі, новинні сайти, форуми — те, що раніше потребувало цілої армії перекладачів і аналітиків. Нові алгоритми здатні миттєво відфільтрувати потрібну інформацію й навіть перевіряти її достовірність.

Китайські фахівці у своїх дослідженнях відзначають, що сучасні OSINT-мережі, оснащені ШІ, можуть отримувати дані від сотень тисяч інформаторів онлайн і за допомогою великих моделей автоматично виконувати перехресної перевірки та історичного аналізу, відфільтровуючи фейки та значно підвищуючи правдивість інформації.

Обсяги таких перевірених даних і швидкість їхньої публікації стають недосяжними для суто людських аналітичних центрів.

Китайські збройні сили стрімко інтегрують штучний інтелект у систему військової розвідки, прагнучи створити "цифрового військового аналітика", здатного працювати 24/7 без перерв. Мовиться про потужні алгоритми штучного інтелекту – великі мовні моделі (LLM), адаптовані спеціально для розвідувальних завдань.

Зокрема, провідний військовий виш КНР, Національний університет оборонних технологій (NUDT), спільно з іншими установами активно розробляє власні LLM, налаштовані на обробку даних розвідки з відкритих джерел (OSINT), радіоелектронної розвідки (SIGINT), геопросторової розвідки (GEOINT) та агентурної розвідки (HUMINT).

Відкрита розвідка стала незамінним та асиметричним інструментом у протидії іноземному інформаційному маніпулюванню та втручанню. Систематичне застосування GeoINT, SOCMINT та сучасних AI-assisted інструментів дозволяє незалежним і інституційним акторам оперативно виявляти, верифікувати та атрибутувати інформаційні атаки.

Водночас, для забезпечення стійкості та легітимності OSINT у довгостроковій перспективі необхідно подолати два ключові виклики. По-перше – методологічна прозорість: в умовах зростання загрози deepfakes та маніпуляцій GenAI верифікація даних вимагає запровадження уніфікованих, прозорих і криміналістично сумісних стандартів. По-друге – правова легітимізація: OSINT-розслідування мають чітко відповідати вимогам захисту персональних даних, покладаючись на законний інтерес як правову підставу та мінімізуючи збір надлишкової інформації.

### **Список використаних джерел**

1. Онищенко Ю. М. Міжнародний досвід використання OSINT. Актуальні питання протидії кіберзлочинності та торгівлі людьми (м. Харків, 23 листоп. 2018 р.) / МВС України, Харків. нац. ун-т внутр. справ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС. 2018. С. 379–381
2. Про правомірність відсилання до відкритих джерел у відповідь на запит про надання інформації. URL: <https://zaholovok.com.ua/pro-pravomirnist-vidsylannya-do-vidkrytykh-dzherel-uvipovid-na-zapyt-pro-nadannya-informatsiyi>.
3. GDPR essentials for OSINT research. URL: <https://www.blockint.nl/methods/gdpr-essentialsfor-osint-research>.
4. Досвід організації та здійснення розвідувального забезпечення ЗС України під час широкомасштабного вторгнення зс рф в Україні (інформаційний бюлетень, 2023).
5. Воєнна розвідка. 2023. Вид. 1, 2.
6. How OSINT shaped reporting on the war in Ukraine. URL: <https://www.info-res.org/eyes-onrussia/articles/how-osint-shaped-reporting-on-the-war-in-ukraine>.
7. OSINT як доказ у розслідуванні воєнних злочинів: представники ВС взяли участь у тематичному семінарі. Вебсайт: Верховний суд України. URL: <https://supreme.court.gov.ua/supreme/pres-centr/news/1883443>.
8. Гаценко С. С., Металіди О. Г., Богатирьов С. О., Василяйко І. І. Застосування програмного забезпечення для комплексного ведення розвідки в інтересах вогневого ураження противника. Збірник наукових праць ЦВСД НУОУ. 2024. № 1 (80). С. 87–93.
9. Уфімцева О. С. Використання OSINT в умовах збройної агресії рф проти України.

**Лісов О. С.,**  
доцент кафедри управління та інформаційно-аналітичного  
забезпечення оперативної-службової діяльності,  
кандидат історичних наук  
(Національна академія Служби безпеки України)

**Меншаков А. С.,**  
начальник відділу  
(Департамент інформаційно-аналітичного забезпечення  
Служби безпеки України)

## **МЕТОДИЧНІ АСПЕКТИ ІМПЛЕМЕНТАЦІЇ ІІІ В СЛУЖБОВУ ДІЯЛЬНІСТЬ ДЛЯ ПОСИЛЕННЯ ОСІНТ-СПРОМОЖНОСТЕЙ СУБ'ЄКТІВ РОЗВІДУВАЛЬНОГО СПІВТОВАРИСТВА**

Швидке зростання обсягів відкритих даних радикально змінило умови здійснення аналітичної діяльності у сфері розвідки. Потіки інформації, що генеруються в цифровому середовищі, вже не можуть бути ефективно опрацьовані виключно традиційними методами. Це зумовлює потребу в залученні інструментів штучного інтелекту. Розвиток ОСІНТ-спроможностей дедалі більше залежить не лише від доступу до джерел, а від здатності швидко структурувати, інтерпретувати та верифікувати великі масиви даних. Відтак запровадження технологій ІІІ у службову діяльність не є питанням технологічної модернізації як такої, а виступає методичним викликом, що потребує переосмислення підходів до збору, аналізу та оцінки інформації.

Водночас у науковому та аналітичному середовищі поступово утвердився прагматичний підхід до використання ІІІ. Його не розглядають як автономне «універсальне рішення» або беззаперечне джерело істини. Генеративні моделі за своєю природою є ймовірнісними алгоритмами, які доцільно використовувати як інструмент формування гіпотез, автоматизації рутинних операцій, структурування даних і первинної підготовки матеріалів до експертної верифікації. Такий підхід дозволяє максимально реалізувати потенціал технології, зберігаючи визначальну роль людського інтелекту, критичного аналізу та відповідальності за кінцеві висновки.

У цьому контексті ключова перевага ІІІ в ОСІНТ полягає у значному прискоренні аналітичного циклу під час роботи з великими масивами даних. Моделі здатні здійснювати автоматичне узагальнення (сумаризацію) об'ємних документів, класифікувати інформаційні потоки, виявляти приховані тематичні зв'язки, виконувати багатомовний переклад і фіксувати фактичні суперечності між різними джерелами. Це, своєю чергою, дозволяє ОСІНТ-аналітику зосередитися не на технічній обробці, а на оцінюванні достовірності, інтерпретації змісту та формуванні прогнозів.

Реалізація зазначеного потенціалу на практиці потребує комбінованого використання різних типів штучного інтелекту. Базові ІІІ-системи застосовуються для автоматичного збору даних (агрегації) і моніторингу показників у режимі реального часу; алгоритми машинного навчання забезпечують кластеризацію контенту, аналіз тональності, виявлення аномальної активності та прогнозування інформаційних трендів; глибоке навчання використовується для аналізу фото- і відеоматеріалів (у т.ч. для розпізнавання обличчя та голосу), супутникових знімків та розпізнавання об'єктів; великі мовні моделі – для узагальнення інформації, побудови складних запитів і підготовки аналітичних продуктів.

Методично обґрунтований підхід до організації процесів передбачає відмову від використання одного універсального інструмента на користь побудови інтегрованих агентних

систем. У межах такої структури окремі інструменти виконують спеціалізовані функції: ОСІНТ-платформи забезпечують збір даних, ШІ-асистенти упорядковують інформаційні масиви, а системи RAG (Retrieval-Augmented Generation) інтегрують модель із верифікованими базами документів, зменшуючи ризики викривлення фактів. Додатково застосування методики формування запитів ReAct (міркування та дія) та послідовного промптингу дозволяє покращити внутрішню логіку роботи моделей і підвищити якість результатів.

Практична значущість цих підходів найбільш виразно проявляється у сфері національної безпеки. Рішення на основі ШІ дають змогу здійснювати раннє виявлення загроз, аналізувати кампанії дезінформації, відстежувати ворожі інформаційно-психологічні операції та оцінювати ризики для критичної інфраструктури. Особливу роль відіграє здатність моделей працювати у мультилінгвальному середовищі, що є критично важливим у контексті транснаціонального характеру сучасних загроз.

Одним із найбільш перспективних напрямів є автоматизована геопросторова розвідка. Системи комп'ютерного зору забезпечують первинну ідентифікацію техніки, аналіз змін на місцевості та верифікацію локацій через зіставлення візуальних ознак. Водночас результати ШІ мають розглядатися як робочі гіпотези, що потребують додаткової перевірки за допомогою картографічних даних, метаданих і незалежних джерел.

Ще одним важливим напрямом є оптимізація підготовки аналітичних матеріалів. Використання ШІ дозволяє швидко формувати брифінги, порівнювати альтернативні інтерпретації подій, виділяти ключові наративи та створювати попередні варіанти управлінських рішень. Це підвищує оперативність реагування, однак не скасовує необхідності дотримання принципу «людина в контурі».

Попри значні переваги, застосування ШІ супроводжується низкою ризиків. Найбільш критичним серед них є феномен «галюцинацій», коли модель генерує недостовірну або вигадану інформацію, включно з неіснуючими джерелами чи зв'язками. У контексті ОСІНТ це створює загрозу хибних аналітичних висновків і підриву довіри до результатів діяльності.

Додаткові виклики пов'язані з активним використанням ШІ супротивником. Генеративні технології застосовуються для створення дипфейків, масштабування бот-мереж та проведення цілеспрямованих інформаційних атак. У таких умовах використання ШІ має поєднуватися з впровадженням інструментів виявлення ШІ-генерованого контенту як складової протидії.

У зв'язку з цим особливого значення набуває методична складова. Ефективне використання ШІ передбачає постійне оновлення знань, адаптацію інструментів і розуміння принципів функціонування моделей. Аналітик має володіти не лише технічними навичками, а й критичним баченням їхніх обмежень.

Ключовою умовою є впровадження чіткої процедури верифікації. Будь-який результат роботи ШІ має розглядатися як гіпотеза, що підлягає перевірці через декомпозицію тверджень, пошук незалежних джерел, перехресний аналіз і фіксацію доказової бази (Chain of Custody). Такий підхід дозволяє мінімізувати ризики та забезпечити належний рівень достовірності аналітичних продуктів.

Не менш важливими є питання операційної безпеки. Використання публічних ШІ-сервісів для обробки чутливої інформації може призвести до витоку даних. Тому доцільним є застосування корпоративних або локальних рішень, що забезпечують контроль над інформаційними потоками.

Отже, ШІ виступає потужним інструментом посилення ОСІНТ-спроможностей, проте його ефективність визначається не стільки технологічними можливостями, скільки якістю методології його використання. Найбільш результативним є поєднання можливостей ШІ щодо пошуку закономірностей і формування гіпотез із роллю аналітика, який забезпечує контекстуалізацію, верифікацію та відповідальність за кінцеві висновки.

Лукашук Ю. А.,  
асистент кафедри  
автоматизованих систем управління,  
доктор філософії

(Національний університет «Львівська політехніка»)

## **ІНТЕЛЕКТУАЛІЗАЦІЯ OSINT-ДОСЛІДЖЕНЬ: РОЛЬ ГЛИБОКОГО НАВЧАННЯ У ЗАБЕЗПЕЧЕННІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ**

Інтелектуалізація OSINT-досліджень у контексті стрімкої цифровізації набуває критичного значення, оскільки відкриті джерела інформації формують основу оперативного аналізу безпекового середовища. Зростання обсягів даних із соціальних мереж, новинних платформ, форумів і супутникових знімків одночасно розширює аналітичні можливості та ускладнює їх обробку. Традиційні методи аналізу виявляються недостатньо ефективними через масштаб і швидкість оновлення інформації, що зумовлює необхідність застосування методів глибокого навчання як ключового інструменту інтелектуалізації OSINT [1].

Метою дослідження є підвищення ефективності OSINT-аналітики у сфері національної безпеки шляхом інтеграції методів глибокого навчання. Для досягнення цієї мети визначено такі завдання: аналіз сучасних підходів до інтелектуалізації OSINT; дослідження можливостей застосування глибоких нейронних мереж для обробки неструктурованих даних; оцінка їх переваг та обмежень; формування концептуальних засад побудови інтелектуалізованих OSINT-систем. Об'єктом дослідження є процеси аналізу відкритих джерел інформації, предметом – методи глибокого навчання в задачах OSINT.

OSINT як підхід до збору та аналізу відкритих даних характеризується доступністю, легальністю та широким охопленням інформаційного простору. Його роль у забезпеченні національної безпеки полягає у своєчасному виявленні загроз, аналізі суспільних настроїв, моніторингу діяльності потенційно небезпечних суб'єктів і протидії дезінформаційним кампаніям. Водночас значні обсяги різнорідних даних формують ефект інформаційного перевантаження, що ускладнює виділення релевантних сигналів і потребує автоматизованих методів обробки [2]. Зокрема, обсяги даних у соціальних мережах можуть досягати мільйонів повідомлень щоденно, що унеможлиблює їх ефективний ручний аналіз.

Додатковим викликом є низька інтерпретованість результатів глибокого навчання, оскільки складні нейронні мережі функціонують як «чорні скриньки». Це обмежує їх застосування у сфері національної безпеки, де критично важливо забезпечити прозорість і обґрунтованість рішень. Крім того, існує загроза адверсійних впливів, які здатні навмисно спотворювати вхідні дані та призводити до помилкових результатів аналізу. Це зумовлює необхідність розробки стійких і захищених моделей.

Особливу увагу слід приділити впровадженню методів пояснюваної штучної інтелектуальної системи, що дозволить аналітикам інтерпретувати логіку прийняття рішень нейромережами, мінімізуючи ризики помилок у критичних безпекових сценаріях. Це забезпечить необхідний рівень довіри до автоматизованих висновків та дозволить ефективно протидіяти цілеспрямованим маніпуляціям із вхідними даними

Глибоке навчання, як підгалузь машинного навчання, базується на багатошарових нейронних мережах і демонструє високу ефективність при роботі з неструктурованими даними, включаючи текст, зображення та відео. Його ключова перевага полягає у здатності автоматично виявляти складні закономірності та адаптуватися до нових даних, що

забезпечує якісно новий рівень аналізу інформації. Серед основних архітектур виділяються згорткові (CNN), рекурентні (RNN, LSTM, GRU) та трансформерні моделі, які забезпечують глибоку семантичну обробку даних і формування прогностичних моделей [3].

Згорткові нейронні мережі ефективні для аналізу візуальних даних, зокрема супутникових знімків та зображень із відкритих джерел, забезпечуючи точну ідентифікацію об'єктів. Рекурентні моделі доцільні для аналізу часових рядів і послідовностей повідомлень у соціальних мережах. Трансформерні архітектури демонструють найвищу ефективність у задачах обробки природної мови завдяки механізму уваги, що дозволяє враховувати контекст і виявляти приховані семантичні зв'язки. Це робить їх ключовим інструментом аналізу дезінформації та інформаційних кампаній.

Застосування глибокого навчання в OSINT охоплює насамперед аналіз текстових даних. Методи обробки природної мови забезпечують автоматичну класифікацію інформації, визначення тональності повідомлень, виявлення маніпулятивного контенту та проведення тематичного аналізу великих масивів даних. Це є критично важливим для своєчасного виявлення інформаційно-психологічних операцій і формування відповідних заходів реагування [4].

Окремого значення набувають мультимодальні моделі, здатні одночасно обробляти текстові, візуальні та аудіодані. У межах OSINT це забезпечує комплексний аналіз інформаційних потоків, поєднуючи новини, зображення та відео з соціальних мереж. Такий підхід підвищує достовірність результатів і зменшує вплив дезінформації.

Взаємодія компонентів OSINT-системи реалізується у вигляді послідовного конвеєра обробки даних. Первинна інформація проходить етапи очищення, нормалізації та семантичного збагачення, після чого надходить до аналітичного модуля. Він здійснює мультимодальний аналіз і формує узагальнені ознаки для прогнозування та оцінки ризиків. Отримані результати інтегруються у підсистему підтримки прийняття рішень, яка забезпечує формування аналітичних висновків і рекомендацій для суб'єктів безпеки. Запропонована архітектура має модульно-ієрархічну структуру, що забезпечує масштабованість і можливість інтеграції нових джерел даних без зміни базової системи.

Глибоке навчання активно застосовується для аналізу соціальних мереж, зокрема для виявлення бот-мереж, аналізу механізмів поширення інформації та прогнозування суспільних настроїв. Це дозволяє не лише фіксувати поточні тенденції, але й моделювати сценарії розвитку інформаційних кампаній, що є ключовим для інформаційної безпеки держави. Паралельно методи комп'ютерного зору забезпечують аналіз супутникових знімків, ідентифікацію об'єктів, визначення їх геолокації та виявлення потенційних загроз у реальному часі [5].

Здатність глибокого навчання до прогнозування складних процесів дозволяє оцінювати ризики, моделювати кризові ситуації та формувати сценарії реагування. Це забезпечує перехід від реактивного до проактивного підходу у сфері національної безпеки. У цьому контексті інтелектуалізовані OSINT-системи формують основу систем раннього попередження, які забезпечують своєчасне виявлення загроз і підтримку стратегічних рішень [6].

Практичним прикладом є виявлення інформаційно-психологічних операцій у соціальних мережах. Використання трансформерних моделей дозволяє ідентифікувати аномальні патерни поширення інформації, координовану поведінку користувачів і джерела дезінформації. Додатково методи кластеризації та семантичного аналізу забезпечують виявлення тематичних наративів інформаційних кампаній.

Попри переваги, застосування глибокого навчання в OSINT супроводжується низкою викликів. До них належать проблеми якості даних, наявність шуму та упередженості, низька інтерпретованість моделей, а також ризики ворожих атак. Це може призводити до

помилкових висновків, що є критичним у сфері національної безпеки. Додатково постають етичні та правові аспекти використання персональних даних і необхідність регулювання застосування штучного інтелекту [7].

Сучасні підходи до аналізу супутникових даних передбачають використання глибоких нейронних мереж для виявлення змін на місцевості, ідентифікації інфраструктурних об'єктів і військової техніки, а також виявлення ознак підготовки до загроз. Поєднання комп'ютерного зору з геоінформаційними системами забезпечує підвищення точності просторового аналізу.

Розвиток нейромережевих технологій захисту даних у реальному часі створює додаткові можливості для їх застосування в OSINT-аналітиці [8].

Концептуальна модель інтелектуалізованої OSINT-системи може включати модуль збору даних, підсистему попередньої обробки, аналітичний модуль глибокого навчання, модуль прогнозування ризиків і підсистему підтримки прийняття рішень. Така структура забезпечує комплексний аналіз інформації та підвищує ефективність реагування на сучасні загрози.

Інтелектуалізовані OSINT-системи стають ключовим елементом сучасної аналітичної інфраструктури, забезпечуючи інтеграцію різнорідних даних, підвищення швидкості аналізу та ефективну протидію інформаційним і кіберзагрозам, особливо в умовах гібридних конфліктів.

Подальший розвиток інтелектуалізації OSINT пов'язаний із удосконаленням алгоритмів глибокого навчання, впровадженням мультимодальних моделей та розвитком пояснюваного штучного інтелекту. Це забезпечить підвищення прозорості, надійності та ефективності аналітичних систем у сфері національної безпеки, а також формування нової парадигми обробки інформації, орієнтованої на швидкість, точність і адаптивність.

Впровадження інтелектуалізованого конвеєра обробки даних дозволить скоротити цикл OODA (Observe-Orient-Decide-Act (спостерігати – орієнтуватися – приймати рішення – діяти)), забезпечуючи перевагу в швидкості реагування на гібридні загрози. Це трансформує OSINT з допоміжного інструменту збору інформації на стратегічну систему раннього попередження про загрози національній безпеці.

### Список використаних джерел

1. Russell S., Norvig P. *Artificial Intelligence: A Modern Approach*. 4th ed. Harlow: Pearson, 2021. 1136 p.
2. Batrinca B., Treleaven P. Social media analytics: a survey of techniques, tools and platforms. *AI & Society*. 2015. Vol. 30. № 1. P. 89–116.
3. Goodfellow I., Bengio Y., Courville A. *Deep Learning*. Cambridge: MIT Press, 2016. 775 p.
4. Vaswani A. et al. Attention Is All You Need. *Advances in Neural Information Processing Systems*. 2017. Vol. 30.
5. LeCun Y., Bengio Y., Hinton G. Deep learning. *Nature*. 2015. Vol. 521. P. 436–444.
6. Jordan M. I., Mitchell T. M. Machine learning: Trends, perspectives, and prospects. *Science*. 2015. Vol. 349. № 6245. P. 255–260.
7. Floridi L. et al. AI4People—An ethical framework for a good AI society. *Minds and Machines*. 2018. Vol. 28. № 4. P. 689–707.
8. Лукашук Ю. А. Інформаційна технологія захисту даних у реальному часі для мобільних смарт-систем з використанням нейроподібних мереж : дис. ... д-ра філософії : 122 «Комп'ютерні науки». Львів, 2023. 155 с.

## **OSINT-ДОСЛІДЖЕННЯ: ОСОБЛИВОСТІ ВИКОРИСТАННЯ ПРОГРАМНИХ ПРОДУКТІВ ДЛЯ ЗБИРАННЯ ЦИФРОВИХ ДОКАЗІВ У КРИМІНАЛЬНИХ ПРОВАДЖЕННЯХ ЩОДО ВОЄННИХ ЗЛОЧИНІВ**

Особливості інформаційної структури та локалізації слідів злочинів актуалізують необхідність постійного вдосконалення та оптимізації OSINT-досліджень з метою збирання цифрових доказів та встановлення обставин, що підлягають доказуванню у кримінальних провадженнях, відкритих за ознаками ст. 438 Кримінального кодексу України. Ратифікація 15 липня 2025 р. Верховною Радою України Угоди між Україною та Радою Європи про створення Спеціального трибуналу щодо злочину агресії проти України додає перспективності зазначеній проблематиці.

Ключовим завданням постає ідентифікація цифрових слідів суб'єктів воєнних злочинів через аналіз віртуального простору в прив'язці до його географічної та технічної інфраструктури. Зазначена слідова інформація об'єктивована в комп'ютерній інформації на електронних носіях, засобах зв'язку та у інших формах відображення: супутникових знімках, серверах, які обслуговують системи зв'язку, соціальних мережах тощо.

Таким чином, цифрові докази, отримані з відкритих джерел (OSINT), дозволяють:

- фіксувати пропаганду, заклики до агресії, кібератаки та інші інформаційні операції, які супроводжують збройну агресію РФ проти України;
- ідентифікувати виконавців воєнних злочинів;
- доводити факти злочинів проти людяності та порушення Женевських конвенцій, аналізуючи цифрові матеріали – від супутникових знімків руйнувань цивільної інфраструктури до публічних закликів до насильства у медіапросторі;
- передавати систематизовані матеріали до Міжнародного кримінального суду (МКС), Спеціального трибуналу щодо злочину агресії проти України, а також до інших міжнародних трибуналів і правозахисних організацій для правової оцінки дій агресора.

Реалії сьогодення вимагають від працівників правоохоронних органів та органів досудового розслідування трансформації професійного підходу, формування нової парадигми доказування, ключовим елементом якої стає використання цифрових даних та доказів. В зазначених умовах цифрові сліди (дані), зокрема матеріали з відкритих джерел (OSINT), дані, що містяться у спеціалізованих програмних продуктах (як службових, комерційних, так і загальнодоступних), супутникові знімки, інформація з соціальних мереж та інші дані, набувають вирішального значення для встановлення обставин вчинення воєнних злочинів та ідентифікації осіб, причетних до них.

Важливість та специфіку функціонування таких даних активно досліджують як міжнародні, так і українські науковці. Зокрема, у працях іноземних фахівців значна увага приділяється стандартам автентичності та збереження «ланцюжка зберігання» цифрових матеріалів. У свою чергу, вітчизняні дослідники, такі як, Г. Авдєєва, Д. Афонін, І. Гловюк, І. Гора, І. Каланча, В. Колесник, О. Метелєв, Ю. Найдьон, М. Погорецький, О. Пазюк, В. Шевчук, Д. Цехан та інші представники академічної спільноти, детально описують процесуальні аспекти інтеграції та використання новітніх технологій у кримінальне

провадження, практичні способи ідентифікації доказів, що мають електронну форму [1], ідентифікацію правової природи контекстуальних елементів воєнних злочинів [2], роль та потенціал новітніх технологій у документуванні, розслідуванні та доказуванні воєнних злочинів в умовах російської агресії проти України тощо [3]. Наукові розвідки спрямовані на теоретичне обґрунтування цифрового доказу як автономного джерела відомостей, що потребує чіткої законодавчої регламентації. Кримінальний процесуальний кодекс України не виокремлює цифрові докази як окрему категорію та не надає їм окремого статусу. Для позначення іншого формату таких доказів він використовує термін «комп'ютерні дані», наслідуючи підхід, визначений у Конвенції про кіберзлочинність, а також поняття «електронний документ». Однак визначення цих понять в Кодексі відсутнє як і їх співвідношення між собою. Лише ч. 3 ст. 99 КПК містить інформацію щодо того, що «оригіналом електронного документа є його відображення, якому надається таке ж значення, як документу». Крім цього, з аналізу ч. 4 ст. 99 КПК України можна зробити висновок, що до комп'ютерних даних законодавець відносить інформацію, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних та комп'ютерних системах [4].

Міжнародні стандарти роботи з електронними доказами закріплені у Будапештській конвенції про кіберзлочинність від 23 листопада 2001 року, ратифікованій Україною 7 вересня 2005 року, та Другому додатковому протоколі до неї від 12 травня 2022 року, підписаному Україною 30 листопада 2022 року, присвяченому посиленню співпраці та розкриттю електронних доказів.

На міжнародному рівні важливе значення має Римський статут МКС, юрисдикція якого визнана Україною, який встановлює основоположні принципи допустимості доказів у міжнародному правосудді.

Натомість визначення поняття електронних доказів сформульовано в постанові Касаційного кримінального суду від 06.02.2024 у справі № 645/6247/16-к, під яким, відповідно розуміється інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи, зокрема, електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), веб-сайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі. Такі дані можуть зберігатися, зокрема, на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (в тому числі в мережі інтернет).

Правові підстави застосування технічних засобів у кримінальному провадженні визначаються не лише кримінальним процесуальним законодавством, а й низкою спеціальних законів України, зокрема Законами України «Про Службу безпеки України», «Про оперативно-розшукову діяльність», «Про контррозвідувальну діяльність», «Про адвокатуру та адвокатську діяльність», іншими законами та підзаконними нормативно-правовими актами. Особливістю цих норм є відсутність вичерпного переліку технічних засобів і методів, що обумовлено їх різноманіттям і постійним розвитком. У зв'язку з цим законодавство закріплює загальні принципи їх застосування, визначає коло уповноважених суб'єктів, межі використання, процедурні вимоги та доказове значення отриманих результатів.

КПК України передбачає можливість використання технічних засобів у діяльності учасників провадження, зокрема спеціалістів, а також визнає доказами матеріали фото-, аудіо- та відеофіксації і комп'ютерні дані. Норми, що регулюють проведення слідчих і

негласних слідчих дій, допускають застосування різних способів фіксації інформації, включаючи зйомку, запис, вимірювання, створення графічних матеріалів та роботу з електронними даними. Окремі положення також визначають порядок огляду комп'ютерної інформації та її відображення.

Зміни до кримінального процесуального законодавства, що набрали чинності у березні 2022 року, деталізували порядок роботи з електронними доказами та комп'ютерними системами. Вони передбачають можливість отримання доказів у межах міжнародного співробітництва, визнають копії та дублікати електронної інформації як оригінали за певних умов, регламентують процедури доступу до електронних систем без їх вилучення, копіювання даних із залученням спеціалістів, а також особливості тимчасового вилучення, арешту та обшуку комп'ютерних систем. Такий підхід є обґрунтованим, оскільки дозволяє забезпечити гнучкість правового регулювання і уникнути необхідності постійного оновлення норм у зв'язку з розвитком сучасних технологій.

З огляду на вищевикладене, важливим постає питання, які інноваційні програмні продукти здатні забезпечити достовірність та належність електронних доказів для підвищення ефективності документування воєнних злочинів. Окремим вектором досліджень у цьому напрямі є специфіка використання інноваційних програмних продуктів для OSINT-розвідки, де основний науковий інтерес зміщується від простого збору інформації до розробки методології підтвердження автентичності та цілісності отриманих цифрових масивів у межах кримінального процесу.

Практичний досвід використання методів OSINT у поєднанні зі спеціалізованим програмним забезпеченням та сучасними технологічними інструментами (зокрема Palantir, Maltego, Clearview AI, Artelligence, Delta) свідчить про їхню високу результативність за умови комплексного та узгодженого застосування. Водночас для досягнення максимальної результативності пошуку інформації доцільно застосовувати так званій «метод зачіпок» - поетапного розширення інформаційного поля на основі навіть мінімальних вихідних даних.

Зокрема, за наявності будь-якої вихідної інформації суб'єкт пошуку та вивчення інформації має не лише володіти відповідними інструментами, а й розуміти логіку побудови інформаційних зв'язків: те, як одна деталь може розкрити ширший контекст, виявити нових осіб, події або встановити чітку геолокацію. Відповідно, за такого підходу процес пошуку ознак трансформується у процесуальну діяльність із доказування причетності особи до вчинення злочину. Саме системне мислення, поєднане з технічними можливостями сучасних інструментів, формує основу ефективного OSINT-аналізу.

У цьому контексті ключовим викликом залишається забезпечення належного рівня верифікації отриманих даних. В умовах інформаційної війни та навмисного поширення дезінформації будь-який цифровий матеріал потребує багаторівневої перевірки через перехресний аналіз джерел, встановлення метаданих, часових і просторових маркерів. Недотримання цих принципів може не лише нівелювати доказову цінність зібраної інформації, а й поставити під сумнів результати розслідування в цілому.

Не менш важливим є питання стандартизації підходів до збирання, збереження та передачі електронних доказів. Формування єдиних методологічних підходів, адаптованих до процесуального порядку кримінального провадження в умовах воєнного часу, дозволить підвищити якість доказової бази та забезпечити її прийнятність у міжнародних судових інституціях, включаючи МКС та Спеціальний трибунал. У перспективі це стане одним із

визначальних факторів у забезпеченні невідворотності покарання за воєнні злочини та відновленні справедливості для нашої держави.

В Україні вказану сферу також регулює ДСТУ ISO/IEC 27037:2017 «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів», який діє з 1 січня 2019 року [5]. Разом з цим, загальноприйнятим документом у вказаній сфері також вважається Протокол Берклі [6]. Це перший набір глобальних керівних положень щодо використання цифрових даних, які є у відкритому доступі, як доказів у міжнародних розслідуваннях щодо порушень прав людини. Документ містить стандарти знаходження, збирання, зберігання, перевірки та аналізу контенту із соцмереж та інших відкритих джерел [7].

Вагомим прикладом ефективності синергії методів OSINT та спеціалізованого програмного забезпечення є документування обставин воєнного злочину – ракетного обстрілу дитячої лікарні «Охматдит» у м. Києві 8 липня 2024 року. Внаслідок удару по лікувальному корпусу, де перебували пацієнти та персонал, загинули дві цивільні особи, а 34 особи, серед яких дев'ять дітей, отримали поранення різного ступеня тяжкості.

Використання програмних продуктів та методів OSINT дозволило відтворити трек польоту ракети, ідентифікувати її як російську крилату ракету класу «повітря-земля» Х-101 та спростувати дезінформацію РФ щодо можливої причетності українських сил протиповітряної оборони.

Завдяки аналізу отриманих даних було встановлено командну ієрархію зс РФ та ідентифіковано особу, яка надала наказ на застосування стратегічної авіації. Як наслідок, на основі зібраних електронних доказів російському генерал-майору Сергію Кувалдіну було заочно повідомлено про підозру у порушенні законів та звичаїв війни (ч. 2 ст. 438 КК України). Це стало черговим кроком до формування беззаперечної доказової бази для українських судів та міжнародних судових інстанцій, підтверджуючи, що цифрові сліди є невід'ємним елементом забезпечення невідворотності покарання за міжнародні злочини [8].

### Список використаних джерел

1. Каланча І. Г. Докази, що мають електронну форму в кримінальному процесі України: ідентифікація та цілісність у світлі концепції chain of custody. *Věda a perspektivy*. 2025. № 8(51). С. 206. DOI:10.52058/2695-1592-2025-8(51)-206-230.
2. Гловюк І. В., Тетерятник Г. К. Контекстуальні елементи у провадженнях щодо воєнних злочинів: предмет доказування sui generis. 2022. URL: <https://scholar.google.com/citations>.
3. Погорецький М. А. Застосування новітніх технологій у розслідуванні та доказуванні воєнних злочинів. *Вісник кримінального судочинства*. 2023. № 3–4. С. 84. DOI: <https://doi.org/10.17721/2413-5372.2023.3-4/84-102>.
4. Кримінальний процесуальний кодекс України. *Відомості Верховної Ради України (ВВР)*. 2013. № 9-10. № 11-12. № 13. Ст. 88
5. Національний стандарт України «Інформаційні технології. Методи захисту. Настанови для ідентифікації, збирання, здобуття та збереження цифрових доказів». URL: [https://www.ksv.biz.ua/GOST/DSTY\\_ALL/DSTU5/DSTU\\_ISO\\_IEC\\_27037-2017.pdf](https://www.ksv.biz.ua/GOST/DSTY_ALL/DSTU5/DSTU_ISO_IEC_27037-2017.pdf).
6. URL: [Berkeley-Protocol-Ukrainian.pdf](#).
7. Протокол Берклі щодо розслідування із використанням відкритих цифрових даних — Jurfem.
8. *Урядовий кур'єр*. № 39 (7699). С. 18. URL: [39\\_7699r.pdf](#)

**Манжай О. В.,**  
завідувач кафедри протидії кіберзлочинності,  
кандидат юридичних наук, професор  
(Харківський національний університет внутрішніх справ)

**Манжай І. А.,**  
старший викладач кафедри  
інформаційних систем та технологій  
(Харківський національний університет внутрішніх справ)

## **СПЕЦИФІКА ВИЯВЛЕННЯ ЦИФРОВИХ СЛІДІВ НЕЗАКОННОГО ОБІГУ ПРЕКУРСОРІВ МЕТОДАМИ OSINT**

В умовах стрімкої конвергенції злочинності та кіберпростору значна частина незаконного обігу наркотичних засобів та сировини для їх виготовлення перемістилася у кіберпростір. За порушення встановлених правил виробництва, виготовлення, зберігання, обліку, відпуску, розподілу, торгівлі, перевезення, пересилання чи використання прекурсорів передбачено кримінальну відповідальність згідно зі ст. 320 Кримінального кодексу України.

Легальний порядок обігу прекурсорів жорстко регламентований законодавством, зокрема постановою Кабінету Міністрів України від 06.04.2016 № 282. Базовим документом для ідентифікації таких речовин є Перелік наркотичних засобів, психотропних речовин і прекурсорів, затверджений Постановою Кабінету Міністрів України від 06.05.2000 № 700.

Особливу увагу під час моніторингу мережі Інтернет правоохоронним органам доцільно зосередити саме на прекурсорах списку 2 таблиці IV. Такий фокус дослідження зумовлений подвійною природою цих речовин. На відміну від специфічних хімікатів з інших списків, більшість речовин зі списку 2 є поширеними промисловими розчинниками та реагентами, що мають масовий легальний цивільний обіг. Правопорушники активно користуються цим фактом, маскуючи тіньовий збут сировини для синтезу наркотиків під звичайну господарську торгівлю. Великі обсяги легального продажу створюють інформаційний шум, що нівелює ефективність прямого пошуку та вимагає застосування специфічних аналітичних підходів.

Відповідно до зазначеного Переліку, до прекурсорів списку 2 таблиці IV належать, зокрема:

- антранілова кислота (2-амінобензойна кислота);
- ацетон (2-пропанон);
- етиловий ефір (діетиловий ефір);
- калію перманганат (калій марганцевокислий);
- метилетилкетон (2-бутанон);
- піперидин (гексагідропіридин; пентаметиленімін);
- сірчана кислота (сульфатна кислота);
- соляна кислота (хлористоводнева кислота);
- толуол (метилбензол);
- ANPP / NPP (та їхні похідні, зокрема: 1-бром-2-фенілетан; 1-хлор-2-фенілетан; 1-диметиламіно-2-пропанол; 2,5-диметоксибензальдегід; 4-метоксибензилметилкетон тощо).

Під час моніторингу мережі Інтернет з метою виявлення фактів незаконного поводження з прекурсорами правоохоронці стикаються з тим, що зловмисники свідомо уникають прямих назв контрольованих речовин. Відповідно, безпосередній текстовий пошук за міжнародними назвами прекурсорів не завжди дає бажаного результату або призводить до

інформаційного перевантаження легальними пропозиціями. З огляду на це, ефективний алгоритм пошуку має включати такі непрямі методи:

1) пошук за хімічними формулами. Продавці нелегальних речовин часто маскують оголошення, вказуючи лише хімічну формулу. Наприклад, для пошуку тіньових пропозицій щодо продажу ацетону (2-пропанону) доцільно використовувати формули  $(\text{CH}_3)_2\text{CO}$  або  $\text{C}_3\text{H}_6\text{O}$ . Такий підхід дозволяє виявляти приховані оголошення на платформах на кшталт OLX (рис. 1);

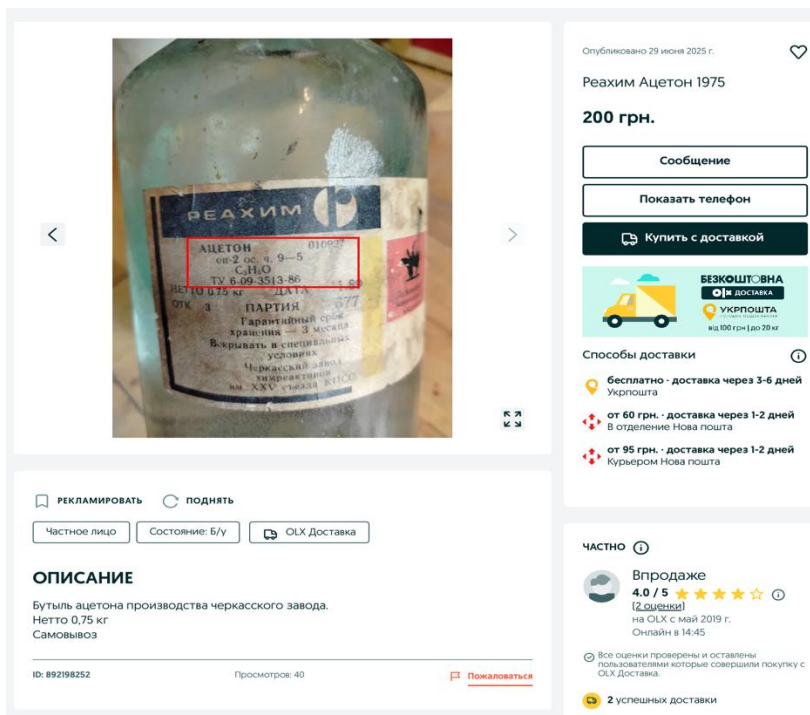


Рис. 1. Результат пошуку на сайті OLX

2) візуальний пошук. Оскільки специфічні хімічні реактиви часто постачаються у стандартизованій тарі, ефективним інструментом є зворотний пошук за зображенням типового пакування конкретного прекурсора (рис. 2). Це дозволяє знаходити сторінки продавців навіть за умови навмисно спотвореного текстового опису. Відповідний пошук можна здійснювати і за зображенням типової тари пакування прекурсорів (рис. 2);

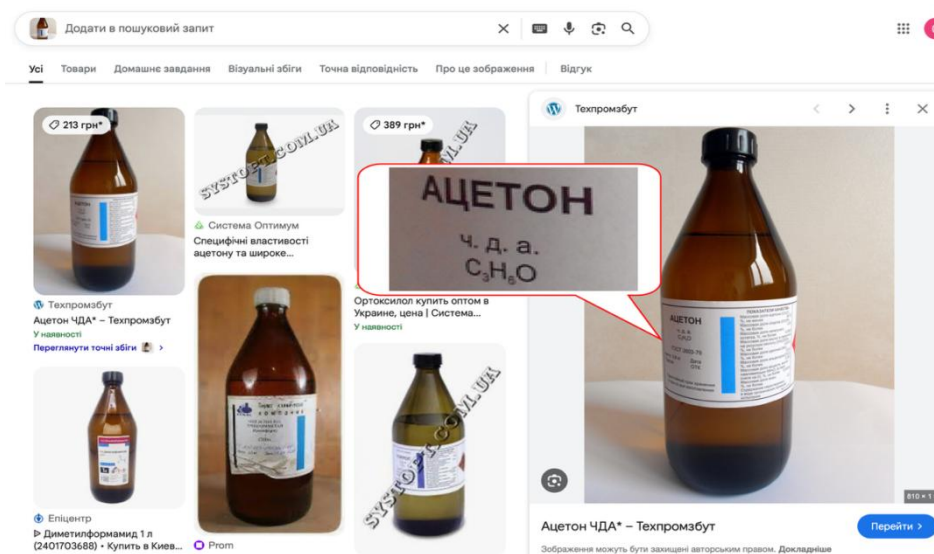
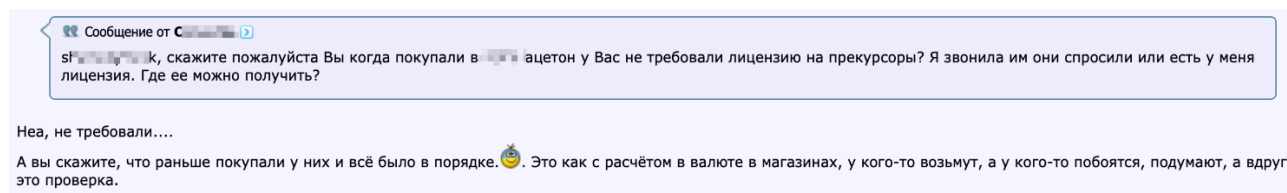


Рис. 2. Результат пошуку за зображенням

3) пошук за виробником та моніторинг спеціалізованих майданчиків. Дієвим підходом є комбінація загальної назви речовини та назви специфічного виробника (наприклад, «Купити ацетон техпромзбут»). Особливу увагу слід звертати на спеціалізовані майданчики та сайти оголошень (зокрема, flagma.ua), де фіксується значний масив торгівлі хімічними речовинами. Не менш важливим є аналіз спеціалізованих форумів, де часто обговорюються схеми придбання прекурсорів у ліцензіатів поза встановленим порядком відпуску (реалізації) таких речовин (рис. 3);



*Рис. 3. Результат вивчення одного з форумів*

4) аналіз месенджерів та залучення штучного інтелекту. У сучасних реаліях комунікація щодо збуту прекурсорів активно переміщується у закриті групи та канали месенджерів на кшталт Telegram. Для ефективного аналізу великих масивів неструктурованого тексту з чатів, виявлення прихованих патернів поведінки та ідентифікації сленгових назв прекурсорів можна використовувати інструменти на базі штучного інтелекту, які здатні виконувати роль автоматизованого аналітика даних.

Отже, протидія незаконному обігу прекурсорів у кіберпросторі вимагає від правоохоронних органів відмови від застарілих прямолінійних методів моніторингу. Ефективна ідентифікація злочинної діяльності можлива лише за умови комплексного застосування інструментів розвідки з відкритих джерел. Поєднання пошуку за хімічними формулами, візуального аналізу тари, глибинного моніторингу спеціалізованих форумів та месенджерів із залученням можливостей штучного інтелекту дозволяє суттєво підвищити результативність виявлення ланцюгів нелегального постачання сировини для виробництва наркотичних засобів.

### **Список використаних джерел**

1. Перелік наркотичних засобів, психотропних речовин і прекурсорів : затверджений постановою Кабінету Міністрів України від 06.05.2000 № 700. URL: <https://zakon.rada.gov.ua/laws/show/770-2000-п#Text> (дата звернення 25.04.2026).

2. Деякі питання ліцензування господарської діяльності з культивування рослин (крім конопель для промислових цілей, визначених Законом України «Про наркотичні засоби, психотропні речовини і прекурсори»), включених до таблиці I переліку наркотичних засобів, психотропних речовин і прекурсорів, затвердженого Кабінетом Міністрів України, розроблення, виробництва, виготовлення, зберігання, перевезення, придбання, реалізації (відпуску), ввезення на територію України, вивезення з території України, використання, знищення наркотичних засобів, психотропних речовин і прекурсорів, включених до зазначеного переліку : Постанова Кабінету Міністрів України від 06.04.2016 № 282. URL: <https://zakon.rada.gov.ua/laws/show/282-2016-п#Text> (дата звернення 25.04.2026).

**Мисик А. Б.,**  
професор кафедри управління,  
доктор військових наук, професор  
(*Національна академія Державної прикордонної  
служби України імені Б. Хмельницького*)

**Бурбела С. В.,**  
доцент кафедри загальновійськових дисциплін,  
доктор філософії в галузі військових наук  
(*Національна академія Державної прикордонної  
служби України імені Б. Хмельницького*)

## **МЕТОДИКА ОЦІНЮВАННЯ ОБСТАНОВКИ ШТАБОМ ПРИКОРДОННОГО ЗАГОНУ**

Охорона державного кордону потребує узгодженої та скоординованої діяльності різних органів державної влади, що володіють відповідними ресурсами, інформацією та повноваженнями у сфері охорони державного кордону. Побудова охорони державного кордону є визначальним елементом в діяльності системи забезпечення його безпеки. Її якість безпосередньо впливає на своєчасність реагування на загрози, ефективність використання сил і засобів, а також на рівень захищеності державного кордону.

У практиці роботи органів управління Держприкордонслужби України, як суб'єкта інтегрованого управління державним кордоном, має місце проблемна ситуація, яка визначається наявністю невідповідності між потребою комплексного моніторингу і оцінювання обстановки в інтересах побудови охорони державного кордону, оцінювання ризиків, які при цьому виникають, та суб'єктивним розумінням змісту та результатів такого оцінювання. Виникає потреба в узагальненні практики застосування існуючих підходів до аналізу та оцінювання обстановки в інтересах побудови охорони державного кордону, зокрема в період підготовки до оперативно-службової діяльності.

Інтегроване управління державним кордоном України ґрунтується на ризико-орієнтованих підходах. Відповідно до Стратегії національної безпеки України та Стратегії розвитку Державної прикордонної служби України одним із стратегічних напрямів розвитку системи забезпечення прикордонної безпеки є проведення аналізу ризиків, як основи прийняття рішень щодо мінімізації впливу наявних та потенційних загроз. Проектом Стратегії інтегрованого управління державним кордоном України визначено завдання впровадження передових методик здійснення всебічного моніторингу обстановки на державному кордоні.

Методика розроблена відповідно до Інструкції про службу прикордонних нарядів Державної прикордонної служби України [1], Порядку роботи органів управління Державної прикордонної служби України з підготовки до оперативно-службової діяльності в наступному календарному році або іншому періоді [2], Інструкції з проведення аналізу ризиків у Державній прикордонній службі України [3].

Методика забезпечує синергетичний ефект методик планування на основі спроможностей, аналізу ризиків, оперативно-тактичних розрахунків щодо оцінювання параметрів обстановки під час підготовки до оперативно-службової діяльності. Її методологічну

основу складає комплексний аналіз загроз прикордонній безпеці та показників спроможностей системи забезпечення охорони державного кордону. Аналіз ризиків у методиці розглядається як сукупність процедур і методів збору та оброблення інформації, одержаної з різних джерел, з метою визначення наявних та потенційно можливих ризиків у сфері прикордонної безпеки.

Штаб прикордонного загону оцінює рівень загроз прикордонній безпеці за моделлю CIRAM 2.0 [4]. Це дає можливість на аналітичному рівні виявити загрози та оцінити ризики, пояснити чому виникає ризик і в чому його сутність. Логіка аналітичного процесу на рівні прикордонного загону полягає у розумінні, яким чином параметри та сценарії загроз проявляються безпосередньо на державному кордоні. Оцінювання загроз відображається в матеріалах періодичних, тематичних та ситуативних аналізів, аналітичних, інформаційних зведеннях та інформаційних довідках. Мета оцінювання полягає в якісно-кількісному оцінюванні величини та імовірності загроз, формуванні та оцінюванні імовірності (пріоритетності) сценаріїв їх реалізації, оцінюванні впливу (можливих наслідків) реалізації загроз. Величина та імовірність загроз оцінюються на основі аналізу чинників, що їх визначають. В основу процедур оцінювання покладаються графічні та табличні методи, експертне оцінювання, статистичні методи, побудова вербально-числових шкал та метод аналізу ієрархій Сааті.

Модель аналізу загроз та ризиків представляє собою аналітичний рівень, а планування та оцінювання побудови охорони державного кордону – це механізм застосування результатів інформаційно-аналітичної роботи у практику прикордонної служби. Основними характеристиками сценаріїв загрози, що визначають побудову охорони державного кордону, є рівень оперативної активності правопорушників на окремих ділянках та імовірність використання правопорушниками певних маршрутів (напрямок) руху, які у сукупності визначають складність обстановки.

Результати аналізу та прогнозування можливих ділянок появи правопорушників, маршрутів їх ймовірного руху, прогнозування можливих способів перебування у контрольованому районі та перетинання кордону за напрямками та часом є підставою для прийняття рішень начальниками прикордонних підрозділів щодо визначення відповідних районів несення служби прикордонними нарядами, їх кількості та видів, формулювання часткових завдань щодо протидії правопорушникам та способів їх виконання у кожному районі (на кожному напрямку та маршруті). Визначальним показником якості побудови охорони державного кордону є імовірність виявлення та затримання правопорушника, яка розраховується для типового складу прикордонних нарядів.

Спроможності прикордонних підрозділів оцінюються за складовими: «бар'єрність» кордону, операційна здатність, ефективність оперативно-службової діяльності, стан нормативно-правового забезпечення. Оцінювання «бар'єрності» розглядається як оцінювання впливу на дії порушників фізико-географічних факторів та інженерного облаштування. Складовими оцінювання «операційної здатності» (спроможності) щодо протидії загрозам та впливу на чинники, які визначають рівень загроз та оперативну активність порушників на ділянках, є стан системи управління, укомплектованість та якісний стан особового складу, забезпеченість технікою та озброєнням, підготовленість підрозділів та органів управління, забезпеченість ресурсами тощо. Уразливість визначається як слабкі місця спроможностей.

Побудова охорони державного кордону вважається ефективною, якщо забезпечено відповідність імовірності виявлення правопорушників рівню складності обстановки, прогнозованим напрямкам зосередження основних зусиль, годинам доби (періодам) підвищення оперативної активності, своєчасне виявлення правопорушників на рубежах, що робить можливим їх затримання.

Працездатність методики експериментально перевірено на ділянці 24 прикордонного загону імені Героя України старшого лейтенанта В'ячеслава СЕМЕНОВА Південного регіонального управління.

#### **Список використаних джерел**

1. Інструкція про службу прикордонних нарядів Державної прикордонної служби України : Наказ МВС України від 19.10.2015 № 1261.
2. Порядок роботи органів управління Державної прикордонної служби України з підготовки до оперативно-службової діяльності в наступному календарному році або іншому періоді : Наказ Міністерства внутрішніх справ України від 26 квітня 2018 року № 350.
3. Інструкція з проведення аналізу ризиків у Державній прикордонній службі України : Наказ Міністерства внутрішніх справ України №1007 від 11 грудня 2017 року.
4. Посібник з аналізу ризиків за моделлю CIRAM 2.0 для аналітиків Державної прикордонної служби. Хмельницький : НАДПСУ. 2015. 136 с.

**Михаліцька Н. Я.,**

доцент кафедри менеджменту та економічної безпеки,  
кандидат наук з державного управління, доцент  
(*Львівський державний університет внутрішніх справ*)

**Яцик М. Р.,**

доцент кафедри менеджменту та економічної безпеки,  
кандидат педагогічних наук, доцент  
(*Львівський державний університет внутрішніх справ*)

## **ІНТЕГРАЦІЯ OSINT-АНАЛІТИКИ ТА ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В УПРАВЛІННЯ ЛЮДСЬКИМ КАПІТАЛОМ В УМОВАХ КРИЗОВИХ ТРАНСФОРМАЦІЙ**

Воєнні виклики суттєво трансформують умови функціонування ринку праці та підходи до управління людським капіталом. Повномасштабна війна в Україні супроводжується зростанням вимушеної трудової міграції, зміною структури зайнятості та посиленням невизначеності, що безпосередньо впливає на процеси формування та відтворення людського капіталу [1]. Особливої актуальності набуває проблема молодіжної міграції, яка зумовлює втрату кваліфікованого кадрового потенціалу та створює довгострокові ризики для економічної безпеки держави [2].

У контексті кризових трансформацій людський капітал доцільно розглядати як сукупність знань, компетентностей і професійних характеристик працівників, що визначають їхню здатність забезпечувати результативність діяльності організації. Управління людським капіталом поступово виходить за межі традиційних кадрових функцій і набуває стратегічного характеру, який орієнтований на забезпечення адаптивності персоналу та стійкості організації до динамічних змін зовнішнього середовища.

Під впливом трансформації ринку праці дедалі більшого значення набувають аналітичні підходи до управління персоналом. Зокрема, HR-аналітика виступає інструментом підвищення обґрунтованості управлінських рішень, оцінювання ефективності персоналу та переходу до data-driven підходів у кадровій політиці [3]. Застосування таких підходів часто обмежується внутрішніми даними організації, що ускладнює своєчасне врахування впливу зовнішнього середовища, у зв'язку з цим посилюється роль OSINT-аналітики як інструменту роботи з відкритими джерелами інформації. Аналіз відкритих даних дає змогу здійснювати моніторинг ринку праці, досліджувати міграційні процеси та виявляти соціально-економічні тенденції, що формують кадрові ризики [4-5]. Дослідження також підтверджують ефективність використання відкритих джерел для аналізу інформаційних загроз і соціальних процесів [6].

Ефективність обробки таких даних значною мірою забезпечується застосуванням технологій штучного інтелекту, які дають змогу систематизувати інформацію, виявляти закономірності та формувати прогностичні моделі розвитку кадрових процесів [3]. Варто наголосити, що використання технологій штучного інтелекту в управлінні персоналом вимагає врахування питань інформаційної безпеки, захисту персональних даних та етичних аспектів використання алгоритмічних рішень.

Таким чином, інтеграція HR-аналітики, OSINT-аналітики та технологій штучного інтелекту сприяє трансформації системи управління людським капіталом у багаторівневу аналітичну систему, орієнтовану на комплексне врахування внутрішніх і зовнішніх чинників

кадрової стійкості та підвищення адаптивності організацій в умовах кризових трансформацій. Для розвитку такого підходу доцільним є синергетичне поєднання інструментарію HR-аналітики, OSINT-аналітики та технологій штучного інтелекту в межах єдиної системи управління людським капіталом.

З урахуванням зазначених підходів запропоновано систему аналітичного управління людським капіталом (рис. 1), яка відображає взаємозв'язок аналітичних рівнів, джерел даних та механізмів ухвалення управлінських рішень.



Рис. 1. Система аналітичного управління людським капіталом на основі OSINT-аналітики та технологій штучного інтелекту

*Джерело: розроблено авторами*

Запропонована система відображає логіку узгодження зовнішніх і внутрішніх даних у процесі управління людським капіталом та демонструє комплексний підхід до його реалізації в умовах воєнних викликів. Вона передбачає об'єднання зовнішніх і внутрішніх інформаційних потоків у єдину аналітичну систему, ключовою особливістю якої є використання відкритих джерел інформації поряд із традиційними HR-даними, що дає змогу комплексно враховувати зміни ринку праці та міграційні процеси.

Інтеграція OSINT-аналітики з внутрішніми HR-даними та їх обробка із застосуванням технологій штучного інтелекту дають змогу формувати прогностні моделі розвитку кадрових процесів, своєчасно виявляти кадрові ризики та підвищувати обґрунтованість управлінських рішень. У результаті формується прогностно-орієнтована система управління людським капіталом, здатна забезпечувати адаптивність, кадрову стійкість і підтримання безперервності діяльності організації в умовах кризових трансформацій.

#### **Список використаних джерел**

1. Азьмук Н. А. Трансформація ринку праці в умовах війни: виклики та стратегії відтворення робочої сили. *Вісник економічної науки України*. 2022. № 1 (42). С. 171–179. DOI: [https://doi.org/10.37405/1729-7206.2022.1\(42\).171-179](https://doi.org/10.37405/1729-7206.2022.1(42).171-179)
2. Михаліцька Н. Я., Верескля М. Р., Караїм О. О. Молодіжна міграція в умовах російсько-української війни: ризики та загрози національній безпеці. *Науковий вісник Львівського державного університету внутрішніх справ. Серія економічна*. 2022. № 2. С. 24–33. URL: <https://nvlvduvs.edu.ua/index.php/economy/article/view/118>
3. Грідін О. (2024). HR-аналітика як ключовий інструмент системи управління персоналом сучасної організації. *Економіка та суспільство*. № (62). URL: <https://doi.org/10.32782/2524-0072/2024-62-29>
4. Ревак І., Підхомний О., Чубаєвський В. Електронні документи як ресурси для соціологічних досліджень рівня безпеки фінансово-правових відносин. *Соціально-правові студії*. 2024. № 7(1). С. 273–282. URL: <https://doi.org/10.32518/sals1.2024.273>
5. Пучков О., Ланде Д., Субач І., Болюх М., Нагорний Д. OSINT-розслідування для виявлення та запобігання кібератак та інцидентів кібербезпеки. *Збірник «Інформаційні технології та безпека»*. 2021. № 9 (2). С. 209–218. URL: <https://doi.org/10.20535/2411-1031.2021.9.2.249921>
6. Думчиков М. О. Відкрита розвідка (OSINT) у протидії інформаційним загрозам. *Актуальні проблеми права та державного управління*. 2025. DOI: <https://doi.org/10.24144/2788-6018.2025.06.2.43>

**Мовчан А. В.,**  
професор кафедри оперативно-розшукової діяльності,  
доктор юридичних наук, професор  
(Львівський державний університет внутрішніх справ)

## **НАПРЯМИ ВИКОРИСТАННЯ OSINT У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ ТА ЗАБЕЗПЕЧЕННІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ**

У сучасному світі інформація стала одним із ключових ресурсів, що визначає ефективність державного управління, правоохоронної діяльності та системи національної безпеки. Стрімка цифровізація, розвиток соціальних мереж і глобалізація інформаційного простору створили нові можливості для збору та аналізу даних.

У цих умовах особливого значення набуває OSINT (Open Source Intelligence) – розвідка на основі відкритих джерел. Для України роль OSINT суттєво зросла після анексії Криму росією та особливо після повномасштабного вторгнення росії в Україну. Відкриті джерела стали важливим інструментом як для державних органів, так і для громадянського суспільства у протидії загрозам національній безпеці.

OSINT – це процес збору, обробки та аналізу інформації, що знаходиться у відкритому доступі, з метою отримання розвідувальних даних. Основними джерелами OSINT є: соціальні мережі (Facebook, X/Twitter, Telegram, TikTok); засоби масової інформації; державні реєстри; супутникові знімки; геолокаційні дані; форуми, блоги, відкриті бази даних; мультимедійний контент (фото, відео, стріми). Особливістю OSINT є те, що він базується виключно на легально доступній інформації, що значно спрощує його використання в правоохоронній діяльності та судовому процесі.

У правоохоронній сфері OSINT виконує широкий спектр функцій – від збору доказів до аналізу складних кримінальних зв'язків. Одним із найбільш відомих прикладів застосування OSINT є розслідування катастрофи рейсу MH17. Завдяки аналізу фото і відео з відкритих джерел було встановлено маршрут пересування зенітно-ракетного комплексу «Бук» та ідентифіковано причетні військові підрозділи РФ. Важливу роль у цьому відіграли аналітики Bellingcat, які довели ефективність відкритих даних у міжнародних розслідуваннях [1].

Відтак, OSINT активно використовується для: документування злочинів через аналіз відео та фото; ідентифікації осіб за цифровими слідами; перевірки алібі та встановлення хронології подій; аналізу соціальних зв'язків між фігурантами справ.

Особливої актуальності ці інструменти набули під час розслідування подій, пов'язаних із бойовими діями, зокрема після звільнення Бучі, де відкриті джерела дозволили встановити причетних осіб і підтвердити факти вчинення злочинів російськими військовослужбовцями.

Водночас у сфері протидії кіберзлочинності OSINT застосовується для виявлення шахрайських схем, аналізу витоків даних та ідентифікації хакерських груп. Наприклад, через аналіз відкритих цифрових слідів було встановлено діяльність групи Fancy Bear. Група Fancy Bear (також відома як APT28, Sofacy, Sednit) – це одна з найвідоміших кіберрозвідувальних груп, яку пов'язують із російськими державними структурами, зокрема з військовою

розвідкою ГРУ. Основна діяльність – це кібершпигунство та інформаційні операції. Їхні цілі зазвичай пов'язані з політикою, безпекою та міжнародними відносинами [2].

OSINT відіграє ключову роль у фіксації воєнних злочинів після повномасштабного вторгнення росії в Україну, зокрема: документування обстрілів цивільних об'єктів через відео очевидців; аналіз супутникових знімків для виявлення руйнувань; встановлення типів озброєння; створення хронології подій. Реальні приклади демонструють, що OSINT: дозволяє встановлювати істину навіть у складних міжнародних конфліктах; забезпечує доказову базу, прийнятну на міжнародному рівні; підсилює спроможності правоохоронних органів без значних ресурсних витрат; сприяє притягненню винних до відповідальності. Відтак, OSINT перестає бути допоміжним інструментом і стає невід'ємною частиною сучасної системи безпеки та правосуддя.

У сфері національної безпеки OSINT став одним із ключових інструментів протидії сучасним загрозам. *По-перше*, він дозволяє виявляти військові загрози. Напередодні повномасштабного вторгнення росії в Україну аналітики фіксували концентрацію військ РФ біля кордонів України на основі супутникових знімків і публікацій у соціальних мережах. *По-друге*, OSINT відіграє важливу роль у боротьбі з дезінформацією. Завдяки перевірці джерел, геолокації відео та аналізу контенту вдається викривати фейки та інформаційні маніпуляції, зокрема використання старих відео з інших конфліктів.

Окремим напрямом є виявлення бот-мереж і координованих інформаційних кампаній. Аналіз поведінки акаунтів, синхронності публікацій і структури взаємодій дозволяє викривати організовані мережі, пов'язані, зокрема, з Internet Research Agency. У контррозвідувальній діяльності OSINT допомагає: ідентифікувати агентів впливу; виявляти колаборантів; аналізувати зв'язки між підозрілими особами [3].

Важливим феноменом є розвиток громадянського OSINT. Українські громадяни та волонтери активно долучаються до збору й аналізу інформації, що суттєво підсилює державні інституції.

На міжнародному рівні OSINT використовується для документування воєнних злочинів і формування доказової бази для судових інстанцій, що сприятиме притягненню винних до відповідальності.

Основними перевагами OSINT сьогодні є: доступність і низька вартість; оперативність отримання інформації; можливість обробки великих масивів даних; легальність використання; ефективність у складних умовах війни.

Крім того, OSINT дозволяє значно скоротити час розслідувань і підвищити їхню результативність.

Натомість, попри значний потенціал, використання OSINT супроводжується певними труднощами, а саме: надлишок інформації; ризик використання недостовірних даних; складність верифікації; інформаційні маніпуляції; правові та етичні питання. Ці виклики потребують розвитку методів перевірки інформації та підготовки кваліфікованих спеціалістів. Подальший розвиток OSINT в Україні передбачає: інтеграцію у діяльність правоохоронних органів; розвиток освітніх програм; використання штучного інтелекту; створення аналітичних платформ; міжнародне співробітництво. Водночас поєднання OSINT із сучасними технологіями відкриває нові можливості для забезпечення безпеки держави [4].

Отже, OSINT сьогодні є не просто допоміжним інструментом, а повноцінним елементом системи правоохоронної діяльності та національної безпеки. Його ефективність підтверджується як міжнародними розслідуваннями, так і практикою України в умовах війни. Використання відкритих джерел дозволяє оперативно виявляти загрози, документувати злочини та протидіяти інформаційним атакам. У сучасних умовах саме поєднання технологій, аналітики та громадянської участі формує нову модель безпеки держави.

#### **Список використаних джерел**

1. MH17 – The Open Source Evidence. URL: [https://www.bellingcat.com/news/2015/10/08/mh17-the-open-source-evidence/?utm\\_source=chatgpt.com](https://www.bellingcat.com/news/2015/10/08/mh17-the-open-source-evidence/?utm_source=chatgpt.com)
2. Аналітики виявили ще одну групу хакерів із РФ, які намагаються зламати комп'ютери дипломатів. URL: <https://www.ukrinform.ua/rubric-ato/3891491-analitiki-viavili-se-odnu-grupu-hakeriv-iz-rf-aki-namagautsa-zlamati-komputeri-diplomativ.html>
3. OSINT Open Source Intelligence. Теорія та методологія : монограф. / О. Користін, С. Демедюк, О. Барановський, Д. Ланде та ін. ; за заг. ред. О. Є. Користіна, С. В. Демедюка. Київ : 7БЦ, 2025. 304 с.
4. Басалик С. А., Туз О. С., Тищук В. В. Генезис інструментів OSINT та окремі аспекти їх використання у правоохоронній діяльності. *Український політико-правовий дискурс*. 2025. № (9). URL: <https://doi.org/10.5281/zenodo.15086041>

**Овдійчук Д. Е.,**  
здобувач вищої освіти  
(Львівський державний університет внутрішніх справ)

**Гуцуляк Ю. В.,**  
доцент кафедри кримінального процесу,  
доктор філософії  
(Львівський державний університет внутрішніх справ)

## **ЗАСТОСУВАННЯ МЕТОДІВ OSINT У ДОСУДОВОМУ РОЗСЛІДУВАННІ**

Цифровізація суспільства стосується всіх без винятку сфер суспільства. Особливості «цифрового століття» мають значний вплив і на правовідносини, зокрема, це стосується і сфери кримінальної юстиції. Одним з ключових чинників, які необхідно враховувати у зв'язку з цим, є збільшення числа віртуальних (електронних) слідів взаємодії суб'єктів вчинення кримінального правопорушення та слідів вчинення кримінального правопорушення. у зв'язку з цим виникає необхідність вивчення змісту та правового врегулювання інструментарію та предмету дослідження таких наслідків, з метою повного, неупередженого, швидкого та всебічного розслідування кримінальних правопорушень.

Вважаємо за необхідне зазначити, що 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. Основна мета OSINT – зібрати релевантну інформацію для подальшої оцінки та прийняття рішень. Цей підхід застосовується в різних сферах, включаючи правоохоронну діяльність, розвідку, бізнес-аналітику, кібербезпеку та інші. В сучасних умовах, коли значна кількість інформації публікується онлайн, OSINT стає важливим інструментом для здійснення різних видів аналізу та досліджень, при розслідуванні кримінальних правопорушень, що відповідно до Закону віднесені до підслідності Національної поліції України [1 с. 221–222].

Проте, існує проблема захисту персональних даних під час використання відкритої інформації, оскільки це може призвести до витоку персональних даних особи, що в подальшому негативно вплине на хід розслідування. Для цього необхідно закріпити на законодавчому рівні межі втручання у приватне життя особи під час застосування таких методів. Недостатня увага до цього аспекту може призвести до ризиків, пов'язаних із порушенням прав людини. Наразі відсутні чіткі правові норми, що регламентують застосування відкритої інформації під час досудового розслідування, а також інших стадій кримінального процесу. Такі прогалини у нормативно-правовому регулюванні в Україні обумовлені відсутністю ретроспективного та теоретичного підходу до цієї проблематики, що пов'язано зі стрімким розвитком технологій, які значно випереджають правозастосовні можливості існуючих правових норм. Невирішені питання щодо використання OSINT мають безпосередній вплив на розвиток законодавства та впровадження відповідних інструментів. Для регулювання цієї сфери необхідно забезпечити баланс між підвищенням ефективності правоохоронної діяльності та захистом основних прав і свобод громадян [2].

У контексті проведення слідчих (розшукових) дій важливим є огляд веб-сторінок, груп та каналів у месенджерах, а також соціальних мережах, що ефективно зробити за допомогою інструментарію OSINT, адже саме ці дані дозволяють отримати інформацію, яка у сукупності із показаннями свідків в подальшому сформує доказову базу під час здійснення досудового розслідування конкретного кримінального провадження.

Під час здійснення досудового розслідування кримінальних проваджень, необхідну інформацію про вчинене кримінальне правопорушення, або особу (осіб), яка його вчинила, її соціальні зв'язки, будь-які інші відомості, які можна в подальшому використати для доведення винуватості тощо, можна отримати із відкритих джерел та публічно доступних відомостей, а саме: 1) мережі Інтернет, яка включає в собі безліч платформ, наприклад, форуми, блоги, соціальні мережі, сайти, пошукові системи тощо; 2) дипломатичних місій; 3) релігійні організації; 4) розвідувальні організації загальнонаціонального рівня; 5) академічний напрямок, наприклад, дисертації, дослідження тощо; 6) архіви (бібліотеки) та дослідницькі центри; 7) «сіра література» (в даному випадку маються на увазі – наукові доповіді, економічні звіти, маркетингові дослідження тощо). Тобто, досліджувана нами методика OSINT має великий спектр можливих технологій, які досить ефективно використовуються під час проведення слідчих (розшукових) дій [3, с.1275].

Ми вважаємо, що інструменти OSINT у досудовому розслідуванні можна ефективно використовувати виключно під час проведення слідчих (розшукових) дій. Доречно буде використати ці інструменти у підготовчому етапі до проведення допиту, проаналізувавши інформацію про особу у відкритих джерелах слідчий зможе підготувати конкретні запитання спираючись уже на попередньо отриману інформацію, а також виявити розбіжності між показаннями та наявною інформацією. Інструмент Foto Forensics доречно використати для Інструмент Foto Forensics доречно використати для попереднього аналізу цифрових зображень, зокрема з метою виявлення ознак їх можливого редагування (наприклад, за допомогою Error Level Analysis), що дозволяє оцінити автентичність наданих матеріалів і сформулювати уточнюючі запитання під час допиту щодо походження, часу та обставин створення відповідного зображення, що може замінити проведення експертизи. Під час проведення слідчого експерименту інструменти OSINT можуть використовуватися як допоміжний засіб для відтворення обстановки та обставин події на основі відкритих джерел. Зокрема, аналіз картографічних сервісів, фото, відеоматеріалів дає змогу уточнити розташування об'єктів, особливості місцевості та можливість здійснення певних дій у конкретному місці. Крім того, за допомогою відкритих даних можна перевірити умови видимості, освітлення та погодні фактори на момент події. OSINT також сприяє геолокаційній верифікації, дозволяючи підтвердити або спростувати місце перебування особи. Використання таких інструментів допомагає більш точно змодельовати умови експерименту та перевірити показання. Водночас отримана інформація має допоміжний характер і підлягає обов'язковій перевірці у процесуальному порядку.

Використання інструментів OSINT під час здійснення досудового розслідування можливе лише за умови, непорушності конституційного права особи на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції (стаття 31 Конституції України).

Отже, застосування методів OSINT у досудовому розслідуванні є ефективним інструментом отримання та аналізу інформації з відкритих джерел, що сприяє підвищенню якості та оперативності слідчих (розшукових) дій. Використання таких інструментів дозволяє поглибити підготовку до процесуальних дій, перевірити достовірність відомостей та сформулювати обґрунтовану доказову базу. Водночас застосування OSINT потребує чіткого нормативно-правового регулювання та обов'язкового дотримання прав і свобод людини, зокрема права на приватність. Таким чином, подальший розвиток і впровадження OSINT має здійснюватися з урахуванням балансу між ефективністю правоохоронної діяльності та гарантіями конституційних прав громадян.

### **Список використаних джерел**

1. Дерев'ягін О. Використання OSINT інструментарію при розслідуванні кримінальних правопорушень проти власності. *СБУ в умовах війни в Україні: сучасні реалії та інноваційні стратегії забезпечення національної безпеки*. 2024. С. 221–225.
2. Басалик С.А, Туз О.С, Тищук В.В. Генезис інструментів OSINT та окремі аспекти їх використання у правоохоронній діяльності. *Український політико-правовий дискурс*. 2025. DOI <https://doi.org/10.5281/zenodo.15086041> (дата звернення: 14.04.2026).
3. Мельник А. М, Кисельов А. О. Використання OSINT технологій під час проведення слідчих (розшукових) дій. *Modern problems of Science, Education and Society*. 2024. С. 1274–1277. URL: <https://dspace.uzhnu.edu.ua/bitstreams/77edfb02-8b6e-43a8-b1be-55c5af899ef0/download#page=1274> (дата звернення: 14.04.2026).

**Пацула О. І.,**  
заступник директора з освітньої  
та науково-дослідної діяльності ННГУПБ,  
кандидат економічних наук, доцент  
*(Львівський державний університет внутрішніх справ)*

## **АНАЛІТИЧНИЙ ПОТЕНЦІАЛ ВІДКРИТИХ ДЖЕРЕЛ У ПРОТИДІІ ФІНАНСОВИМ ПРАВОПОРУШЕННЯМ**

Сучасні фінансові правопорушення набувають дедалі більш складних транснаціональних і цифровізованих форм. Використання електронних сервісів, криптовалют, підставних компаній та багаторівневих фінансових схем ускладнює їх виявлення традиційними методами розслідування. Поряд з тим, значний обсяг інформації про економічну діяльність суб'єктів господарювання залишається у відкритому доступі. Це формує нові можливості для аналітичної роботи на основі відкритих джерел, що у міжнародній практиці визначається як OSINT – Open Source Intelligence.

Застосування OSINT у сфері протидії фінансовим правопорушенням дозволяє ефективно поєднувати швидкість отримання даних, їхню різноманітність та аналітичну глибину, що робить його – важливим інструментом сучасного фінансового контролю.

Питання використання OSINT протягом останнього періоду стало предметом дослідження серед науковців та практиків, зокрема: Басистої І.В., Гаврилук Л. В. [1], Дикого О.В. [2], Гловюк І.В. [3], Підхомного О.М., Ревак І.О. [4], Мовчана А.В., Федчака І.А. [5] та ін. Багато публікацій присвячено юридичним та правовим аспектам вивчення цього питання.

Метою нашого дослідження є розкриття аналітичного потенціалу відкритих джерел інформації та визначення їх ролі у виявленні, аналізі та запобіганні фінансовим правопорушенням.

OSINT об'єднує у собі систему методів і засобів збору, обробки, аналізу та інтерпретації інформації, отриманої з відкритих джерел з метою формування аналітичних висновків і підтримки процесу прийняття рішень. Його концептуальну основу становить інформаційно-аналітична діяльність, що передбачає комплексне використання відкритих інформаційних ресурсів у межах правового поля. Як зазначають у своїй публікації автори Басиста І., Гаврилук Л. та ін.: «Розвідка за відкритими джерелами (OSINT) може бути застосовною для вирішення питання про вжиття заходів забезпечення безпеки (захисту свідків), як довідкова інформація для прийняття рішень, відшукування прихованих активів, які мали б бути обкладені санкціями тощо» [1]. Теоретичне підґрунтя застосування OSINT ґрунтується на міждисциплінарному поєднанні методів інформаційного аналізу, кібербезпеки, комунікаційних технологій та прикладної аналітики. Важливе значення при цьому має верифікація даних, яка передбачає перевірку достовірності інформації шляхом порівняння декількох незалежних джерел. Однією з ключових проблем застосування OSINT є надлишковість інформаційних потоків, що ускладнює процес відбору релевантних і достовірних даних.

Аналітичний потенціал відкритих джерел полягає у можливості комплексного аналізу економічної поведінки суб'єктів господарювання. В цьому контексті інформація з відкритих джерел дозволяє встановити зв'язки між суб'єктами, що дає змогу виявити мережі пов'язаних компаній, які можуть реалізовуватися для реалізації схем ухилення від

оподаткування або відмивання коштів. Такі джерела інформації відносять до ідентифікаційних, тобто тих, які забезпечують встановлення основних відомостей про контрагентів – юридичний статус, структуру власності, бенефіціарів, географію діяльності та участь у міжнародних ланцюгах постачання. Їх використання дозволяє виявляти потенційні зв'язки із підсанкційними структурами на початковому етапі аналізу ризиків [4]. Власне, головними індикаторами ризикової діяльності можуть стати: динаміка змін статутного капіталу; частота змін керівництва; участь у державних закупівлях; судові спори та виконавчі провадження; реєстрація різних юридичних осіб за однією адресою; відсутність реальної господарської діяльності; наявність так званих «номінальних» керівників.

Використання OSINT інструментів у фінансово-контрольній та правоохоронній діяльності забезпечує оперативність отримання інформації без запиту до закритих джерел. Особливо ефективним стає його застосування на етапі первинної перевірки інформації, коли необхідно швидко оцінити ризиковість суб'єкта господарювання, а також як доповнення доказової бази у кримінальних провадженнях.

Попри значні переваги, варто сказати і про деякі обмеження у використанні OSINT, серед них: рівень достовірності інформації в контексті застарілості даних, навмисно викривленої інформації та отримання фрагментарних відомостей; юридична придатність, адже далеко не вся інформація, отримана через OSINT може бути використана як процесуальний доказ і здебільшого вимагає додаткової верифікації; використання відкритих даних повинно враховувати баланс між розслідуванням та захистом персональних даних.

Підсумовуючи, зазначимо, що аналітичний потенціал відкритих джерел є одним із ключових інструментів сучасної системи протидії фінансовим правопорушенням. Проте, його ефективність залежить від рівня підготовки спеціалістів, їх володіння аналітичними навиками, перевірки джерел та критичного мислення. Подальший розвиток OSINT-методик, автоматизація обробки даних та інтеграція з аналітичними платформами сприятимуть посиленню фінансової безпеки держави та підвищенню якості розслідувань у сфері економічної злочинності.

### Список використаних джерел

1. Басиста І. В., Гаврилюк Л. В., Гутник А. В., Хитра А. Я. Використання цифрових даних з відкритих джерел під час розслідування кримінальних правопорушень: окремі аспекти. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія: Право.* 2024. Вип. 17. С. 227–243. DOI: <https://doi.org/10.33098/2078-6670.2024.17.29.227-243>.
2. Дикий О. В., Сидорчук В. В. Поняття OSINT та суміжні категорії. *Юридичний науковий електронний журнал.* 2024. № 9. С. 332–335. URL: [https://lsei.org.ua/9\\_2024/80.pdf](https://lsei.org.ua/9_2024/80.pdf).
3. Гловюк І. В. Оцінка результатів OSINT у судовій практиці: окремі питання. *Науковий вісник Ужгородського національного університету.* Серія: Право. 2025. Вип. 91. Ч. 4. С. 251–259. DOI: <https://doi.org/10.24144/2307-3322.2025.91.4.35>.
4. Ревак І. О., Підхонний О. М. Відкриті джерела інформації в управлінні корпоративним санкційним компласом логістичних підприємств. *Науковий вісник ЛьвДУВС.* 2025. № 2. С. 48–54. URL: <https://dspace.lvduvs.edu.ua/bitstream/1234567890/9280/1/%D0%A0%D0%B5%D0%B2%D0%B0%D0%BA.pdf>.
5. Мовчан А. В., Шляховський О., Козій В. В., Федчак І. А. Розслідування злочинів про фінансування криптовалютою тероризму та збройної агресії. *Соціально-правові студії.* 2023. Т. 6. № 4. С. 123–131. URL: <http://analyticbase.nlu.org.ua/?arg5=OSINT>.

**Перемибіда Д. О.,**  
начальник науково-дослідної лабораторії СОП  
(*Національна академія сухопутних військ  
імені гетьмана Петра Сагайдачного*)

**Перемибіда І. В.,**  
старший викладач кафедри управління  
повсякденною діяльністю підрозділів  
(*Національна академія сухопутних військ  
імені гетьмана Петра Сагайдачного*)

## **ВАЖЛИВІСТЬ ДОСЛІДЖЕННЯ ВІДКРИТИХ ДЖЕРЕЛ У КОНТЕКСТІ ВЖИТТЯ ЗАХОДІВ КОНТР-OSINT**

Широке визнання OSINT як ефективного методу збору розвідувальної інформації закономірно спонукає суб'єктів, які становлять інтерес для аналітиків, до вжиття заходів протидії – так званого контр-OSINT. У контексті повномасштабної війни між російською федерацією та Україною протиборство у відкритому інформаційному просторі набуває стратегічного виміру: одночасно з нарощуванням потенціалу власних OSINT-підрозділів, ворожа сторона систематично реалізує комплекс заходів, спрямованих на унеможливлення або дискредитацію розвідувальної діяльності на основі відкритих джерел. Дослідження відкритих джерел в умовах активної протидії є самостійним і малодослідженим напрямом аналітичної роботи, який потребує виокремлення специфічних методологічних підходів.

Контр-OSINT (Counter-OSINT) – це сукупність технічних, організаційних та інформаційних заходів, спрямованих на обмеження або нейтралізацію можливостей противника щодо збору, верифікації та аналізу розвідувальних даних із відкритих джерел [1]. На даний час виділяють три основні категорії контр-OSINT. Перша – заходи обмеження доступу до інформації: геоблокування ресурсів, закриття акаунтів у соціальних мережах, видалення публічних реєстрів, встановлення обмежень на індексування вебсторінок пошуковими системами. Друга – заходи дезінформації та цифрового камуфляжу: свідоме поширення хибних або маніпулятивних даних у відкритому просторі з метою введення аналітиків в оману. Третя – технічний захист цифрового сліду: видалення метаданих із опублікованих файлів, використання засобів анонімізації, застосування процедур цифрової гігієни в підконтрольних медіаструктурах.

Характерним прикладом системних контр-OSINT-заходів є практика збройних сил та спецслужб росії, задокументована після 2022 року. Зокрема, було запроваджено жорсткі обмеження на публікацію особовим складом будь-якого контенту, пов'язаного зі службовою діяльністю; здійснювались масові видалення геотегованих публікацій у соціальних мережах та зачищення акаунтів військовослужбовців; застосовувалось цілеспрямоване поширення фейкових координат та дезінформації щодо дислокації військових підрозділів [2]. Водночас ці заходи виявились лише частково ефективними, оскільки OSINT-аналітики виробили методи подолання кожного з них.

Ефективне дослідження відкритих джерел в умовах контр-OSINT спирається на кілька ключових методологічних принципів. Принцип крос-верифікації передбачає обов'язкове підтвердження будь-якої значущої інформації з незалежних джерел різної природи. Якщо противник здійснює дезінформаційну операцію, вміло сфабриковані матеріали, як правило, не витримують зіставлення з геопросторовими даними, сигналами радіоелектронної розвідки чи свідченнями незалежних очевидців. Перехресна верифікація є головним методологічним щитом проти навмисних маніпуляцій у відкритому просторі [3].

Принцип архівування та темпорального аналізу полягає у збереженні первинних цифрових артефактів до їх можливого видалення та відстеження динаміки змін інформаційного сліду об'єкта дослідження. Безумовно видалення публікацій і акаунтів є характерним індикатором усвідомленого застосування контр-OSINT, тоді як порівняльний аналіз архівних та актуальних версій ресурсів (із залученням Wayback Machine, CachedView та аналогічних інструментів) дозволяє відновлювати видалений контент та виявляти закономірності в поведінці об'єкта. Цей підхід довів свою ефективність під час дослідження характеру переміщень ворожих підрозділів, коли видалені публікації вдавалось відновити через кеші пошукових систем [4].

Принцип пасивного збору даних передбачає мінімізацію активних взаємодій із досліджуваними ресурсами – уникнення підписок, реакцій та прямих запитів, що можуть сигналізувати об'єкту дослідження про інтерес з боку аналітика. Для цього застосовуються спеціалізовані інструменти пасивної розвідки, VPN-сервіси та операційна безпека (OPSEC) аналітика. Активний моніторинг об'єкта може спровокувати його перехід до більш жорстких заходів захисту цифрового сліду або підштовхнути до реалізації операцій введення в оману, спрямованих безпосередньо проти OSINT-дослідника.

Особливу складність становить верифікація контенту в умовах цілеспрямованої дезінформаційної операції, коли противник свідомо наповнює відкритий простір фабрикатами, розрахованими на виявлення OSINT-аналітиками. Такі «медові пастки» (honeypots) можуть містити правдоподібні, але хибні геолокаційні мітки, сфальсифіковані документи або скомпрометовані акаунти нібито достовірних джерел. Протидія цьому типу контр-OSINT вимагає розвинутих навичок аналізу метаданих, обізнаності з типовими патернами дезінформаційних операцій та критичного ставлення до надто «очевидних» або легкодоступних даних [5].

Таким чином, дослідження відкритих джерел в умовах вжиття заходів контр-OSINT є самостійним науково-практичним напрямом, що потребує розвитку спеціалізованої методології. Ефективна протидія контр-OSINT-заходам ворога забезпечується комплексним застосуванням крос-верифікації, темпорального аналізу, пасивних методів збору та критичної оцінки достовірності джерел. Для підвищення спроможності українських OSINT-підрозділів у цій сфері необхідне: чітке формування спеціалізованих навчальних програм із протидії контр-OSINT; розроблення методичних рекомендацій щодо виявлення дезінформаційних операцій; налагодження обміну досвідом між аналітичними спільнотами та державними структурами. Усе це є важливою складовою зміцнення розвідувально-аналітичного потенціалу України в умовах тривалого гібридного протистояння.

#### **Список використаних джерел**

1. Hassan N., Hijazi R. Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence. Apress, 2018. 371 p.
2. Watling J., Reynolds N. Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine. Royal United Services Institute (RUSI), 2023. 56 p.
3. Chaslot G. How Algorithms Can Learn to Discredit the Media. The Guardian. 2018. URL: <https://www.theguardian.com/technology/2018/feb/02/how-youtubes-algorithm-distorts-truth> (дата звернення: 12.04.2025).
4. Toler A. How to Use the Wayback Machine for OSINT Research. Bellingcat. 2022. URL: <https://www.bellingcat.com/resources/how-tos/2022/01/18/using-the-wayback-machine> (дата звернення: 12.04.2025).
5. Hutchins E. M., Cloppert M. J., Amin R. M. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Proceedings of the 6th International Conference on Information Warfare and Security. 2011. P. 113–125.

**Пилипенко Є. О.,**  
старший науковий співробітник  
науково-дослідної лабораторії  
з актуальних питань кримінального аналізу  
навчально-наукового інституту підготовки фахівців  
для підрозділів кримінальної поліції  
Національної поліції України,  
кандидат юридичних наук, старший дослідник  
(*Одеський державний університет внутрішніх справ*)

## **ЩОДО ВИКОРИСТАННЯ OSINT ПІД ЧАС РОЗШУКУ ВОЄННИХ ЗЛОЧИНЦІВ**

Відповідно до ст. 438 Кримінального кодексу України (КК України) воєнними злочинами визнаються такі суспільно небезпечні протиправні діяння: жорстоке поводження з військовополоненими або цивільним населенням, вигнання цивільного населення для примусових робіт, розграбування національних цінностей на окупованій території, застосування засобів ведення війни, заборонених міжнародним правом, незаконне переміщення або депортація дитини, невинуватого затримка репатріації дитини, вербування або використання дитини для участі у збройному конфлікті, воєнних (бойових) діях, інші порушення законів та звичаїв війни, що передбачені міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України, а також віддання наказу про вчинення таких дій (ч. 1), а також ті самі діяння, якщо вони спричинили загибель людини (ч. 2) [1].

Даний вид кримінального правопорушення згідно із класифікацією, наданою у ст. 12 КК України, є особливо тяжким злочином, адже за його вчинення передбачене покарання у вигляді позбавлення волі на строк від восьми до дванадцяти років (ч. 1 ст. 438 КК України) та позбавлення волі на строк від десяти до п'ятнадцяти років або довічне позбавлення волі (ч. 2 ст. 438 КК України) [1].

Величезну допомогу у розшуку осіб, що вчинили воєнні злочини на території України займає використання розвідки на основі відкритих джерел (Open Source Intelligence, OSINT), що передбачає збір, аналіз відкритої доступної інформації: соціальних мереж, новин, супутникових знімків тощо. Це дає можливість дослідникам виявляти обставини, місце та час скоєння правопорушення. За допомогою різноманітних інструментів та методів OSINT-аналітики особи, що здійснюють дослідження можуть зібрати та проаналізувати дані, щоб допомогти в ідентифікації злочинців [2].

Так, основними напрямками використання OSINT під час розшуку воєнних злочинців та розкриття воєнних злочинів є [3]:

- ідентифікація осіб. Аналітики використовують соціальні мережі (VK, Telegram, Instagram) для встановлення особистих даних воєнних злочинців, їхніх військових частин та посад. Тільки протягом 2022–2023 років за допомогою соціальних мереж ідентифікували 182 тисячі російських воєнних злочинців, причетних до війни в Україні [4].

- геолокація та хронологія. За допомогою супутникових знімків можна точно визначити місце та час скоєння воєнного злочину, спростовуючи фейкові нарративи.

- документування руйнувань, у тому числі будівель, що становлять національну цінність. Відкриті дані дозволяють оцінити масштаби атак та руйнувань, завдані збитки культурній спадщині.

- створення цифрових профілів. OSINT допомагає розкрити не лише дії окремих «гвинтиків», а й структуру всієї системи, що віддавала злочинні накази [3].

Отже, використання OSINT є критично важливим для пошуку воєнних злочинців, оскільки цей метод дозволяє перетворювати величезні масиви публічних даних на юридично значущі докази задля того, щоб кожний воєнний злочинець на території України поніс справедливе неминуче заслужене покарання за вчинення суспільно небезпечних протиправних діянь, передбачених ст. 438 КК України.

### **Список використаних джерел**

1. Кримінальний кодекс України : Закон України від 05.04.2001 р. № 2341-III. Дата оновлення: 15.04.2026. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (дата звернення: 27.04.2026).

2. OSINT у документуванні воєнних злочинів. *Освітній дім прав людини. Чернігів*. URL: <https://ehrh.org/vazhlyvist-osint-u-dokumentuvanni-voenykh-zlochyniv-v-ukrayini/> (дата звернення: 27.04.2026).

3. Думчиков М. О. Відкрита розвідка (OSINT) у протидії інформаційним війнам: аналітичні інструменти та правові межі. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2025. № 6. Ч. 2. С. 273–277. DOI: <https://doi.org/10.24144/2788-6018.2025.06.2.43>

4. Активісти та журналісти заявляють про 182 тисячі воєнних злочинців. Вироки отримали 66 людей. *Українська гельсінська спілка з прав людини*. URL: <https://www.helsinki.org.ua/articles/aktyvisty-ta-zhurnalisty-zaiavliaiut-pro-182-tysiachi-voienykh-zlochynsiv-vyroky-otrymaly-66-liudey/> (дата звернення: 27.04.2026).

**Підхонний О. М.,**  
професор кафедри фінансів,  
грошового обігу і кредиту  
доктор економічних наук, професор  
*(Львівський національний університет імені Івана Франка)*

## **ТАКТИЧНІ ПРИЙОМИ ДОСЛІДЖЕННЯ СИСТЕМ ІЗ ЗАКРИТИМ ІНФОРМАЦІЙНИМ ПРОСТОРОМ**

Сучасні гібридні загрози й санкційне протистояння в умовах трансформації цифрового середовища актуалізують необхідність удосконалення підходів до дослідження систем із закритим інформаційним простором. Особливого значення ця проблематика набуває у контексті аналізу діяльності росії, Північної Кореї та Ірану, де поєднуються різні форми інформаційної ізоляції, контроль за інформаційними потоками, дезінформаційні практики й механізми приховування транснаціональних зв'язків. При цьому росію доцільно розглядати не як повністю ізольовану систему, а як систему, що перебуває у процесі посилення контрольованості інформаційного простору, у якій зберігаються окремі канали зовнішньої взаємодії, але водночас суттєво зростають масштаби цензури, фрагментації інформаційного середовища та використання механізмів контр-OSINT.

Закриті інформаційні системи доцільно класифікувати за ступенем інформаційної ізоляції, характером цифрових слідів, структурою прихованих зв'язків і рівнем протидії зовнішньому дослідженню. Такий підхід дає змогу ситуативно адаптувати тактичні прийоми аналітичної роботи залежно від типу інформаційного бар'єра та рівня доступності непрямих індикаторів. Для дослідження подібних систем особливе значення має використання OSINT як інструменту реконструкції прихованих процесів через аналіз фрагментарних відкритих даних, цифрових слідів, поведінкових аномалій і непрямих інформаційних ознак.

Важливу роль у дослідженні закритих інформаційних систем відіграє багатоджерельний аналіз, який забезпечує зіставлення відомостей із різних джерел та підвищує достовірність аналітичних висновків. Особливого значення набувають системи моніторингу руху суден, експортно-імпорتنі бази даних, митна статистика, торговельні реєстри та мережеві інформаційні ресурси, які дають змогу виявляти приховані ланцюги постачання, протисанкційні обхідні маршрути, тіншову логістику й мережі посередників. У багатьох випадках саме аналіз непрямих взаємозв'язків між транспортними маршрутами, торговельними операціями, змінами власників, фінансовими потоками та цифровою активністю дає змогу реконструювати структуру прихованих мереж.

Ефективним інструментом дослідження закритих систем є графовий аналіз, який допомагає інтегрувати розрізнені дані в єдину структуру взаємозв'язків, виявляти ключові вузли координації та моделювати приховані мережі взаємодії

[<https://arxiv.org/abs/2102.05571>]

Особливо важливим є виявлення латентних зв'язків між суб'єктами обходу санкцій, транспортною інфраструктурою, фінансовими посередниками, цифровими платформами та логістичними маршрутами

[<https://academic.oup.com/pnasnexus/article/2/3/pgad051/7059318>]

Водночас критичною проблемою стає верифікація даних, оскільки закриті системи часто характеризуються високим рівнем дезінформації, інформаційного шуму та навмисного приховування реальних взаємозв'язків. Це потребує застосування багаторівневої перевірки інформації, оцінювання рівня кореляції непрямих індикаторів, аналізу повторюваних патернів і виявлення структурних суперечностей.

Водночас дослідження закритих інформаційних систем супроводжується підвищеними ризиками для самого дослідника. У зв'язку з цим важливою складовою аналітичної діяльності є дотримання принципів кібергігієни та кібербезпеки. Аналіз контрольованих або ворожих інформаційних середовищ може супроводжуватись ризиками цифрового стеження, фішингових атак, шкідливого програмного забезпечення, компрометації дослідницької інфраструктури та навмисного інформаційного впливу. У таких умовах поєднання OSINT, багатоджерельного аналізу, графового моделювання, верифікації даних і кібербезпеки формує основу сучасних підходів до дослідження систем із закритим інформаційним простором та виявлення прихованих транснаціональних загроз.

### **Список використаних джерел**

1. Rastogi N. et al. TINKER: A framework for Open source Cyberthreat Intelligence. *Cryptography and Security*. 2021. DOI: <https://doi.org/10.48550/arXiv.2102.05571>
2. Chang H. et al. Complex systems of secrecy: the offshore networks of oligarchs. *PNAS Nexus*. 2023. № 2(3). DOI: <https://doi.org/10.1093/pnasnexus/pgad051>

**Поляк А. Ю.**

курсант 2 курсу навчально-наукового інституту  
з підготовки фахівців для підрозділів кримінальної поліції  
(Львівський державний університет внутрішніх справ)

**Огірко О. І.**

кандидат технічних наук,  
професор кафедри інформаційних технологій  
(Львівський державний університет внутрішніх справ)

## **OSINT ЯК ЗАСІБ ЗБОРУ ДОКАЗОВОЇ ІНФОРМАЦІЇ У КРИМІНАЛЬНИХ РОЗСЛІДУВАННЯХ**

Розвідка на основі відкритих джерел (OSINT) використовується сьогодні у різних сферах – від бізнес-аналітики до кібербезпеки та діяльності правоохоронних і розвідувальних органів. Вона передбачає використання відкритих джерел інформації, які у сукупності дозволяють сформулювати цілісне уявлення про об'єкт аналізу.

Для працівників правоохоронних органів, слідчих і детективів такі можливості мають прикладне значення, оскільки OSINT виступає додатковим засобом збору, перевірки та уточнення інформації у кримінальних провадженнях. Він дозволяє не лише фіксувати наявні обставини, а й аналізувати відкриті дані та цифрові сліди для подальшого розуміння подій і поведінки осіб, що становлять інтерес для слідства [1].

Узагальнені результати такого аналізу формують аналітичний продукт, який може використовуватися у правоохоронній діяльності – від базових відомостей про особу до складніших висновків щодо її зв'язків і поведінки. При цьому ефективність отриманих результатів залежить від обраних методів опрацювання відкритих джерел.

Практично це реалізується за допомогою спеціалізованих OSINT-інструментів. До них належать сервіси розпізнавання облич (Face8, FaceCheck, Faceagle), засоби аналізу метаданих (StolenCameraFinder, Extract.pics), інструменти визначення геолокації (GeoSpy, EarthKit), а також рішення для виявлення прихованої або закодованої інформації (Immerse.zone, Aperisolve, Stylesuxx Steganography) і платформи на основі штучного інтелекту (Kili-Technology) [2].

Застосування таких ресурсів дозволяє здійснювати комплексний аналіз цифрових даних та підвищує ефективність формування доказової бази у кримінальних провадженнях.

В умовах повномасштабної війни OSINT набув особливого значення у роботі правоохоронних органів України та міжнародної співпраці. Так, відкриті джерела використовуються в межах проєктів з документування воєнних злочинів, зокрема за участю спеціалізованих підрозділів OSINT OTF. Опрацювання відповідних матеріалів дозволяє встановлювати обставини інцидентів і причетних осіб навіть без доступу до місця подій. Результати аналізу оформлюються у вигляді аналітичних матеріалів, які використовуються у кримінальних провадженнях. Наприклад, досвід документування подій у Бучі показав, що поєднання фото- та відеоматеріалів з іншими відкритими даними дає змогу відтворювати їх перебіг і встановлювати причетних осіб [3].

Важливим підтвердженням ролі OSINT у доказуванні є практика міжнародних і національних судових інституцій. Рішення Європейського суду з прав людини від 30 листопада 2022 року у справі «Україна та Нідерланди проти Росії» засвідчило значення відкритих джерел у розслідуванні порушень прав людини, пов'язаних із подіями в Криму, на Донбасі та збиттям

рейсу MH17. У цій справі використовувалися матеріали дослідницької групи Bellingcat, що підтвердило можливість використання OSINT як елемента доказової бази [4, с. 235].

У національній судовій практиці показовим є вирок Солом'янського районного суду міста Києва від 21 листопада 2025 року у справі про державну зраду. Суд підтвердив допустимість використання відкритих інструментів аналізу інформації, зокрема щодо Telegram-акаунтів, водночас наголосивши, що такі дані не мають самостійного доказового значення і підлягають оцінці у сукупності з іншими доказами [4, с. 235].

Зазначена практика свідчить про поступове формування підходів до використання OSINT у кримінальному судочинстві як допоміжного інструменту збору та перевірки інформації, хоча і з певними застереженнями.

З огляду на це, особливого значення набуває підготовка правоохоронців до використання OSINT у кримінальних розслідуваннях. Актуальність таких навичок зумовлена зростанням обсягів відкритих цифрових даних і розвитком соціальних мереж, що розширює інформаційне середовище правоохоронної діяльності. Опанування OSINT-підходів підвищує якість аналітичної роботи та сприяє формуванню доказової бази у кримінальних провадженнях [5].

Отже, OSINT виступає ефективним засобом збору та аналітичної обробки доказової інформації у кримінальних розслідуваннях, забезпечуючи можливість отримання та перевірки даних з відкритих джерел. Його застосування дозволяє формувати доказову базу, яка за умови належної процесуальної оцінки може використовуватися у кримінальному провадженні.

### **Список використаних джерел**

1. OSINT: чому цей напрям такий перспективний і кому він може знадобитись? : [публікація від 08.02.2023]. URL: <https://www.issp.training/post/osint-chomu-tsey-napryam-takyy-perspektyvnyy-i-komu-vin-mozhe-znadobytysya> (дата звернення: 30.04.2026).

2. Інструменти OSINT для роботи з зображеннями : [публікація від 04.09.2024]. URL: <https://hackyourmom.com/kibervijna/instrumenty-osint-dlya-analizu-zobrazhen-u-2024-roczni/> (дата звернення: 30.04.2026).

3. Україна та партнери в Європолі посилюють роботу з відкритими даними для розслідування воєнних злочинів : [публікація від 25.04.2026]. URL: [https://npu.gov.ua/news/ukraina-ta-partnery-v-ievropoli-posyliuiut-robotu-z-vidkrytymy-danymy-dlia-rozsliduvannia-voiennykh-zlochyniv?utm\\_source=chatgpt.com](https://npu.gov.ua/news/ukraina-ta-partnery-v-ievropoli-posyliuiut-robotu-z-vidkrytymy-danymy-dlia-rozsliduvannia-voiennykh-zlochyniv?utm_source=chatgpt.com) (дата звернення: 30.04.2026).

4. Користін О. Є., Демедюк С. В. OSINT Open Source Intelligence. Теорія та методологія : монографія. Київ: 7БЦ, 2025. 304 с. URL: [file:///C:/Users/HP/Downloads/OSINT\\_Open\\_Source\\_Intelligence\\_Teoriya\\_%D0%9A%D0%BD.1.pdf](file:///C:/Users/HP/Downloads/OSINT_Open_Source_Intelligence_Teoriya_%D0%9A%D0%BD.1.pdf) (дата звернення: 30.04.2026).

5. Застосування OSINT-інструментів для ідентифікації осіб за фотозображенням: практичне заняття з кримінального аналізу в ДДУВС. Дніпровський державний університет внутрішніх справ. URL: <https://dduvs.edu.ua/2026/03/17/zastosuvannya-osint-instrumentiv-dlya-identyfikatsiyi-osib-za-fotozobrazhenniam-praktychne-zanyattya-z-kryminalnogo-analizu-v-dduvs/> (дата звернення: 30.04.2026).

## **ВИКОРИСТАННЯ OSINT (OPEN SOURCE INTELLIGENCE) У ВСТАНОВЛЕННІ ЮРИДИЧНО ЗНАЧУЩИХ ФАКТІВ ПРИ СПАДКУВАННІ В УМОВАХ ВОЄННОГО СТАНУ**

Актуальність дослідження використання OSINT (Open Source Intelligence) у встановленні юридично значущих фактів при спадкуванні в умовах воєнного стану зумовлена суттєвими трансформаціями правозастосовної практики в Україні внаслідок збройної агресії та пов'язаних із нею обмежень. Воєнний стан ускладнив доступ до традиційних джерел доказів, архівів, державних реєстрів, а також фізичне підтвердження окремих юридичних фактів, що є необхідними для реалізації спадкових прав.

У цих умовах особливого значення набувають відкриті джерела інформації (соціальні мережі, онлайн-реєстри, медіаресурси, геолокаційні дані, цифрові сліди), які можуть бути використані для встановлення факту смерті спадкодавця, останнього місця проживання, наявності майна, родинних зв'язків або обставин, що мають юридичне значення для спадкування. Водночас застосування OSINT у спадкових правовідносинах порушує низку правових і етичних питань, зокрема щодо допустимості таких доказів у суді, їх достовірності, способів верифікації та відповідності принципам захисту персональних даних [1]. Це зумовлює необхідність наукового осмислення ролі відкритої розвідки як сучасного інструменту встановлення юридичних фактів у сфері спадкового права в умовах воєнного стану[3].

Подальший розвиток теми потребує розуміння того, що OSINT (Open Source Intelligence) як метод роботи з відкритими джерелами інформації сформувався у сфері розвідувальної діяльності, однак сьогодні активно інтегрується у юридичну практику, зокрема в частині доказування. Його сутність полягає у зборі, аналізі та верифікації даних із відкритих джерел, які перебувають у вільному доступі: соціальних мереж, офіційних публічних реєстрів, медіа, супутникових знімків, цифрових архівів та інших онлайн-платформ. У контексті спадкових правовідносин OSINT може використовуватися для підтвердження або спростування юридично значущих фактів, таких як факт і дата смерті особи (у разі відсутності офіційного документального підтвердження в умовах бойових дій), останнє місце проживання спадкодавця, наявність майнових активів, родинні зв'язки або фактичні обставини володіння майном. [4]. Особливо це актуалізується в умовах воєнного стану, коли частина державних реєстрів може бути недоступною, пошкодженою або втраченою, а традиційні способи доказування ускладнені. Водночас використання OSINT у юридичній сфері потребує чіткої методологічної перевірки інформації, оскільки відкриті джерела можуть містити неповні, застарілі або навмисно викривлені дані. Тому ключовим є принцип крос-перевірки (corroboration), коли інформація підтверджується з кількох незалежних джерел, а також фіксація цифрових доказів у спосіб, придатний для подальшого судового дослідження (зокрема через нотаріальне засвідчення вебсторінок або використання технічних засобів фіксації) [2]. З огляду на це, OSINT може розглядатися як допоміжний інструмент у системі доказування у спадкових справах, але не як самостійна і безумовна підстава для встановлення юридичних фактів. Його значення полягає у розширенні доказової бази та підвищенні ефективності захисту спадкових прав у кризових умовах[5].

OSINT у спадкових правовідносинах не «замінює» класичні докази, але часто стає тим інструментом, який дозволяє відновити або підтвердити юридично значущі факти, коли

традиційні джерела недоступні або втрачені через воєнні дії. Його практична цінність полягає саме у вирішенні конкретних проблем, що виникають під час оформлення спадщини.

Передусім, OSINT може допомогти у встановленні факту смерті спадкодавця. У ситуаціях, коли відсутній офіційний актовий запис або немає доступу до органів РАЦС, використовуються повідомлення у соціальних мережах, некрологи в онлайн-медіа, публікації органів місцевої влади чи волонтерських організацій. Такі дані не є самостійним доказом, але можуть слугувати підставою для звернення до суду із заявою про встановлення факту смерті, а також допомагають сформулювати доказову базу.

Другий важливий аспект — визначення останнього місця проживання спадкодавця, що має ключове значення для відкриття спадщини. OSINT дозволяє аналізувати геолокаційні дані (публікації з прив'язкою до місця), активність у соцмережах, згадки в публічних реєстрах або навіть участь особи у місцевих ініціативах, що може підтвердити її фактичне проживання в певному населеному пункті.

Третій напрям — встановлення складу спадкового майна. Через відкриті реєстри (наприклад, нерухомості, бізнесу, судових рішень), оголошення про продаж, згадки в медіа чи навіть фото/відео у відкритому доступі можна виявити наявність майна, корпоративних прав або інших активів, які не були задекларовані або інформація про які втрачена.

Не менш важливим є використання OSINT для підтвердження родинних зв'язків. У випадках втрати документів або неможливості їх отримання (наприклад, з окупованих територій), інформація з соціальних мереж (спільні фото, публікації, коментарі), генеалогічних платформ, публічних баз даних може допомогти встановити фактичні сімейні відносини, що в подальшому використовуються у суді.

Окремо варто відзначити роль OSINT у розшуку спадкоємців. Через аналіз цифрових слідів, контактів, професійних мереж і відкритих профілів можна встановити місцезнаходження осіб, які мають право на спадщину, але втратили зв'язок або були переміщені внаслідок війни.

Водночас ключова умова ефективного використання OSINT — це належна перевірка та процесуальне оформлення інформації. Дані з відкритих джерел повинні бути:

- перевірені через кілька незалежних джерел;
- зафіксовані (скріншоти, архівування сторінок, протоколи огляду вебсайтів);
- подані до суду у формі електронних доказів відповідно до вимог процесуального законодавства.

Таким чином, OSINT виступає як інструмент подолання доказових прогалин, що виникають в умовах воєнного стану. Він не підміняє офіційні документи, але дозволяє їх відновити, доповнити або обґрунтувати звернення до суду, що суттєво підвищує ефективність реалізації спадкових прав у кризових умовах.

#### **Список використаних джерел**

1. NATO. *Open Source Intelligence Handbook*. NATO Intelligence Exploitation of Open Sources, 2001.

2. European Union External Action Service. *Handbook on OSINT for analysts*. EU Institute for Security Studies, 2020.

3. McDermott, R. *Open Source Intelligence in the Digital Age*. Intelligence and National Security Journal, 2019.

4. Міністерство юстиції України. Роз'яснення щодо використання електронних доказів у судовому процесі. Офіційний вебсайт, 2023.

5. Кравчук В. М. Використання електронних доказів у цивільному судочинстві України. *Юридична наука*. 2022. № 4.

**Прокопов С. О.,**  
старший викладач кафедри  
інформаційних технологій  
(Дніпровський державний університет внутрішніх справ)

## **ДОСЛІДЖЕННЯ ЦИФРОВИХ ФОТО ТА ВІДЕО ЗА МЕТОДИКОЮ OSINT**

Під час досудового розслідування та при проведенні оперативної діяльності доволі часто в поле зору правоохоронців попадають фотозображення фігурантів розслідувань, які можуть мати важливу інформацію для слідства щодо місця перебування осіб, часу створення фотозображення та інших деталей. Дані фотозображення можна знайти під час дослідження технічних пристроїв фігурантів, у соціальних мережах та у мережі Інтернет. Тому важливо знати яка інформація міститься у фотозображеннях та вміти проводити дослідження цифрових слідів фото, відео та звукових файлів.

У цій доповіді розглянемо методику OSINT-дослідження фотозображень, яка буде цікава як для курсантів, під час проведення практичних занять за тематикою OSINT, так і практичним працівникам Національної поліції.

При дослідженні цифрових фото або відеозображень важливо не просто дивитися, а бачити деталі, які автор фото міг залишити випадково. Розглянемо покрокову методику, як отримати максимум інформації з одного знімка.

По-перше, необхідно провести технічний аналіз фотозображення, тобто отримати його метадані. Варто перевірити «цифровий відбиток» файлу — EXIF-дані. Вони можуть містити модель камери, час знімка та навіть точні GPS-координати [3]. Соціальні мережі (Facebook, Instagram, Twitter (X), WhatsApp, Telegram), при звичайному відправленні, повністю очищують EXIF для захисту приватності користувачів. Але якщо фото надіслано файлом у месенджері або знайдено на сайті — шанси є. Для цього доцільно використовувати наступні програми Jeffrey's Image Metadata Viewer, exiftool або онлайн-сервіси на кшталт ExtractMetadata. Якщо фото знайдене в соцмережі й метаданих немає, необхідно спробувати знайти це ж фото через реверсивний пошук у блогах, на особистих сайтах або локальних форумах. Там власники часто завантажують оригінали, забуваючи про очищення.

По-друге, використовується реверсивний пошук зображень, тобто перевіряється, чи з'являлося це фото раніше в мережі, що допоможе знайти першоджерело або контекст. Для цього використовуються наступні інструменти: Google Lens — найкращий для пошуку об'єктів та локацій, Yandex Images залишається одним із найпотужніших для розпізнавання облич та пошуку в Східній Європі, Bing Visual Search добре працює з архітектурою та товарами, PimEyes — це спеціалізований сервіс для пошуку людей за обличчям по всьому Інтернету [1].

По-третє, проводиться візуальний аналіз, або «метод декомпозиції», тобто якщо реверсивний (автоматичний) пошук зображень не дав результату, розбираємо фото на деталі. Особливу увагу необхідно приділяти наступним підказкам: написам та знакам, тобто назвам магазинів, дорожнім вказівникам, номерам авто (код регіону), оголошенням на стовпах та в інших місцях; архітектурі, тобто типу забудови (сталінки, хрущовки, європейський стиль),

кольору дахів, формі вікон; інфраструктурі — формі ліхтарів, типу смітників, дизайну вуличних табличок, кольору розмітки на дорогах; природі, яка включає в себе тип рослинності (акації чи сосни), рельєф (гори, рівнини), тип ґрунту [4].

По-четверте, досліджуємо геолокацію, тобто пошук місця створення фотозображення. Коли знайдено якусь зачіпку, наприклад, назву кафе або характерну будівлю, необхідно використовувати мапи. Найбільш поширеними є Google Maps або Google Earth, які дозволяють за допомогою режиму Street View, порівняти фото з панорамою місцевості [4]. Ресурс Вікімапія також може бути у нагоді, на вікі-карті, деякі користувачі позначають навіть військові частини чи закинуті заводи. Якщо на фото є гори, то сервіс PeakVisor допоможе ідентифікувати вершини за їхнім профілем.

Наприкінці, правоохоронців цікавить час, коли були зроблені фото або відео, тобто хронолокація. Зрозуміти, коли було зроблено фото можна за допомогою розташування тіней від предметів. За довжиною та напрямком тіней можна визначити час доби та пору року. Допомогти у цьому може інструмент SunCalc, який дозволяє розрахувати положення сонця в конкретній точці планети в будь-який час. Якщо знати місце, то можна вирахувати годину зйомки.

Більш детально розглянемо технічний аналіз метаданих, це є першим і важливим кроком дослідження фото та відео. Якщо саму картинку можна порівняти з фасадом будинку, то метадані — це його технічний паспорт, де записано, хто, коли і як цей будинок збудував. Метадані складаються з трьох складових, а саме: EXIF, IPTC та XMP. Більшість користувачів чули лише про EXIF, але для аналізу важливі всі три стандарти.

Найважливішим є EXIF (Exchangeable Image File Format). Цей стандарт створюється автоматично камерою або смартфоном. Тут містяться технічні параметри зйомки (діафрагма, витримка, ISO), модель пристрою та, найголовніше, GPS-координати.

Стандарт IPTC (International Press Telecommunications Council) використовується здебільшого фотографами та ЗМІ. Сюди вручну вписують назву знімка, опис, ключові слова, авторські права та дані про місцевість.

Стандарт від фірми Adobe — XMP (Extensible Metadata Platform). Він цікавий тим, що зберігає історію редагування. Тут можна побачити, чи проходило фото через Photoshop або Lightroom, і іноді навіть побачити шлях до файлу на комп'ютері автора (що може розкрити ім'я користувача в системі).

При аналізі метаданих в першу чергу необхідно звертати увагу на наступні важливі позиції, як Make & Model, які містять інформацію про телефон чи камеру, ця інформація може бути важливою для ототождження автора знімків. Наступним видом інформації метаданих є DateTimeOriginal, де зберігається точний час, коли натиснули на кнопку затвора. Якщо порівняти його з ModifyDate, то в разі суттєвої різниці інформації можна зробити висновок, що файл редагували [2]. Розглянемо найважливіший вид метаданих GPS Latitude / Longitude. Якщо ці дані є, ми можемо визначити точне місце створення цифрового файлу. Ці координати необхідно вставити у Google Maps, і місце створення фото або відео відобразиться на місцевості. При вивченні Orientation / Software, можна з'ясувати чи оброблялося фото на телефоні. Про це свідчать записи "Snapseed" або "Instagram" в полі Software. Дуже цікавим є вивчення меню метаданих Thumbnail (Ескіз). Іноді основне фото обрізають, щоб приховати деталі, але в метаданих залишається автоматично згенерований ескіз (прев'ю) повного зображення.

Наведена у доповіді інформація може допомогти правоохоронцям в опануванні інструментів OSINT для ефективного дослідження фото та відео в рамках службової діяльності, отримання необхідної інформації з фотозображень, використання практичних навичок роботи з «цифровими слідами».

### **Список використаних джерел**

1. Гребенюк А. М., Прокопов С. О., Рибальченко Л. В. Використання технологій розпізнавання обличчя на відео- та фотозображеннях : метод. рекомендації. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2023. 48 с. URL: [https://er.dduvs.edu.ua/bitstream/123456789/13273/5/%D0%BC%D0%B0%D0%BA%D0%B5%D1%82\\_%D1%80%D0%BE%D0%B7%D0%BF%D1%96%D0%B7%D0%BD%D0%B0%D0%B2\\_%D0%B2%D1%96%D0%B4%D0%B5%D0%BE\\_%D0%9C%D0%B5%D1%82%D0%BE%D0%B4.%20%D1%80%D0%B5%D0%BA%D0%BE%D0%BC%D0%B5%D0%BD%D0%B4.pdf](https://er.dduvs.edu.ua/bitstream/123456789/13273/5/%D0%BC%D0%B0%D0%BA%D0%B5%D1%82_%D1%80%D0%BE%D0%B7%D0%BF%D1%96%D0%B7%D0%BD%D0%B0%D0%B2_%D0%B2%D1%96%D0%B4%D0%B5%D0%BE_%D0%9C%D0%B5%D1%82%D0%BE%D0%B4.%20%D1%80%D0%B5%D0%BA%D0%BE%D0%BC%D0%B5%D0%BD%D0%B4.pdf)
2. Приватна розвідка методами OSINT. Сайт Molfar. URL: <https://molfar.com/blog/privatna-rozvidka-metodami-osint>
3. Прокопов С. О. Визначення геопозиціонування за фотозображеннями та відеозаписами під час проведення пошуку інформації з відкритих джерел (OSINT). *Міжнародна та національна безпека: теоретичні і прикладні аспекти* : матеріали ІХ Міжнар. наук.-практ. конф. (м. Дніпро, 21 березня 2025 р.). У 2-х ч. Дніпро : ДДУВС, 2025. Ч. II. С. 538–541. URL: <https://er.dduvs.edu.ua/handle/123456789/16290>
4. Michael Bazzell & Jason Edison. OSINT techniques:resources for uncovering online information eleventh edition. 2024. URL: <https://elhacker.info/manuales/Hacking%20y%20Seguridad%20informatica/IntelTechniques%20-%20OSINT%2011%202025.04.02%20.pdf>

**Проценко М. В.,**  
курсант 1 курсу факультету № 2  
(Львівський державний університет внутрішніх справ)  
**Галайко Н. В.,**  
старший викладач кафедри інформаційних технологій  
(Львівський державний університет внутрішніх справ)

## **ЕТИКО-ПРАВОВІ РЕГУЛЮВАННЯ OSINT У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ**

Розвідка з відкритих джерел (OSINT) є новим і перспективним напрямом діяльності правоохоронних органів. Її інтеграція у професійну діяльність сприяє підвищенню ефективності виконання завдань Національної поліції України (НПУ). Значний обсяг доступної інформації, її відкритість і відносно невисокі матеріальні витрати роблять цей напрям одним із найбільш перспективних, здатним суттєво доповнити традиційні (усталені) методи отримання інформації.

Водночас розвиток цифрового середовища та зростання ролі соціальних мереж, онлайн-платформ і відкритих баз даних зумовлюють необхідність системного підходу до використання OSINT. Сучасні правоохоронні органи дедалі частіше стикаються з ситуаціями, коли саме відкриті джерела стають первинним або навіть ключовим джерелом інформації. Це актуалізує питання не лише ефективності, а й правомірності та етичності таких методів.

OSINT як складова правоохоронної діяльності має бути належним чином законодавчо врегульована, як і інші її види. Основною проблемою є те, що законодавець не завжди встигає за динамічними суспільно-технологічними змінами. Станом на сьогодні відсутнє чітке нормативне визначення OSINT як інструменту правоохоронної діяльності, що створює певні труднощі, однак не унеможлиблює його використання органами НПУ. Водночас формально така діяльність може розглядатися як різновид оперативно-розшукової діяльності в контексті способу отримання інформації [1, с. 13].

Показовим прикладом використання OSINT у межах оперативно-розшукової діяльності є вирок Жовтневого районного суду м. Дніпра, в якому зазначено, що дані, отримані з відкритих джерел за допомогою OSINT, були прийняті судом як докази у кримінальному провадженні відповідно до «Протоколу Берклі», який визначає мінімальні стандарти пошуку, збирання, зберігання, перевірки та аналізу відкритих джерел. Фактично це свідчить про формування судової практики, за якої OSINT може виступати самостійним джерелом доказування.

Важливо також враховувати, що використання OSINT як доказової бази вимагає належної процесуальної фіксації та перевірки достовірності інформації. Без дотримання цих вимог навіть релевантні дані можуть бути визнані недопустимими доказами. Тому поряд із розвитком практики застосування OSINT виникає потреба у виробленні чітких методичних рекомендацій для працівників правоохоронних органів.

Окрім «Протоколу Берклі», існує низка міжнародних документів, що регулюють використання розвідки з відкритих джерел, на які можуть орієнтуватися органи НПУ. Серед них – Керівництво з базових стандартів розслідування для документування міжнародних злочинів в Україні, а також практика Європейського суду з прав людини, зокрема рішення у справі «Україна та Нідерланди проти Росії» (2022 р.), яке фактично підтвердило допустимість використання OSINT-даних як належних і надійних доказів [2, с. 86, 88; 3, с. 32].

Водночас, відповідно до практики ЄСПЛ (справа «Сегерштедт-Віберг та інші проти Швеції», 06.09.2006), використання розвідки з відкритих джерел може розцінюватися як втручання у право на приватне життя. У зв'язку з цим для фахівців у сфері OSINT надзвичайно важливою є належна правова обізнаність, що дозволяє мінімізувати ризики юридичної відповідальності [4, с. 44].

Не менш важливим є питання етичного регулювання OSINT. Йдеться про сукупність норм професійної поведінки, яких мають дотримуватися працівники правоохоронних органів, зокрема під час здійснення OSINT-діяльності, з метою забезпечення служіння суспільству.

Міжнародні документи не лише встановлюють правові межі використання OSINT, але й визначають ключові етичні принципи. До них належать: підзвітність і прозорість, захист конфіденційної інформації (принцип «не нашкодь»), професійна компетентність, дотримання стандартів і меж допустимого, а також об'єктивність і неупередженість. Особливого значення набувають принципи законності, захисту приватності та дотримання меж дозволеного [3, с. 32; 5].

Крім того, етичний вимір OSINT пов'язаний із проблемою потенційного зловживання відкритою інформацією. Навіть публічно доступні дані можуть бути використані таким чином, що завдаватимуть шкоди особі або суспільству. Це підсилює необхідність формування професійної етики аналітиків OSINT, яка має базуватися не лише на формальному дотриманні закону, а й на усвідомленні соціальної відповідальності.

Варто наголосити на можливості виникнення конфліктів між правовими та етичними нормами, оскільки не все законне є етичним. Зокрема, збір інформації з відкритих джерел може формально не порушувати закон, однак суперечити принципу захисту приватності або мінімізації шкоди. Крім того, прагнення до прозорості розслідування інколи конфліктує з необхідністю обмеження поширення чутливої інформації. Таким чином, використання OSINT потребує балансу між ефективністю розслідування, суспільним інтересом і дотриманням етичних та правових меж.

Отже, етико-правове регулювання OSINT у правоохоронній діяльності набуває системоутворюючого значення в умовах цифровізації суспільства та трансформації підходів до отримання доказової інформації. Відсутність чіткої нормативної регламентації не лише ускладнює практичне застосування цього інструменту, але й створює ризики порушення фундаментальних прав людини, зокрема права на приватність. Водночас формування судової практики та орієнтація на міжнародні стандарти свідчать про поступову інституціоналізацію OSINT як повноцінного елементу доказування.

У цьому контексті ключовим завданням є розроблення комплексного підходу до регулювання OSINT, який поєднуватиме чіткі правові норми, уніфіковані методичні рекомендації та закріплені етичні стандарти. Лише за умови такого поєднання можливе забезпечення балансу між ефективністю правоохоронної діяльності, суспільним інтересом і дотриманням прав людини.

### Список використаних джерел

1. Басалик С. А., Туз О. С., Тищук, В. В. Генезис інструментів OSINT та окремі аспекти їх використання у правоохоронній діяльності. *Український Політико-правовий Дискурс*. 2025. № 9. URL: <https://doi.org/10.5281/zenodo.15086041>
2. Скуратівський Є. Використання OSINT-технологій у розшуковій діяльності під час досудового розслідування. *Матеріали конференції МЦНД* (12.09.2025; Рівне, Україна), 2025. С. 85–89. URL: <https://doi.org/10.62731/mcnd-12.09.2025.003>
3. Торбас О. О. OSINT при розслідуванні кримінальних правопорушень : підручник. Одеса : Видавництво «Юридика», 2024. 180 с.
4. Синьколодєзський Р., Кисельов А. Соціальні мережі та OSINT -аналіз в розшуковій діяльності та діагностиці особистості. *UNIVERSUM* | Вересень 2024, 12, 2024. С. 40–48. URL: <https://archive.liga.science/index.php/universum/article/view/1204>.
5. Протокол Берклі з ведення розслідувань з використання відкритих цифрових даних. URL: <https://www.law.berkeley.edu/wp-content/uploads/archive/2022/03/Berkeley-Protocol-Ukrainian.pdf>

**Пряхіна Н. О.,**  
професор кафедри, кандидат психологічних наук, доцент  
(Львівський державний університет внутрішніх справ)  
**Пряхіна В. Є.,**  
здобувач вищої освіти  
(Львівський національний університет імені Івана Франка)

## **ІНТЕГРАЦІЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПРОЦЕСИ ВІДКРИТОЇ РОЗВІДКИ (OSINT)**

Технологія штучного інтелекту набуває все більшого значення у всіх сферах людської діяльності. У світі, де інформація є стратегічним ресурсом, її обсяг на усіх інтернет-платформах стрімко зростає. ШІ, як інструмент, допомагає у аналізі та обробці великих масивів даних, які часом ускладнюють цей процес. Слід зазначити, що «OSINT» – це процес збору, аналізу і використання інформації, яка відкрито доступна. Така інформація після обробки може бути використана для отримання аналітичних висновків у сфері безпеки, правоохоронної діяльності, кібербезпеки та інших галузях [3]. Основна мета OSINT – зібрати релевантну інформацію для подальшого аналізу та прийняття рішень. Автоматизований аналіз текстів, зображень і поведінкових патернів відкриває нові можливості для протидії дезінформації та загрозам. Інтеграція AI у системи безпеки є необхідною відповіддю на гібридні виклики.

Тематика відкритої розвідки широко досліджується у сучасній літературі: Thomas Oakley Browne, Mohammad Abedin та Mohammad Javed Morshed Chowdhury здійснили систематичний огляд наукових праць, присвячених використанню штучного інтелекту в OSINT та окреслили перспективні напрями подальших досліджень, Riccardo Ghioni, Mariarosaria Taddeo та Luciano Floridi, дослідили етичні, правові та соціальні аспекти використання штучного інтелекту, вона наголошує на необхідності незалежного регулювання використання таких технологій, оскільки автоматизація аналізу великих обсягів даних може створювати ризики для захисту приватності та інформаційної безпеки. Метою є дослідження особливостей інтеграції технологій штучного інтелекту у процеси відкритої розвідки, а також визначення можливостей, переваг і обмежень для алгоритмів ШІ для автоматизації процесів збору даних.

Використання штучного інтелекту у відкритій розвідці дозволяє автоматизувати окремі етапи розвідувального циклу, зокрема[5]:

- Виявлення закономірностей
- Моделювання злочинної активності в певному регіоні
- Створення кримінальних профілів
- Оцінювання ризиків рецидиву
- Виявлення аномалій у великих масах даних, які можуть свідчити про приховані злочинні дії

Проте найбільш ефективними залишаються технології NLP, автоматичне сортування повідомлень і аналіз візуального контенту. Обробка природної мови (NLP) – це підгалузь комп'ютерних наук і штучного інтелекту, що займається взаємодією між комп'ютерами і людськими (природними) мовами. Серед ключових завдань – виявлення фейків, бот-мереж і скоординованих інформаційних атак. Алгоритми розпізнають повторювані повідомлення й поведінкові шаблони, що дає змогу аналітику зосередитися на глибокій інтерпретації даних та формуванні ефективних стратегій інформаційної безпеки. Алгоритми штучного інтелекту лежать в основі процесів, що забезпечують автоматичне виявлення тенденцій, загроз і аномалій у складному інформаційному середовищі. Найбільш поширеними серед них є кластеризація (групування подібної інформації), класифікація (розподіл за категоріями), виявлення аномалій (фіксація нетипових змін або сигналів) і семантичний аналіз, який дозволяє розрізнити значення текстів у залежності від контексту [2].

В умовах війни та кризової економіки, використання штучного інтелекту для OSINT дозволяє AI швидко обробляти великі обсяги інформації, знаходити кореляції між даними та фільтрувати шум. Моделі, такі як GPT, Gemini, DeepSeek та інші можуть розшифровувати складні повідомлення та аналізувати текст. AI, крім іншого, допомагає визначати фейкові акаунти та дезінформацію. Однак сам AI також може використовуватись для інформаційного впливу. AI дозволяє виявляти мережі ботів і відстежувати наративи, які розповсюджують ворожу пропаганду. Погоджуємось із Едуардом Рижковим, який зазначає, що його успішно можна використовувати для розробки нових алгоритмів виявлення інформаційних операцій. Військові та правоохоронці можуть використовувати AI для аналізу активності у соцмережах, визначення локацій та ідентифікації підозрілих груп. Комп'ютерний зір дозволяє аналізувати супутникові знімки, відео та фотографії[1].

Важливим обмеженням використання ШІ в OSINT є залежність від якості даних: неповна або викривлена інформація з відкритих джерел може призводити до помилкових аналітичних висновків, що потребує обов'язкової перевірки результатів людиною.

Отже, технологія OSINTу гармонійному поєднанні із штучним інтелектом не лише дозволяє отримувати цінну інформацію з відкритих джерел, доповнювати оперативно-розшукову та розвідувальну діяльність, а також підвищує ефективність та швидкість самого аналізу. Безперечно окрім переваг, зустрічають і недоліки роботи ШІ, наприклад хибні спрацьовування, неякісні відповіді та різні бар'єри [4]. У таких випадках роль аналітика зростає, бо він забезпечує захист від дезінформації, тому важливою є наявність фахівця який зможе поєднувати знання ШІ з аналітикою, варто впроваджувати ознайомчі курси щодо поняття та роботи штучного інтелекту аби ще більше його інтегрувати в роботу з громісткими процесами. Таким чином, оптимальним є поєднання аналітичних можливостей штучного інтелекту з професійним досвідом людини, що дозволить досягти максимальної ефективності у процесах відкритої розвідки. Окрім того, корисним може бути подальша регламентація використання AI для запобігання зловживання, відповідно до твердження фахівців, про недосконалість правового регулювання штучного інтелекту як в Україні, так і за кордоном[1].

### Список використаних джерел

1. Рижков Е. Перспективи використання штучного інтелекту під час реалізації технології OSINT. *Міжнародна та національна безпека: теоретичні і прикладні аспекти* : матеріали IX Міжнародної науково-практичної конференції (ДДУВС, 21.03.2025). Ч. II. С. 519–521. URL: <https://er.dduvs.edu.ua/bitstream/123456789/16293/1/66.pdf>
2. Шипрінський Н. О., Моргунова Т. І. Штучний інтелект як інструмент удосконалення OSINT-аналітики. С. 178–181 URL: <https://dspace.oduvs.edu.ua/server/api/core/bitstreams/c401fb4a-5d4e-4b47-87eb-ef0869026083/content?page=179>
3. Дерев'ягін 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 Міжнародної науково-практичної конференції. С. 221–225. URL: [https://www.researchgate.net/profile/Anna-Politova-2/publication/382116695\\_Politova\\_AS\\_Analiz\\_okremih\\_polozen\\_kriminalnoi\\_vidpovidalnosti\\_za\\_voenni\\_zlocini\\_Rozdil\\_114\\_proektu\\_Kriminalnogo\\_kodeksu\\_Ukraini\\_SBU\\_v\\_umovah\\_vijni\\_v\\_Ukraini\\_sucasni\\_realii\\_ta\\_innovacijni\\_strategii\\_za/links/668e70053e0edb1e0fdb4195/Politova-AS-Analiz-okremih-polozen-kriminalnoi-vidpovidalnosti-za-voenni-zlocini-Rozdil-114-proektu-Kriminalnogo-kodeksu-Ukraini-SBU-v-umovah-vijni-v-Ukraini-sucasni-realii-ta-innovacijni-strategii-za.pdf?page=221](https://www.researchgate.net/profile/Anna-Politova-2/publication/382116695_Politova_AS_Analiz_okremih_polozen_kriminalnoi_vidpovidalnosti_za_voenni_zlocini_Rozdil_114_proektu_Kriminalnogo_kodeksu_Ukraini_SBU_v_umovah_vijni_v_Ukraini_sucasni_realii_ta_innovacijni_strategii_za/links/668e70053e0edb1e0fdb4195/Politova-AS-Analiz-okremih-polozen-kriminalnoi-vidpovidalnosti-za-voenni-zlocini-Rozdil-114-proektu-Kriminalnogo-kodeksu-Ukraini-SBU-v-umovah-vijni-v-Ukraini-sucasni-realii-ta-innovacijni-strategii-za.pdf?page=221).
4. Systematic Literature Review to Investigate the Application of Open Source Intelligence (OSINT) with Artificial Intelligence 2020 URL: <https://www.tandfonline.com/doi/full/10.1080/19361610.2020.1761737?needAccess=true>
5. Олексієнко Д. О., Нікішенко Д. О., Іващук Р. С., Кисельов А. О. Інформаційні Технології та системи. Розділ 13 Штучний інтелект в кримінальному аналізі. *Universum*. 2025. № 21. URL: <https://archive.liga.science/index.php/universum/article/view/2021/2049>

**Радик В. В.,**  
аспірант кафедри фінансів, грошового обігу і кредиту  
(Львівський національний університет імені Івана Франка)

## **НАПРЯМИ ВИКОРИСТАННЯ OSINT У СИСТЕМІ САНКЦІЙНОГО КОНТРОЛЮ**

Важливою складовою санкційного контролю є збір та аналіз великих обсягів інформації, яка б свідчила про причетність фізичних та юридичних осіб до певного протиправного діяння чи інших підсанкційних осіб. В умовах масштабної цифровізації важливим джерелом такої інформації є OSINT.

На рівні санкційної політики OSINT використовується для виявлення потенційних загроз національній безпеці, підтвердження фактів вчинення небажаної поведінки та ідентифікації осіб, причетних до такого діяння, що в подальшому розглядається в межах прийняття рішення про ініціювання санкційного режиму, у випадку, коли застосування механізму спеціальних обмежувальних заходів визначається доцільним.

Дослідження С. Шафі, А. Бессані та П.М. Феррейра [1] свідчить, що ефективно виявлення інформації, що стосується певної сфери, наприклад кібербезпеки, на основі аналізу відкритих даних можливе з використанням як спеціалізованих систем, так і GenAI, проте розпізнавання іменованих сутностей (Named Entity Recognition) у такій інформації потребує використання спеціалізованих моделей глибокого машинного навчання – доступні станом на липень 2023 року версії GenAI показали як низьку якість розпізнавання, так і набагато довшу тривалість аналізу.

Якщо рішення про відкриття санкційного режиму прийняте, державні органи, відповідальні за лістинг підсанкційних осіб, забезпечують їхнє внесення до санкційних списків, разом із наявною про них інформацією. Одночасно відбувається пошук додаткової ідентифікаційної та іншої інформації, визначення пов'язаних осіб, а також налагоджується періодичний моніторинг із метою виявлення нових причетних осіб. Для цих цілей поширеним методом є аналіз соціальних мереж (social network analysis). Наприклад, М. Лісон, Р. Джованеллі, М.Д. Бернардін та А. Травілья [2], використовуючи відкриті дані, зобразили мережу зв'язків між російськими власниками творів мистецтва та виявили, що частина з них не перебувають під санкціями.

Втім, часто санкційні списки публікуються в текстовій чи табличній формі та містять мінімальну інформацію про підсанкційні об'єкти. На нашу думку, інформація про підсанкційну особу повинна містити також опис підстав накладення санкцій як конкретних небажаних дій особи та іншу контекстну інформацію, що б дало змогу покращити розуміння санкційного заходу з боку приватного сектору та сприяло б проведенню санкційної перевірки при здійсненні господарської діяльності. Це може бути реалізовано, наприклад, через додання спеціальних інформаційних полів до поточних форм санкційних списків, формування баз чи реєстрів санкцій (як, наприклад, колонка “additional\_info” у Державному реєстрі санкцій [3]), або публікацію спеціальних прес-релізів, як, наприклад, практикується OFAC [4]. Перспективним також може виявитися наведення фотографій підсанкційних осіб та логотипів юридичних осіб, що б дало змогу швидко порівнювати одержані під час санкційної перевірки візуальні дані фізичних осіб без необхідності окремої ідентифікації всіх інших осіб на таких зображеннях для виявлення можливих незадокументованих зв'язків, або

проводити автоматичну оцінку подібності логотипів компаній для виявлення шаблонів їхнього створення. Деякі успіхи в цьому напрямі присутні в діяльності Головного управління розвідки Міністерства оборони України – Головний портал про спонсорів та співучасників агресії [5] наводить фотографії фізичних осіб, суден та логотипи компаній для окремих категорій об'єктів, частина з яких перебувають під санкціями.

Особливо важливим є наявність фотографій суден, що дає змогу ідентифікувати їх на основі супутникових знімків у випадку вимкнення ними автоматичної ідентифікаційної системи (Automatic Identification System) або перевантаження товарів у відкритому плаванні. Інші методи виявлення обходу санкцій під час проведення морської торгівлі включають використання відкритих джерел для відстеження суден через AIS, перевірку наявності декількох суден з однаковими ідентифікаційними даними, чи розрахунок відповідності швидкості отримання AIS сигналу до відстані розташування судна, відповідно до переданої інформації, а також використання супутникових радарів із синтетичною апертурою (Synthetic Aperture Radar), які працюють незалежно від погодних умов [6-7].

Лістинг підсанкційних осіб зобов'язує суб'єктів виконання санкцій впровадити передбачені обмеження, що може включати виявлення активів, що їм належать. Для ефективності такої діяльності невід'ємним є проведення аналізу на основі відкритих джерел даних, що підтверджується практикою Агентства з розшуку та менеджменту активів [8].

Упродовж дії обмежувальних заходів приватний сектор проводить санкційні перевірки клієнтів та контрагентів для забезпечення належного виконання законодавчих вимог щодо санкційного комплаєнсу. На цьому етапі використання OSINT все ще є доволі обмеженим. Банки та небанківські фінансові посередники можуть проводити поверхневий огляд інтернет-джерел та медіа-публікацій для оцінки ставлення до об'єкта в рамках автоматизованої системи санкційного скринінгу, однак, у разі виявлення будь-яких сумнівів, відразу надсилають фінансове повідомлення про підозрілу операцію до підрозділу фінансової розвідки, замість проведення більш глибокого аналізу. З іншого боку, транснаціональні корпорації, особливо у сфері роздрібної торгівлі, можуть пов'язувати аналіз відкритих джерел із метою санкційної перевірки із формуванням профілю клієнта для подальшого створення персональних рекламних пропозицій.

OSINT також актуальний для загального аналізу підприємством ринків збуту чи ресурсів. Оцінка ризиковості територій повинна враховувати інформацію з відкритих джерел, у тому числі в частині даних про кількість підсанкційних об'єктів, які здійснюють звідти діяльність, та фактів використання таких юрисдикцій для обходу чи підриву санкцій.

Оцінка ефективності санкцій також може враховувати результати OSINT, наприклад у частині підтвердження зміни ринків збуту чи постачальників підсанкційними компаніями або повідомлення в соціальних мережах, які підтверджують відсутність певних категорій товарів, торгівля якими потрапила під санкційні обмеження, а також визначення загальних економічних втрат підсанкційної країни від накладених обмежень.

Отже, можливості використання OSINT у сфері санкційного контролю проявляються на всіх його етапах та дають змогу отримати інформацію, необхідну для прийняття управлінських рішень, забезпечення санкційного комплаєнсу, проведення розслідувань та загалом сприяють підвищенню національної безпеки. Як державний, так і приватний сектор повинні забезпечити ефективне впровадження процесів, результатом яких є формування OSINT-звітів та їхню інтеграцію з іншою аналітичною діяльністю, зокрема для підвищення ефективності системи санкційного контролю.

### Список використаних джерел

1. Shafee S., Bessani A., Ferreira P. M. Evaluation of LLM-based chatbots for OSINT-based cyber threat awareness. *Expert Systems with Applications*. 2025. Vol. 261. Article 125509. DOI: <https://doi.org/10.1016/j.eswa.2024.125509>
2. Leeson M., Giovanelli R., Bernardin M.D., Traviglia A. War, art, and sanctions: social network analysis on the NACP's databases of sanctioned russian individuals and art collectors. *International Journal of Digital Humanities*. 2024. Vol. 6. P. 189–215. DOI: <https://doi.org/10.1007/s42803-024-00089-y>
3. Державний реєстр санкцій. Рада національної безпеки і оборони України. URL: <https://drs.nsd.gov.ua/> (дата звернення: 01.05.2026).
4. OFAC related press releases. *Office of foreign assets control*. URL: <https://ofac.treasury.gov/press-releases> (date of access: 01.05.2026).
5. Головний портал про спонсорів та співучасників агресії. Головне управління розвідки Міністерства оборони України. URL: <https://war-sanctions.gur.gov.ua/> (дата звернення: 01.05.2026).
6. Schmitt B. Catching russia sanctions busters - from orbit. *Center for European Policy Analysis*. URL: <https://cepa.org/article/catching-russia-sanctions-busters-from-orbit/> (date of access: 01.05.2026).
7. Automatic Identification System spoofing. *Oceana*. URL: <https://usa.oceana.org/wp-content/uploads/sites/4/2023/07/AIS-Spoofing-Factsheet.pdf> (date of access: 01.05.2026).
8. Як працює OSINT-розвідка у сфері розшуку незаконних активів? *Агентство з розшуку та менеджменту активів*. URL: <https://arma.gov.ua/news/typical/yak-pratsyue-osint-rozvidka-u-sferi-rozshuku-nezakonnih-aktiviv> (дата звернення: 01.05.2026).

**Ревак І. О.,**  
завідувач науково-дослідної лабораторії  
OSINT-досліджень та безпекової аналітики,  
доктор економічних наук, професор  
(Львівський державний університет внутрішніх справ)

## **РОЙОВИЙ ІНТЕЛЕКТ ЯК КОНЦЕПТУАЛЬНА ОСНОВА КОЛЕКТИВНИХ OSINT-РОЗСЛІДУВАНЬ**

Стрімке зростання обсягів відкритих даних, висока швидкість поширення інформації та ускладнення інформаційного середовища формують нові виклики для сучасної аналітичної діяльності. За таких умов індивідуальна обробка інформації дедалі частіше виявляється недостатньою для своєчасного виявлення прихованих взаємозв'язків, слабких сигналів і складних багаторівневих загроз. Це зумовлює посилення ролі колективних форм розвідки з відкритих джерел, у межах яких аналітичний результат формується завдяки взаємодії великої кількості учасників, розподіленому пошуку інформації та колективній верифікації даних.

Однією з перспективних концептуальних моделей пояснення таких процесів є ройовий інтелект, який доцільно розглядати як механізм самоорганізованої колективної поведінки, за якої глобальна аналітична система формується через локальні взаємодії окремих агентів без потреби у жорсткому централізованому управлінні [1]. Для таких систем характерними є самоорганізація, адаптивна координація, розподілене пізнання, колективне виявлення слабких сигналів та виникнення нових аналітичних властивостей у результаті взаємодії елементів системи. У сфері розвідки з відкритих джерел це проявляється через паралельну обробку інформації, розподілений аналіз цифрових слідів, колективне уточнення гіпотез та багатоетапну перевірку результатів.

Особливу роль у функціонуванні ройових аналітичних систем відіграють комунікаційні зв'язки. Саме через них здійснюється поширення сигналів, накопичення колективної обізнаності, формування довіри між учасниками та колективна перевірка інформації. У таких системах комунікація виконує не лише функцію передачі повідомлень, а й формує саму структуру мережевої взаємодії. Внаслідок цього окремі локальні спостереження та фрагментарні дані здатні перетворюватися на цілісну аналітичну картину. Особливого значення набуває непряма взаємодія через спільні середовища даних, графові моделі, колективні бази знань, відкриті сховища інформації та інші інструменти спільної роботи.

Важливим елементом ройового підходу є графова координація, що забезпечує виявлення прихованих зв'язків між сутностями, формування мережевих кластерів та ідентифікацію посередницьких структур. У межах такої моделі доцільно виділяти структурні, функціональні, комунікаційні та класифікаційні зв'язки, сукупність яких формує багаторівневу систему мережевої аналітики. Поєднання таких зв'язків дає змогу виявляти аномальні маршрути, приховані ланцюги взаємодії, нетипові інформаційні кореляції та інші складні форми взаємопов'язаних загроз.

Окремий інтерес становлять OSINT-хакатони та квест-конкурси, які створюють контрольоване середовище для прояву окремих механізмів ройового інтелекту. У межах таких заходів виникають елементи розподіленого пізнання, адаптивного розподілу ролей, колективної верифікації та спільного пошуку аналітичних рішень [2]. Водночас класичні хакатони та квест-конкурси значною мірою ґрунтуються на конкуренції між командами, що

стимулює інтенсивність аналітичної діяльності та швидкість виконання завдань, однак одночасно обмежує рівень відкритого обміну інформацією між учасниками.

На відміну від конкурентної моделі, ройові системи орієнтовані переважно на кооперацію, спільну оптимізацію результатів та накопичення колективного знання. У зв'язку з цим перехід від OSINT-хакатонів та квест-конкурсів до більш наближених до ройового інтелекту моделей передбачає поступове зміщення акценту від міжкомандної конкуренції до мережевої кооперації, спільної верифікації інформації та формування єдиного середовища колективної аналітики. На початкових етапах конкуренція може виконувати роль каталізатора активності й мотивації, однак подальший розвиток ройових систем вимагає формування сталих мережевих спільнот, накопичення колективної пам'яті, розвитку комунікацій та безперервного моніторингу інформаційного середовища.

Водночас ройові моделі аналітики мають і суттєві вразливості. До них належать інформаційні каскади, колективні помилки, когнітивні викривлення, координовані маніпуляції та ризики хибної атрибуції. Це зумовлює необхідність поєднання механізмів самоорганізації з процедурами перевірки достовірності, елементами координації та інструментами аналітичного контролю. У зв'язку з цим найбільш перспективною видається гібридна модель ройового інтелекту, яка поєднує мережеву самоорганізацію, графову аналітику, інструменти автоматизованого аналізу даних, колективну верифікацію та контроль координаційної підсистеми за ухваленням остаточних рішень.

Таким чином, ройовий інтелект доцільно розглядати як одну з перспективних концептуальних основ розвитку колективних OSINT-розслідувань, здатну забезпечити підвищення ефективності виявлення складних мережевих загроз, прихованих взаємозв'язків та слабких сигналів у сучасному інформаційному середовищі.

### **Список використаних джерел**

1. WANG C. et al. Swarm intelligence: A survey of model classification and applications, *Chinese Journal of Aeronautics*. 2025. № 38(3). Pp. 1–20. DOI: <https://doi.org/10.1016/j.cja.2024.03.019>
2. Mukhopadhyay A. et al. OSINT Research Studios: A Flexible Crowdsourcing Framework to Scale Up Open Source Intelligence Investigations, *CSCW, Human-Computer Interaction*. 2024. DOI: <https://doi.org/10.1145/3637382>

**Решетняков М. А.,**  
курсант  
навчально-наукового інституту роботи з персоналом  
(*Національна академія Національної гвардії України*)  
Науковий керівник: **Гриньків О. О.,**  
професор кафедри правових дисциплін,  
доктор юридичних наук  
(*Національна академія Національної гвардії України*)

### **ШІ ТА OSINT У СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ: ПЕРСПЕКТИВИ ЇХ РОЗВИТКУ ДЛЯ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ**

Сучасне безпекове середовище характеризується стрімкою трансформацією загроз: гібридні війни, інформаційні операції противника, кіберагресія та асиметричні методи ведення бойових дій вимагають від силових структур якісно нових підходів до збору, обробки та аналізу інформації [1].

OSINT як методологія збору розвідувальних даних із відкритих джерел (соціальних мереж, новинних агрегаторів, супутникових знімків, геолокаційних сервісів та публічних баз даних) набула особливого значення в умовах повномасштабного вторгнення рф в Україну. Досвід таких організацій, як Bellingcat, InformNapalm та волонтерських OSINT-спільнот, підтвердив: систематизований аналіз відкритих даних здатний забезпечувати розвідувальну цінність, порівняну із класичними методами агентурної розвідки [2].

Підкреслимо, що інтеграція ШІ в OSINT-процеси відкриває принципово нові можливості. По-перше, алгоритми машинного навчання дозволяють опрацьовувати масиви даних, недосяжні для людського аналізу, зокрема за часом і обсягом. Разом із тим, використання ШІ у сфері безпеки пов'язане з низкою системних ризиків, які потребують окремої уваги. Проблема галюцинацій великих мовних моделей генерації правдоподібної, але недостовірної інформації – є критичною в оперативному середовищі, де рішення ухвалюються на основі розвідувальних даних [3].

Застосування геолокації за фотографіями, аналіз руху військової техніки через відкриті джерела та моніторинг комунікацій у відкритому доступі стали невід'ємними елементами інформаційного протистояння. Наприклад, технології обробки природної мови (NLP) забезпечують автоматичний моніторинг і класифікацію публікацій у соціальних мережах, виявлення пропагандистських наративів та їх джерел, відстеження координації інформаційних операцій противника в режимі реального часу [4].

По-друге, технології обробки природної мови (NLP) забезпечують автоматичний моніторинг і класифікацію публікацій у соціальних мережах, виявлення пропагандистських наративів та їх джерел, відстеження координації інформаційних операцій противника в режимі реального часу. Алгоритмічні упередження можуть систематично спотворювати аналітичні висновки. Нарешті, противник також має доступ до аналогічних технологій: дипфейки, синтетичні медіа та автоматизовані інформаційні операції створюють принципово нове середовище інформаційної боротьби. Алгоритмічні упередження можуть систематично спотворювати аналітичні висновки. Водночас, варто зазначити, що противник також має доступ до аналогічних технологій: дипфейки, синтетичні медіа та автоматизовані інформаційні операції створюють принципово нове середовище інформаційної боротьби [5].

Системи комп'ютерного зору здатні автоматично ідентифікувати військову техніку на супутникових знімках, розпізнавати обличчя на відео з відкритих камер, визначати координати місця зйомки за елементами зображення тощо [6].

Ми підтримуємо думку, що для Національної гвардії України як правоохоронного органу зі специфічними завданнями щодо охорони громадського порядку, захисту державних об'єктів і участі в антитерористичних операціях, впровадження зазначених технологій має відбуватись за такими пріоритетними напрямками: автоматизований моніторинг периметрів охоронюваних об'єктів за допомогою ШІ-систем відеоаналізу; OSINT-супровід оперативних завдань для оцінки обстановки в зоні відповідальності; виявлення загроз в інформаційному просторі та протидія деструктивним ІІСО проти особового складу

Таким чином, акцентуємо увагу на тому, що ШІ та OSINT-інструменти не є трендом, а об'єктивною необхідністю для силових структур в умовах сучасності. Ефективність їх впровадження визначається не лише технологічними рішеннями, а й рівнем підготовки особового складу, наявністю чіткої нормативної бази та критичним мисленням операторів, які використовують такі системи. Перспективи України у цій сфері значною мірою залежать від інституційної готовності силових структур до технологічної адаптації та системної інтеграції розвідувальних можливостей нового покоління.

#### **Список використаних джерел**

1. Стратегія національної безпеки України: затверджена Указом Президента України від 14 вересня 2020 р. № 392/2020. URL: <https://www.president.gov.ua>.
2. Higgins E. We Are Bellingcat: Global Crime, Online Sleuths, and the Bold Future of News. Bloomsbury Publishing, 2021. 256 p. URL: [https://www.researchgate.net/publication/364084047\\_We\\_Are\\_Bellingcat\\_Global\\_Crime\\_Online\\_Sleuths\\_and\\_the\\_Bold\\_Future\\_of\\_News\\_By\\_Elliot\\_Higgins\\_New\\_York\\_Bloomsbury\\_Publishing\\_2021](https://www.researchgate.net/publication/364084047_We_Are_Bellingcat_Global_Crime_Online_Sleuths_and_the_Bold_Future_of_News_By_Elliot_Higgins_New_York_Bloomsbury_Publishing_2021)
3. Amershi S. et al. Software Engineering for Machine Learning: A Case Study. *IEEE/ACM International Conference on Software Engineering*. 2019. P. 291–300. URL: [https://www.researchgate.net/publication/335361817\\_Software\\_Engineering\\_for\\_Machine\\_Learning\\_A\\_Case\\_Study](https://www.researchgate.net/publication/335361817_Software_Engineering_for_Machine_Learning_A_Case_Study)
4. Tabarez Rienzi. How OSINT shaped reporting on the war in Ukraine. Centre for Information Resilience. 2025. URL: <https://www.info-res.org/eyes-on-russia/articles/how-osint-shaped-reporting-on-the-war-in-ukraine/>
5. Думчиков М. О. Відкрита розвідка (OSINT) у протидії інформаційним війнам: аналітичні інструменти та правові межі. *Аналітично-порівняльне правознавство*. 2025. Вип. 6. Ч. 2. С. 273–274. DOI: <https://doi.org/10.24144/2788-6018.2025.06.2.43>
6. Івкова В. С., Опірський І. Р. OSINT-технології як загроза кібербезпеці держави. *Кібербезпека: освіта, наука, техніка*. 2025. Т. 3. № 27. С. 165–179. DOI: <https://doi.org/10.28925/2663-4023.2025.27.749>

**Рибка Д. М.,**  
доктор філософії  
(Національна академія Служби безпеки України)

## **РОЛЬ API У МАСШТАБУВАННІ ТА ВЕРИФІКАЦІЇ ДАНИХ В OSINT-ДОСЛІДЖЕННЯХ**

Ми живемо в епоху, коли інформації стає забагато для людського ока, але ніколи не буває забагато для алгоритму. Традиційний OSINT, де аналітик вручну переглядає сторінки соцмереж – це вчорашній день. Як перетворити розвідку на точну науку за допомогою API?

Головний ворог дослідника сьогодні – це «аналітичний параліч». Коли обсяг даних зростає експоненціально, ми втрачаємо фокус. API (програмні інтерфейси) – це наш міст. Вони дозволяють нам не просто «дивитися» на дані, а «черпати» їх у структурованому вигляді. JSON-файли замість скріншотів – ось перший крок до валідності.

Чому це важливо для науки? Бо API забезпечує відтворюваність. У науці результат, який не можна повторити, не вважається істинним. Використовуючи API, ви фіксуєте точку доступу та параметри запиту. Будь-який інший вчений може зробити той самий запит і отримати ті самі дані. Це і є фундамент доказової бази.

Наприклад – деконструкція ботоферм. Як відрізнити щире обурення людей від проплаченої атаки? Вручну – майже неможливо. Але через API ми збираємо таймстампи (мітки часу). Коли ми бачимо, що 500 акаунтів опублікували пост із різницею в 0,8 секунди – у нас є математичний доказ автоматизації. Це не гіпотеза, це цифри. І це те, що ми називаємо «цифровим слідом», який неможливо приховати.

Майбутнє за синергією. Ми вже інтегруємо API з великими мовними моделями (LLM). Це дозволяє нам автоматично аналізувати тональність текстів на 50 мовах одночасно. Але потрібно пам'ятати про етику: використання офіційних API – це ваша страховка та гарантія того, що ваші докази будуть прийняті в будь-якому суді чи міжнародному звіті.

Наукова діяльність в OSINT вимагає суворого дотримання норм етики та права. Використання офіційних API дозволяє досліднику діяти в межах правового поля (зокрема, згідно з нормами GDPR), що є вирішальним фактором для легалізації результатів розслідування у судах або міжнародних звітах. Це створює чітку межу між законним дослідженням та несанкціонованим втручанням у приватне життя.

Автоматизація через API трансформує OSINT з описового інструменту в систему предиктивної аналітики. Це дозволяє досліднику зосередитися на когнітивному синтезі – виявленні прихованих сенсів та стратегічних закономірностей, переклавши рутинний збір даних на алгоритми. Майбутнє галузі полягає у створенні цілісних аналітичних конвеєрів, де API-шлюзи інтегровані з нейронними мережами для автономного виявлення загроз у реальному часі.

Час переходити від ролі «пошуковців» до ролі «архітекторів даних». API – це не просто технічний інструмент, це нова мова сучасної розвідки.

### Список використаних джерел

1. Билень П. Я. Алгоритми розвідки з відкритих джерел: технічні аспекти маніпулювання API та аналізу метаданих. WUNU Digital Library. 2023. URL: wunu.edu.ua (дата звернення: 01.05.2026).
2. Конотоп А. О. OSINT: теорія та методологія : монографія. Київ : AORD, 2024. 240 с. URL: aord.com.ua (дата звернення: 01.05.2026).
3. OSINT: інструменти та методи : навч. посіб. / за ред. А. О. Конотопа. Київ : AORD, 2024. 180 с. URL: aord.com.ua (дата звернення: 01.05.2026).
4. Skopik F. et al. On the Application of Natural Language Processing for Advanced OSINT Analysis in Cyber Defence. Proceedings of the 19th International Conference on Availability, Reliability and Security. Zenodo, 2024. P. 1–10. DOI: doi.org.
5. Дрозд М. І., Нестеренко С. Д. Аналіз програмного забезпечення для реалізації OSINT у сфері інформаційної безпеки. *Вісник ХНУ ім. В. Н. Каразіна, серія «Математичне моделювання»*. 2025. Вип. 66. С. 45–52.
6. Yadav A. et al. Automated OSINT Techniques for Digital Asset Discovery and Reconnaissance. *Computers*. 2025. Vol. 14. Iss. 10. Art. 430. URL: mdpi.com (дата звернення: 01.05.2026).
7. Роль OSINT-досліджень у підвищенні рівня національної безпеки України : матеріали круглого столу (м. Львів, 7 трав. 2025 р.). Львів : ЛьвДУВС, 2025. 112 с.
8. Bazzell M. Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information. 10th ed. [S. l.] : IntelTechniques, 2023. 560 p.

**Рижков Е. В.,**  
професор кафедри інформаційних технологій,  
кандидат юридичних наук, професор  
*(Дніпровський державний університет внутрішніх справ)*

## **ПРИКЛАДНІ АСПЕКТИ ВПРОВАДЖЕННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ТА ВІДЕОАНАЛІТИКИ В ДІЯЛЬНОСТІ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ**

Сучасна архітектура глобальної та національної безпеки перебуває на етапі безпрецедентної технологічної сингулярності, спричиненої стрімкою конвергенцією інструментів розвідки на основі відкритих джерел (Open Source Intelligence, OSINT) та систем штучного інтелекту. В умовах тотальної цифровізації суспільних відносин, експоненційного зростання обсягів неструктурованих даних (Big Data), а також ускладнення транскордонних кримінальних проявів традиційні методи оперативно-розшукової діяльності виявляють свою функціональну та гносеологічну обмеженість. Сьогодні правоохоронні органи стикаються з викликами, які неможливо подолати виключно за рахунок збільшення людського ресурсу; натомість потрібна фундаментальна зміна парадигми аналізу даних.

Особливої гостроти та екзистенційної ваги ця проблематика набуває для Національної поліції України (НПУ) та інших інституцій сектору безпеки і оборони в контексті триваючої повномасштабної збройної агресії. Цифрові сліди стають ключовою, а подекуди — єдиною доказовою базою у розслідуванні воєнних злочинів, актів державного тероризму та колабораційної діяльності на тимчасово окупованих територіях. Відповідно, здатність правоохоронної системи ефективно інтегрувати OSINT-розвідку та автоматизовані аналітичні системи стає питанням не лише ефективності правосуддя, а й національного виживання.

Водночас цей стрімкий перехід супроводжується глибокими юридичними та операційними викликами. Виникає нагальна потреба у формуванні абсолютно нової парадигми нормативно-правового регулювання, яка б змогла збалансувати інноваційний потенціал ШІ з імперативами захисту фундаментальних прав і свобод людини. З огляду на це, висловимо свою позицію щодо окремих прикладних аспектів використання ШІ та OSINT-інструментарію в діяльності правоохоронних органів та окреслимо перспективні напрямки їх імплементації в роботу підрозділів Національної поліції України.

Одним з найбільш революційним, впливовим і водночас найбільш дискусійним напрямком застосування штучного інтелекту в поліцейській діяльності є впровадження систем масової біометричної ідентифікації. Сучасні алгоритми глибинного навчання та згорткові нейронні мережі дозволяють здійснювати автоматизований аналіз топології обличчя, розпізнаючи унікальні біометричні параметри навіть на зображеннях низької якості, перекритих медичними масками, окулярами або в умовах слабкого освітлення [1].

Безпрецедентним кейсом успішного застосування цієї технології в Україні є співпраця державних органів з американською технологічною компанією Clearview AI. Ця компанія розробила унікальну платформу, яка в рамках OSINT-діяльності агрегує мільярди зображень облич, зібраних з відкритих профілів соціальних мереж (Facebook, ВКонтакті, Instagram тощо) по всьому світу.

Однак неймовірна операційна ефективність цієї системи нерозривно пов'язана з формальними порушеннями міжнародного законодавства у сфері захисту персональних даних. Методологія Clearview AI базується на безперервному автоматизованому парсингу (скрапінгу) зображень з інтернету без отримання явної згоди власників цих даних. Тому практика компанії є прямо забороненою в країнах Європейського Союзу [2].

Унікальна ідентифікація людини за допомогою обробки її біометричних даних жорстко регламентується та підпадає під дію Статті 9 Загального регламенту про захист даних (GDPR) [3]. Європейські наглядові органи (зокрема, в Австрії, Франції, Італії) неодноразово визнавали діяльність компанії незаконною та накладали багатомільйонні штрафи.

Для України, яка перебуває в процесі євроінтеграції, це створює складну юридичну дилему. В умовах воєнного стану інтереси національної безпеки та ідентифікація воєнних злочинців мають безумовний пріоритет, що виправдовує використання таких агресивних інструментів в рамках дії інституту крайньої необхідності. Сама перспектива використання штучного інтелекту при реалізації технології OSINT в Україні з урахуванням воєнних та правоохоронних потреб є реальною та пріоритетною [4].

Однак у післявоєнний період Національна поліція зіткнеться з необхідністю адаптації своєї діяльності до міжнародних норм. Це може вимагати повної відмови від комерційних систем глобального скрапінгу на користь створення закритих, юридично верифікованих державних правоохоронних баз даних біометрії злочинців та інструментів їх опрацювання із забезпеченням жорсткого аудиту доступу.

Прикладом такого підходу може слугувати попередній вітчизняний досвід правоохоронців з успішної розробки і функціонування інформаційно-аналітичної системи «Сова» та біометричної системи ідентифікації громадян по зображенню обличчя «Аргус» [5]. Комплекс «Безпечне місто» із відеоконтентом реалізується серед іншого за допомогою відеокамер, обладнаних із «розумними» функціями та поступовою обробкою засобами штучного інтелекту.

Крім юридичного аспекту, необхідно враховувати математичні обмеження самих алгоритмів розпізнавання, що безпосередньо впливає на слідчу практику, бо будь-яка система біометрії оперує ймовірностями, а не абсолютними фактами. Ефективність ШІ-моделі визначається співвідношенням рівня хибних збігів та рівня хибних відхилень. Якщо працівники відповідних Департаментів НПУ налаштують систему на максимальну "чутливість", щоб не пропустити жодного злочинця, це неминуче призведе до сплеску хибного ідентифікування невинних громадян як підозрюваних. Це може спровокувати незаконні затримання та інші обмеження прав громадян. І навпаки, надто "суворі"

налаштування дозволять злочинцям проходити перевірки непоміченими. Отже, результати ШІ-розпізнавання завжди повинні перевірятися досвідченими фахівцям, серед яких аналітик, оперативник, експерт-криміналіст та інші.

Одним із найперспективніших напрямів розвитку концепції Intelligence-Led Policing (поліцейської діяльності, керованої аналітикою) є використання розумних окулярів, інтегрованих із технологіями штучного інтелекту та камерами високої роздільної здатності.

В контексті оперативно-розшукової діяльності та досудового розслідування такий інструмент здатний перетворити звичайний допит чи опитування на високотехнологічний процес вилучення прихованої інформації.

Сучасне програмне забезпечення на базі нейронних мереж здатне здійснювати мультимодальний аналіз стану співбесідника в режимі реального часу або при опрацюванні збереженого відеоконтенту. Такий підхід здатен суттєво компенсувати недостатню обізнаність правоохоронців у прикладних питаннях професійної психології, за допомогою яких ефективність діяльності оперативника і слідчого аксіоматично краща [6; 7].

Розумні окуляри з ШІ для фізіогномічного аналізу створюють ефект "доповненої реальності" безпосередньо під час бесіди, не відволікаючи правоохоронця на екран комп'ютера чи смартфона. Їх використання — це не фантастика, а технологія, яка вже тестується передовими правоохоронними органами світу (наприклад, поліцією Китаю та ОАЕ, а також розробляється підрядниками Міністерства оборони США) [8; 9; 10]. Для Національної поліції України це перспективний інструмент розвідувальної аналітики, який значно посилить інтелектуальний потенціал оперативників та слідчих.

Проте, ця технологія ніколи не замінить професійної інтуїції та критичного мислення правоохоронця — вона слугуватиме лише високоточним "цифровим компасом" у пошуку істини та дієвим інструментом у отриманні оперативної орієнтуючої інформації.

Таким чином, замість повної залежності від зовнішніх комерційних OSINT-рішень, НПУ слід поглиблювати інтеграцію ШІ-алгоритмів біометричної ідентифікації та фізіогноміки у вже існуючі локальні системи, вдосконалювати свої програмно-апаратні комплекси з функціями AI, проводити розробки над суто «правоохоронним ШІ», в тому числі у співпраці з міжнародними партнерами.

Впровадження потужних інструментів біометричної ідентифікації та фізіогноміки вимагає термінового створення галузевого нормативного підґрунтя. Практичним кроком є розроблення нормативних актів використання штучного інтелекту у правоохоронній діяльності. Крім того, необхідно запровадити спеціалізовані тренінги для аналітиків та оперативників НПУ, щоб вони розуміли технічні обмеження систем розпізнавання і не допускали так званої алгоритмічної упередженості чи сліпої довіри до машинних висновків.

## Список використаних джерел

1. Рижков Е. В. Реалізація біометричних систем ідентифікації особи на перепускних пунктах в умовах АТО. *Протидія проявам тероризму, сепаратизму, екстремізму та нелегальній міграції в сучасних умовах: стан, проблеми та перспективи* : матеріали Міжнар. наук.-практ. конф. (м. Дніпро, 28 жовтня 2016 р.). Дніпро : Дніпроп. держ. ун-т внутр. прав, 2016. С. 320–322.
2. Булгакова Д. Заборонена практика компанії Clearview AI, Inc. щодо розпізнавання фотозображень обличчя онлайн. *Слово Національної школи суддів України*. 2025. № 2(51). С. 4–15. URL: <https://slovo.nsj.gov.ua/index.php/ua/arkhiv-nomeriv/2025/2-51-2025/45-2-51-ukr/1081-zaboronena-praktika-kompaniji-clearview-ai-inc-shchodo-rozpiznavannya-fotozobrazhen-oblich-onlajn>
3. Регламент (ЄС) 2016/679 Європейського Парламенту і Ради від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, що скасовує Директиву 95/46/ЄС (Загальний регламент про захист даних). URL: [https://zakon.rada.gov.ua/laws/show/984\\_008-16#Text](https://zakon.rada.gov.ua/laws/show/984_008-16#Text)
4. Рижков Е. В. Перспективи використання штучного інтелекту при реалізації технології OSINT. *Міжнародна та національна безпека: теоретичні і прикладні аспекти* : матеріали ІХ Міжнар. наук.-практ. конф. (м. Дніпро, 21 бер. 2025 р.) ; у 2-х ч. Дніпро : Дніпров. держ. ун-т внутр. справ, 2025. Ч. II. С. 459–461.
5. Гуславский В. С., Задорожний Ю. А., Розовский Б. Г. Информационно-аналитическое обеспечение раскрытия и расследования преступлений : монография. Луганск : Изд-во «Элтон-2», 2008. 136 с.
6. Використання психологічних знань в оперативно-розшуковій діяльності : монографія / О. Ф. Долженков, Г. Є. Запорожцев, А.П. Кіцул, Е. В. Рижков. Одеса : НДРВВ ОІВС, 2001. 231 с.
7. Рижков Е. В. Вивідування інформації та її експрес оцінка. *Актуальні проблеми розкриття та розслідування злочинів у сучасних умовах* : матеріали Всеукраїнської науково-практичної конференції (м. Запоріжжя, 3 1 жовтня 2008). У двох частинах. Запорізький юридичний ін-т ДДУВС, 2008. Ч. 1. С. 204 – 206.
8. Xloong – Surveillance Watch (AR startup developing smart glasses for Chinese police). Surveillance Watch. URL: <https://www.surveillancewatch.io/entities/xloong>.
9. Police to use 'smart glasses' to catch criminals in Abu Dhabi. The Express Tribune. 2017. URL: <https://tribune.com.pk/story/1528775/police-use-smart-glasses-catch-criminals-abu-dhabi>.
10. Dalton J. Intelligent Immersion: Integrating AI and XR for Enhanced Military Training and Decision-Making (Partnership between Meta and Anduril Industries). Rabdan Security and Defence Institute. 2025. URL: <https://rsdi.ae/en/publications/intelligent-immersion-integrating-ai-and-xr-for-enhanced-military-training-and-decision-making>.

## **OSINT ЯК ІНСТРУМЕНТ ДОКУМЕНТУВАННЯ ВОЄННИХ ЗЛОЧИНІВ І ВЕРИФІКАЦІЇ ЦИФРОВИХ ДОКАЗІВ**

Під час війни в Україні питання фіксації воєнних злочинів стало особливо важливим. Через бойові дії та небезпеку не завжди є можливість працювати безпосередньо на місці подій, тому значна частина інформації збирається з відкритих джерел - соціальних мереж, новин, фото та відео. Такі матеріали часто з'являються дуже швидко і можуть містити важливі свідчення про події.

Велику роль у цьому процесі відіграють державні органи, зокрема Офіс Генерального прокурора України [0] та Центр протидії дезінформації при РНБО [2], які займаються збором, перевіркою та систематизацією інформації. Водночас до цього процесу долучаються журналісти, аналітики та звичайні користувачі мережі, що дозволяє швидше знаходити та поширювати дані.

Однак важливо не лише зібрати інформацію, а й переконатися в її достовірності. У мережі є багато неправдивих або змінених матеріалів, тому використовуються різні способи перевірки-визначення місця події, аналіз деталей на фото чи відео, порівняння з іншими джерелами. Це допомагає зрозуміти, чи можна вважати ці дані доказами.

Крім того, важливо правильно зберігати зібрані матеріали, адже вони можуть бути видалені або змінені. Для цього використовуються різні цифрові інструменти, які дозволяють зафіксувати інформацію у незмінному вигляді. Усе це робить можливим подальше використання таких даних у розслідуваннях і судах.

Таким чином, використання відкритих джерел і сучасних технологій стало важливою частиною процесу документування воєнних злочинів і допомагає встановлювати правду про події навіть у складних умовах війни.

OSINT (Open Source Intelligence) - це отримання та аналіз інформації з відкритих джерел. До таких джерел належать соціальні мережі, новинні сайти, відео- та фотоматеріали, карти, супутникові знімки та інші доступні онлайн-ресурси. На відміну від закритої інформації, ці дані може знайти практично будь-хто, але їх потрібно правильно обробити й перевірити.

У сучасних умовах цей стиль розвідки став дуже важливим інструментом, особливо під час війни. Він дозволяє швидко отримувати інформацію про події навіть там, де немає доступу для журналістів чи слідчих. Наприклад, відео з місця події або фото, опубліковане в соціальних мережах, може допомогти встановити факт обстрілу чи інші обставини.

Важливою перевагою є можливість перевірки інформації. Дані з одного джерела можна порівняти з іншими, що дозволяє підвищити їхню достовірність. Саме тому відкриті джерела часто використовуються не лише для отримання інформації, а й для її підтвердження.

Значний внесок у розвиток роблять міжнародні спільноти, зокрема Bellingcat[4]. Вони показують, як за допомогою відкритих даних можна проводити повноцінні розслідування та встановлювати важливі факти.

Після збору інформації з відкритих джерел її обов'язково потрібно перевірити, адже в інтернеті поширюється багато неправдивих або змінених матеріалів. Без цього такі дані не можуть використовуватися як докази, тому верифікація є одним із ключових етапів роботи з цифровою інформацією.

Одним із основних методів є геолокація-визначення місця, де було зроблено фото або відео. Для цього аналізують будівлі, дороги, ландшафт, написи та інші деталі, які потім порівнюють із картами або супутниковими знімками. Навіть дрібні елементи, як-от форма дахів чи розташування дерев, можуть допомогти встановити точне місце події.

Також важливо визначити час події. Це роблять за допомогою аналізу тіней, погодних умов, сезонних ознак або метаданих файлів. Наприклад, положення сонця чи стан рослинності може вказати на приблизний час або період зйомки.

Ще одним важливим методом є крос-перевірка інформації-зіставлення даних із різних джерел. Якщо одна й та сама подія підтверджується кількома незалежними матеріалами, це значно підвищує довіру до неї. Також використовується аналіз метаданих, який може містити інформацію про дату створення або пристрій.

Наприклад, аналітики Bellingcat[4] перевіряють відео з місць бойових дій, порівнюючи об'єкти на записах із супутниковими знімками. Вони звертають увагу на розташування будівель, дороги та інші деталі, що дозволяє точно визначити місце події.

Крім цього, застосовується візуальний аналіз-уважне вивчення фото та відео для виявлення можливих ознак редагування або змін.

У процесі документування воєнних злочинів важливо не лише зібрати та перевірити інформацію, а й зробити це відповідно до міжнародних правил. Це потрібно для того, щоб зібрані матеріали могли бути використані як докази у суді, зокрема в міжнародних інстанціях.

Одним із головних документів у цій сфері є Berkeley Protocol on Digital Open Source Investigations [5]. Він визначає основні принципи роботи з інформацією з відкритих джерел і пояснює, як правильно збирати, перевіряти, зберігати та представляти цифрові докази.

Згідно з цим протоколом, дуже важливо забезпечити автентичність даних, тобто довести, що вони не були змінені. Також потрібно зберігати їх у такому вигляді, щоб можна було підтвердити їх походження. Окрема увага приділяється дотриманню прав людини, зокрема під час збору та поширення інформації.

Крім того, протокол наголошує на необхідності чіткої фіксації всіх етапів роботи з доказами-від моменту їх отримання до використання в суді. Це дозволяє уникнути сумнівів щодо їх достовірності.

Таким чином, міжнародні стандарти допомагають зробити процес документування більш надійним і забезпечують можливість використання цифрових доказів у правовому полі.

Після збору та перевірки інформації важливо правильно її зберегти. Це пов'язано з тим, що матеріали з інтернету можуть бути швидко видалені, змінені або стати недоступними. Якщо їх не зафіксувати вчасно, важливі докази можуть бути втрачені.

Для цього використовуються різні способи архівування. Наприклад, створюються копії веб-сторінок, зберігаються оригінальні фото та відео, а також фіксуються метадані файлів. Це дозволяє зберегти інформацію в тому вигляді, в якому вона була знайдена.

Також важливо забезпечити цілісність даних-тобто гарантувати, що після збереження вони не змінювались. Для цього можуть використовуватись спеціальні цифрові інструменти та сховища, які дозволяють контролювати доступ до файлів і відстежувати будь-які зміни.

Окрему увагу приділяють систематизації матеріалів. Зібрані дані потрібно впорядкувати, щоб у разі необхідності їх можна було швидко знайти та використати. Це особливо важливо під час проведення розслідувань або підготовки матеріалів для суду [3].

Попри те, що OSINT є дуже корисним інструментом, його використання має і певні труднощі. Насамперед це велика кількість інформації в інтернеті, серед якої багато неправдивих або спеціально змінених матеріалів. Це ускладнює процес пошуку та перевірки достовірних даних [2].

Ще однією проблемою є складність верифікації. Не всю інформацію можна легко перевірити, особливо якщо вона походить із маловідомих або анонімних джерел. У таких випадках потрібно витратити більше часу та використовувати кілька методів перевірки.

Також важливим є рівень підготовки фахівців. Робота з відкритими джерелами потребує не лише технічних навичок, а й уважності, критичного мислення та досвіду. Без цього є ризик помилок або неправильних висновків.

На кінець можна сказати, що використання відкритих джерел стало важливою частиною документування воєнних злочинів. OSINT дає можливість отримувати інформацію навіть тоді, коли немає доступу до місця подій, а також перевіряти її за допомогою різних методів.

### **Список використаних джерел**

1. Офіс Генерального прокурора України. Фіксація та розслідування воєнних злочинів. URL: <https://www.gp.gov.ua>
2. Центр протидії дезінформації при РНБО. URL: <https://cpd.gov.ua>
3. Міністерство цифрової трансформації України. Цифрові інструменти документування злочинів. URL: <https://thedigital.gov.ua>
4. Bellingcat. Open Source Investigations. URL: <https://www.bellingcat.com>
5. Berkeley Protocol on Digital Open Source Investigations, 2020. URL: <https://www.ohchr.org>

**Ряшко О. В.,**  
доцент кафедри  
кримінального процесу та криміналістики,  
кандидат юридичних наук, доцент  
*(Львівський державний університет внутрішніх справ)*

## **ВИКОРИСТАННЯ ВІДКРИТИХ ДЖЕРЕЛ ІНФОРМАЦІЇ OSINT ТА ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПОШУКУ БЕЗВІСТИ ЗНИКЛИХ ОСІБ ЗА ОСОБЛИВИХ ОБСТАВИН**

На сьогоднішній день болюча проблема безвісно зниклих осіб є однією з найгостріших та найактуальніших у сфері захисту прав людини. На превеликий жаль, масштаби насильницьких зникнень, депортацій та порушень особистої безпеки невпинно збільшуються. За таких обставин, традиційні підходи та методи щодо розшуку (опитування свідків, патрулювання, робота з архівами) не завжди спрацьовують у повній мірі. У зв'язку з цим зростає потреба у впровадженні високотехнологічних підходів до розшукової діяльності, серед яких особливе місце посідає OSINT, який охоплює систематичний збір, обробку та аналіз інформації з відкритих джерел, таких як соціальні мережі, інтернет-форуми, цифрові бази даних, супутникові знімки, новинні ресурси, блоги, карти та сервіси геолокації.

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 [1, с. 200]

Такі ресурси створюють аналітичні продукти, які не просто здатні суттєво доповнити традиційні можливості кримінального аналізу, а подекуди навіть замінити їх в повній мірі. OSINT забезпечує можливості виявлення цифрових слідів зниклої особи через її публікації, коментарі, профілі та взаємодії в соціальних мережах, окрім цього аналіз та синтез геопросторових даних дозволяє припустити версію відносно останнього місця перебування або маршруту пересування такої особи, сюди ж віднесемо й можливість ідентифікації особи на фото- та відеоматеріалах за допомогою технологій розпізнавання обличь, перевірку соціальних контактів з метою виявлення та встановлення зв'язків між зниклими особами.

Сам процес збирання, перевірки та оцінки інформації, в якій містяться докази воєнних злочинів представляють собою складний механізм. Це стосується як технічних, так і правових та етичних аспектів, що в свою чергу вимагає залучення різного роду стратегій. Найбільша проблема щодо фіксації та збору цифрового контенту полягає у гарантіях автентичності та збереженні. Розпізнати справжні докази від шахрайського/ або фальшивого контенту стає все складніше [2, с. 906]

Розвиток штучного інтелекту (ШІ) надає надзвичайно широкі можливості щодо обробки великих обсягів неструктурованих даних. За допомогою повідомлень із соціальних мереж, інформації з камер відеоспостереження, перехоплених розмов можливо відновлювати хід події, виявляти активності, що викликають підозру або ж встановлювати місце можливого

перебування зниклої особи. Україні, фактично із початком повномасштабного вторгнення, надали можливість використання такої системи штучного інтелекту як «Clearview», яку в Україні використовують не лише для ідентифікації загиблих, а й живих людей.

Цілком зрозуміло, що використання сучасних технологій, на кшталт біометричних та генетичних методів ідентифікації, цифрових інформаційних систем та алгоритмів штучного інтелекту під час розшуку безвісно зниклих військовослужбовців має здійснюватися із дотриманням тактичних правил та врахування умов воєнного стану [3]

Попри велику користь OSINT у розслідуваннях, існує низка проблем, які обмежують його ефективність. Зокрема, це автентичність даних. верифікація інформації є критично важливою, адже в інтернеті поширюється багато фейкових новин та маніпуляцій. Крім того, необхідно звернути увагу на юридичні аспекти, тому що у багатьох судових процесах докази, отримані через OSINT, можуть бути оскаржені через відсутність офіційного підтвердження. Етичні питання, пошук та використання персональних даних осіб можуть викликати заперечення щодо конфіденційності та прав людини. Технічні бар'єри, так як деякі відкриті дані можуть бути складними для обробки без спеціального програмного забезпечення [4, с.347]

Аналіз інтернет-ресурсів, супутникових знімків, відкритих баз даних та інших джерел, використання штучного інтелекту як інструменту обробки великого обсягу інформації, дозволяє оперативно фіксувати докази злочинів, верифікувати та перехресно підтверджувати інформацію з різних незалежних джерел, підвищуючи її достовірність. Аналіз та огляд фото- та відеоматеріалів, інших цифрових слідів, геопросторових даних, проведені із дотриманням належної процесуальної форми, часто є незамінними у процесі збирання, перевірки та оцінки доказів, які можуть бути використані в національних та міжнародних судових процесах [5, с.152].

У сфері розшуку безвісно зниклих осіб OSINT забезпечує можливість: - виявлення цифрових слідів зниклої особи через її публікації, коментарі, профілі та взаємодії в соціальних мережах; - аналізу геопросторових даних для встановлення останнього місця перебування або маршруту пересування; - ідентифікації особи на фото- та відеоматеріалах за допомогою технологій розпізнавання обличчя; - побудови зв'язків між зниклими особами, подіями та місцями через візуалізацію соціальних графів або аналіз контактів [6, с.32]

Як велику перевагу активного OSINT можна виокремити значно глибше розуміння дослідником ситуації, що значно перевершує можливості пасивного OSINT. Його застосування відкриває доступ до відомостей, прихованих від загалу. Практичним прикладом використання активного OSINT є: застосування програм для збору даних із соціальних мереж, взаємодія з користувачами в мережі, використання інструментів для виявлення прихованих відомостей. Вибір між пасивним і активним OSINT базується на ваших специфічних потребах, що постають перед аналітиками. У випадку потреби у відомостях, що вже є у вільному доступі, пасивний OSINT — оптимальний варіант. В інших випадках активний OSINT може продемонструвати вищу ефективність. Велика кількість засобів, що використовуються в теперішніх розслідуваннях, розроблені виключно для однієї цілі — відшукування телефонних номерів, або електронних адрес, або «nickname» користувачів. Проте, важливо зауважити, що збільшується кількість інструментів, спроектованих для одночасного пошуку в десятках — а то й сотнях — різних джерел [7, с.818–819]

### Список використаних джерел

1. Свиридчук Н. OSINT в умовах воєнного стану. 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.
2. Тома М. Г., Василюва О. В. Інструменти OSINT: фіксація воєнних злочинів в Україні. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2025. № 02. С. 905–909 DOI: <https://doi.org/10.24144/2788-6018.2025.02.134>
3. Шепеленко Д. К., Прокопов С. О. Штучний інтелект у сфері інформаційного забезпечення Національної поліції. 2024. URL: <https://er.dduvs.edu.ua/bitstream/123456789/14158/1/181.pdf> (дата звернення: 01.06.2025)
4. Погоріла С. І. Використання OSINT-технологій у розслідуванні воєнних злочинів: сучасний стан і перспективи. *Актуальні проблеми сучасної науки в дослідженнях молодих учених, курсантів та студентів* : тези доп. Всеукр. наук.-практ. конф. (м. Вінниця, 16 трав. 2025 р.) / МВС України, Харків. нац. ун-т внутр. справ ; Нац. акад. правових наук України. Вінниця : ХНУВС, 2025. С. 346–348.
5. Третяк С. В., Квашук О. Д. Значення OSINT-технологій у розслідуванні воєнних злочинів. *Кримінальний аналіз і кібербезпека: об'єднання зусиль для нових викликів* : збірник тез Науково-практичної конференції (м. Одеса, 23 травня 2025 року). Одеса : Одеський державний університет внутрішніх справ, 2025. С. 150–152.
6. Коношко В., Подрез О., Рижков Е. OSINT у роботі з безвісті зниклими особами. *UNIVERSUM*. 2025. № 22. С. 31–36. URL: <https://archive.liga.science/index.php/universum/article/view/1886>
7. Правове регулювання дотримання прав і свобод людини та громадянина в умовах адміністративно-правового режиму воєнного стану : колективна монографія / Є. Львова, О. Жильцов, О. Пасько та ін. ; за заг. ред. А. В. Денисової. Одеса : Видавництво «Юридика», 2025. 840 с.

**Савайда О. І.,**  
старший науковий співробітник  
науково-дослідної лабораторії  
вивчення проблем протидії торгівлі людьми  
навчально-наукового інституту з підготовки  
фахівців для підрозділів кримінальної поліції,  
кандидат юридичних наук, доцент  
*(Львівський державний університет внутрішніх справ)*

**Фукал А. Д.,**  
здобувач вищої освіти  
*(Львівський державний університет внутрішніх справ)*

## **РОЛЬ OSINT-СПІЛЬНОТ У ЗАБЕЗПЕЧЕННІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ДОТРИМАННІ ПРАВ ЛЮДИНИ: ВЗАЄМОДІЯ ДЕРЖАВИ ТА ВОЛОНТЕРІВ**

У сучасну епоху «прозорих кордонів» та тотальної цифровізації концепція національної безпеки зазнала фундаментальних змін. Традиційна монополія державних інституцій на збір, опрацювання та аналіз стратегічно важливої інформації остаточно відійшла в минуле. Поява та стрімкий розвиток розвідки на основі відкритих джерел (Open Source Intelligence, OSINT) змінили архітектуру сучасних конфліктів. Особливу роль у цій новій парадигмі відіграють волонтерські OSINT-спільноти. Вони не просто допомагають державі, а стають самостійними суб'єктами інформаційного простору, здатними завдяки своїй мобільності, технологічним можливостям та гнучкості випереджати у своєму здоров'ї навіть можливості самої держави. У контексті гібридної агресії (так, наприклад як це відбувається зараз в нас в Україні) волонтерський OSINT став першою лінією оборони, що забезпечує прозорість подій та швидку ідентифікацію прихованих загроз [1].

Взаємодія між офіційними безпековими структурами та цивільними дослідниками (такими як Bellingcat, InformNapalm, DeepStateUA або «Molfar») базується на принципі стратегічного партнерства. Держава володіє повноваженнями та легітимними інструментами примусу, тоді як волонтери цього напрямку мають унікальну перевагу – великий масштаб та відсутність жорстких протоколів, що дозволяє проводити аналіз гігантських масивів даних у реальному часі. Ефективність цієї синергії проявляється у трьох основних напрямках:

1. Інформаційна стійкість: так, наприклад, українські волонтери моніторять логістику ворога, переміщення техніки та будівництво фортифікацій через аналіз супутникових знімків та випадкових фото у мережі, що дає державі змогу отримувати незалежне підтвердження розвідданих [2, С. 10].

2. Боротьба з дезінформацією: У часи «постправди» OSINT-спільноти виступають ефективними спеціалістами, які перевіряють достовірність інформації, звітів, заяв та медіаконтенту, виявляючи фейки, маніпуляції та пропаганду. Швидка геолокація пропагандистських роликів дозволяє миттєво спростовувати ворожі фейки, надаючи світовій спільноті неспростовні цифрові докази [3, С. 128].

3. Кібер-соціальна взаємодія: Держава забезпечує правову «парасольку» та канали для передачі критичної інформації (наприклад, через чат-боти або офіційні платформи), що перетворює тисячі громадян на активних учасників системи національної безпеки [4, С. 82].

Найбільш вагомим гуманітарним аспектом діяльності OSINT-спільнот є трансформація розвідки у правозахисний інструмент. Традиційно розвіддані були засекреченими, проте волонтерський OSINT є публічним, що робить його ключовим для захисту прав людини в умовах збройних конфліктів. При документуванні та фіксації воєнних злочинів, а особливо коли агресор блокує доступ міжнародним спостерігачам та правоохоронцям до місць подій, цифрові дослідники стають «віртуальними свідками». Аналіз відео з реєстраторів, телефонів військових та камер спостереження дозволяє детально відтворити хронологію злочинів у містах (наприклад, Буча, Ірпінь, Маріуполь). Це забезпечує реалізацію права на правду та право на життя.

Під час ідентифікація, а також в притягнення до відповідальності OSINT дозволяє виявити військові злочини та злочинців, встановлюючи їхні імена, посади та приналежність до конкретних підрозділів за допомогою алгоритмів розпізнавання обличчя та соціальних мереж [5, р. 60]. Це відновлює порушене право жертви на справедливий суд. Зібрані волонтерами дані сьогодні для України стають основою для розслідувань Міжнародного кримінального суду (МКС), перетворюючи цифрові докази на юридичні аргументи, які не мають терміну давності [6, р. 25]. Також в гуманітарній складовій та пошуку осіб важливою є роль OSINT у розшуку зниклих безвісти та депортованих. Аналізуючи кадри з російських пропагандистських ресурсів, волонтери допомагають ідентифікувати незаконно вивезених дітей, встановлювати місця їх перебування та сприяти їх поверненню [7]. Це прямий механізм відновлення права на сім'ю та особисту недоторканність

Попри очевидну користь, діяльність OSINT-спільнот породжує низку правових та етичних викликів. Головний конфлікт виникає між безпековою доцільністю та правом людини на приватність (Стаття 8 ЄКПЛ) [8, с.430]. Масовий збір та публікація персональних даних можуть нести загрозу життю та здоров'ю людей, які не є прямими учасниками бойових дій або були помилково ідентифіковані. Ризик помилкової ідентифікації є критичним. В історії OSINT відомі випадки, коли через візуальну схожість або помилкову геолокацію невинні люди ставали об'єктами цькування та переслідувань [9, р. 54.]. Це порушує презумпцію невинуватості та право на захист честі і гідності. Тому виникає потреба у верифікації даних за «подвійним стандартом» – перед тим, як інформація стане публічною, вона повинна пройти перехресну перевірку незалежними групами. Держава в цьому процесі має виступати регулятором, який каналізує активність волонтерів у межі закону, запобігаючи перетворенню розвідки на інструмент онлайн-самосуду.

Сьогодні OSINT-спільноти є невід'ємною частиною архітектури національної безпеки демократичних держав. Взаємодія держави та волонтерів створила нову модель «розвідки на демократичних засадах», де прозорість є головною зброєю проти агресії. Проте для того, щоб цей інструмент залишався легітимним, він потребує чіткої інституціоналізації. Основним орієнтиром для майбутнього розвитку є впровадження норм Берклійського протоколу [10, р.15]. Це дозволить стандартизувати збір цифрових доказів так, щоб вони беззаперечно приймалися судами будь-якої юрисдикції. Держава має створити правове поле, у якому волонтери отримують визнання та захист, а їхні напрацювання служать не лише поточним тактичним цілям, а й довгостроковій меті – глобальному відновленню справедливості та захисту фундаментальних прав людини.

### Список використаних джерел

1. Захист кіберпростору: монографія / Ю. М. Ткач, М. Є. Шелест, В. О. Хорошко, І. М. Дюба, Д. В. Кальченко. Ніжин : ТПК «Орхідея» ФОП Лук'яненко В. В., 2024. 240 с.
2. Горбулін В. П., Даник Ю. Г. Національна безпека України: сучасні виклики та загрози. *Стратегічна панорама*. 2022. № 1. С. 5–15.
3. Почепцов Г. Г. Інформаційні війни та дезінформація: теорія і практика. Київ : Видавничий дім «Києво-Могилянська академія», 2021. 256 с.
4. Дубов Д. В. Цифрове суспільство та кібербезпека: виклики сучасності. Київ : НІСД, 2020. 192 с.
5. Bellingcat's Online Investigation Toolkit. 2022. 150 p.
6. Policy on Open Source Evidence. The Hague, 2023. 72 p.
7. Офіс Генерального прокурора України. Звіт про воєнні злочини проти дітей в Україні. Київ, 2024. 120 с.
8. Савайда О. І Свобода вираження поглядів (за матеріалами практики ЄСПЛ). *Міжнародний захист прав людини України* : навчальний посібник / кол. авторів ; за ред. О. Б. Онишко. Львів : ЛьвДУВС, 2022. 540 с. С. 427–467.
9. Guidelines for Addressing Online Disinformation and Protecting Freedom of Expression. Vienna, 2021. 98 p.
10. The Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law. New York; Geneva: United Nations, 2020. 128 p. [https://www.ohchr.org/sites/default/files/Documents/Publications/OHCHR\\_BerkeleyProtocol.pdf](https://www.ohchr.org/sites/default/files/Documents/Publications/OHCHR_BerkeleyProtocol.pdf)

**Сашуріна О.,**  
доктор філософії  
(Харківський національний університет  
внутрішніх справ)

## **ПСИХОЛОГІЧНІ АСПЕКТИ ВИКОРИСТАННЯ ВІДКРИТИХ ДЖЕРЕЛ ДЛЯ ПОШУКУ ТА АНАЛІЗУ ІНФОРМАЦІЇ В УМОВАХ ВОЄННОГО СТАНУ**

Сучасний етап розвитку інформаційного суспільства характеризується стрімким збільшенням обсягів інформації, яка перебуває у відкритому доступі. Соціальні мережі, цифрові платформи, месенджери, супутникові знімки, відкриті бази даних, медіаресурси та інші джерела формують надзвичайно широкий інформаційний простір, який активно використовується у сфері безпеки, правоохоронної діяльності, журналістики, міжнародного правосуддя та наукових досліджень. У таких умовах особливого значення набуває методологія OSINT (Open Source Intelligence), що передбачає пошук, збір, аналіз та інтерпретацію інформації з відкритих джерел.

В умовах воєнного стану та збройної агресії російської федерації проти України використання OSINT стало одним із ключових інструментів документування воєнних злочинів, виявлення фактів порушення міжнародного гуманітарного права, ідентифікації осіб, причетних до злочинної діяльності, а також протидії дезінформації та інформаційно-психологічним операціям. Водночас така діяльність супроводжується значними психологічними навантаженнями, які потребують окремого наукового осмислення.

Психологічний аспект використання відкритих джерел інформації полягає насамперед у специфіці сприйняття, обробки та оцінки великих масивів даних. OSINT-дослідник працює в умовах постійного інформаційного потоку, що потребує високого рівня концентрації уваги, аналітичного мислення, здатності до швидкого прийняття рішень та навичок критичної оцінки інформації. При цьому ефективність аналітичної діяльності значною мірою залежить від психологічної стійкості особи, її здатності протидіяти когнітивним викривленням та інформаційним маніпуляціям.

Однією з ключових психологічних проблем у сфері OSINT є когнітивне перевантаження. Велика кількість інформації, що надходить одночасно з різних джерел, створює ризик зниження якості аналітичної діяльності, втрати важливих деталей та формування помилкових висновків. Особливо актуальною ця проблема є під час воєнного стану, коли інформаційний простір характеризується високою динамічністю, емоційною насиченістю та значною кількістю дезінформаційного контенту.

У процесі аналізу відкритих джерел дослідник може піддаватися впливу когнітивних викривлень, серед яких найбільш поширеними є ефект підтвердження власної позиції, упереджене сприйняття інформації, ефект першого враження та емоційна інтерпретація подій. Небезпека таких викривлень особливо зростає в умовах війни, коли інформація часто має високий рівень емоційного впливу та супроводжується психологічним тиском.

Важливим психологічним аспектом OSINT-досліджень є вплив візуального контенту, пов'язаного з воєнними злочинами. Під час документування фактів убивств цивільного населення, катувань, руйнувань об'єктів цивільної інфраструктури або інших наслідків збройної агресії дослідники змушені систематично працювати з травматичними матеріалами. Тривалий контакт із такими даними може призводити до вторинної травматизації,

професійного вигорання, емоційного виснаження та розвитку симптомів посттравматичного стресового розладу.

Особливої уваги заслуговує проблема десенсибілізації – поступового зниження емоційної реакції на насильство та людські страждання. У контексті документування воєнних злочинів така психологічна адаптація може мати подвійний характер. З одного боку, вона дозволяє досліднику ефективніше виконувати професійні завдання в умовах емоційного навантаження, а з іншого – створює ризик втрати емпатії, моральної чутливості та гуманістичного сприйняття наслідків війни.

У сучасних умовах інформаційної війни значний психологічний вплив здійснюють дезінформаційні кампанії та інформаційно-психологічні операції. Ворог активно використовує соціальні мережі, анонімні телеграм-канали, фальсифіковані фото- та відеоматеріали, технології deepfake для маніпуляції громадською думкою, деморалізації населення та дискредитації органів державної влади. У зв'язку з цим одним із ключових психологічних компонентів ефективного OSINT-аналізу стає розвиток критичного мислення та інформаційної гігієни.

Критичне мислення дозволяє аналітику здійснювати багаторівневу перевірку інформації, оцінювати достовірність джерел, встановлювати причинно-наслідкові зв'язки та уникати маніпулятивного впливу. Важливу роль у цьому процесі відіграють навички емоційної саморегуляції, оскільки надмірна емоційна залученість може негативно впливати на об'єктивність аналізу та якість прийнятих рішень.

Особливого значення психологічні аспекти OSINT набувають у процесі документування воєнних злочинів. Відкриті джерела дедалі частіше використовуються як доказова база у діяльності міжнародних слідчих органів, правозахисних організацій та правоохоронних структур. Фото- та відеоматеріали, геолокаційні дані, супутникові знімки, публікації у соціальних мережах дозволяють встановлювати обставини вчинення злочинів, маршрути переміщення військової техніки, факти обстрілів цивільних об'єктів та ідентифікувати причетних осіб.

Однак специфіка такої діяльності полягає в необхідності поєднання аналітичної точності з психологічною витривалістю. Дослідник повинен не лише перевірити достовірність інформації, а й зберегти професійну об'єктивність в умовах високого емоційного навантаження. Крім того, важливо враховувати ризик маніпулятивного використання емоційно забарвленого контенту для формування викривленого сприйняття подій.

Суттєве значення має також психологічна підготовка фахівців, які здійснюють OSINT-дослідження у сфері воєнних злочинів. Така підготовка повинна включати розвиток стресостійкості, навичок саморегуляції, критичного мислення, психологічної адаптації до роботи з травматичним контентом та методів профілактики професійного вигорання. Доцільним є впровадження систем психологічної підтримки для аналітиків, які тривалий час працюють із матеріалами, пов'язаними з наслідками війни.

Таким чином, психологічні аспекти використання відкритих джерел інформації є важливою складовою сучасних OSINT-досліджень. В умовах воєнного стану їх значення суттєво зростає у зв'язку з необхідністю ефективного протистояння інформаційним загрозам, документування воєнних злочинів та забезпечення інформаційної безпеки держави. Ефективність OSINT-аналізу значною мірою залежить не лише від технічних навичок дослідника, а й від його психологічної підготовки, здатності критично оцінювати інформацію, протидіяти маніпулятивному впливу та зберігати професійну стійкість в умовах тривалого стресу.

**Світличний В. А.,**  
доцент кафедри, кандидат технічних наук, доцент  
*(Харківський національний університет внутрішніх справ)*  
**Вітвіцька К. Е.,**  
здобувач вищої освіти  
*(Харківський національний університет внутрішніх справ)*

## **МЕТОДОЛОГІЯ ІДЕНТИФІКАЦІЇ ЦИФРОВИХ ПРИМАНОК (HONEYTOKENS) У СИСТЕМІ ЗАХОДІВ КОНТР-OSINT**

У сучасних умовах глобальної цифровізації та ведення мережецентричних воєн, розвідка на основі відкритих джерел (OSINT) перетворилася на стратегічний інструмент отримання переваги. Проте ефективність OSINT-заходів змушує протилежну сторону розробляти та впроваджувати агресивні методи контррозвідки (контр-OSINT). Одним із найбільш дієвих засобів у цьому арсеналі є використання дезінформаційних «приманок» або honeytokens. Це цифрові об'єкти, що не мають реальної цінності, але імітують конфіденційні дані (паролі, ключі доступу, бази даних), щоб спровокувати дослідника на активну взаємодію. Головна мета такої приманки — ініціювати «зворотний зв'язок» із сервером зловмисника, розкриваючи IP-адресу, геолокацію та технічні характеристики робочої станції аналітика [1]. Таким чином, здатність ідентифікувати honeytokens на етапі пасивного збору даних є критичною компетенцією для фахівців підрозділів кіберполіції та кримінального аналізу.

Процес ідентифікації honeytokens базується на принципі прихованої сигналізації (web-beacons або call-home triggers). Коли дослідник завантажує або відкриває такий об'єкт, виконується мережевий запит до сервера управління, який реєструє факт доступу. Для мінімізації ризиків розроблено методологію детекції пасток, яка базується на виявленні аномалій у структурі та метаданих об'єктів. Аналіз технічних характеристик дозволяє виділити чотири основні вектори детекції.

По-перше, визначальним фактором є сигнатурний аналіз метаданих. Більшість сервісів створення приманок, як-от Canarytokens, використовують фіксовані шаблони (blueprints), що призводить до появи статичних цифрових відбитків. Дослідження [2] показують, що PDF-приманки часто мають розмір рівно 5 КБ, документи Word — 15 КБ, а таблиці Excel — 7,7 КБ. У метаданих таких об'єктів спостерігаються незмінні унікальні ідентифікатори (DocumentID, InstanceID) та «заморожені» дати створення, які не корелюють із часом публікації ресурсу. Для безпечної перевірки цих параметрів критично використовувати інструменти пасивного аналізу, наприклад exiftool, що дозволяє зчитувати теги без рендерингу вмісту файлу, який міг би активувати прихований веб-маяк (web-beacon) [6].

По-друге, критичне значення має детекція патернів унікальних ідентифікаторів. Функціонування honeytokens базується на зверненні до унікальної URL-адреси або DNS-хосту під час взаємодії. Аналіз структури таких посилань дозволяє виявити алфавітно-цифрові послідовності фіксованої довжини — найчастіше це випадковий рядок із 25 символів [2]. Якщо в структурі піддомену або шляху до файлу спостерігається подібний довгий нечитабельний код, це з високою ймовірністю вказує на токен. Фахівцю слід уникати навіть спроб резолвінгу таких адрес, оскільки звичайний DNS-запит фіксує факт інтересу з боку конкретного IP, що є сигналом для сил контр-OSINT.

По-третє, важливим етапом є статична декомпіляція виконуваних об'єктів. Приманки у форматі exe- або dll-файлів часто містять жорстко закодовані артефакти, специфічні для відкритих бібліотек виявлення вторгнень. Використання утиліти strings дозволяє виявити текстові рядки на кшталт «Canarytoken» [3], шляхи до налагоджувальних символів (PDB-шляхи) або ідентичні сертифікати цифрового підпису, що повторюються в масових реалізаціях. Додатково рекомендується застосовувати спеціалізоване програмне забезпечення, як-от PowerShell-модуль HoneyPotBuster [7], який автоматизує пошук специфічних API-викликів, характерних для дезінформаційних об'єктів.

Нарешті, невід'ємною частиною перевірки є контекстно-логічний аудит облікових записів та документів. Honeytokens часто маскуються під «привабливі» цілі (high-value targets): паролі адміністраторів, конфіденційні списки або облікові записи з провокаційними іменами («secret», «database\_pass»). Ознаками пастки є аномально свіжі або занадто старі дати останньої зміни пароля, а також повна відсутність активності в системних журналах для «адміністративного» акаунта. Складні системи можуть імітувати реальний трафік, проте невідповідність контексту (наприклад, знаходження файлу з паролями у відкритому доступі на другорядному ресурсі) має сприйматися як індикатор загрози [5].

Таким чином, ефективність розпізнавання honeytokens залежить від системного підходу: поєднання технічного аналізу артефактів із логічною оцінкою контексту їх розміщення.

Протидія контр-OSINT заходам вимагає від дослідника переходу від кількісного накопичення інформації до її якісної верифікації. Жоден метод не забезпечує 100% гарантії виявлення індивідуально налаштованих пасток, проте системне поєднання аналізу метаданих, перевірки мережевих ідентифікаторів та статичної декомпіляції дозволяє суттєво підвищити безпеку OSINT-операцій. Впровадження цих технік у практику підготовки кадрів для правоохоронних органів є необхідним кроком для забезпечення надійності доказової бази та безпеки особового складу в умовах сучасної кібервійни.

### Список використаних джерел

1. Honeysweeper: Towards Stealthy Honeytoken Fingerprinting Techniques / M. Msaad, S. Srinivasa, M. M. Andersen et al. *Secure IT Systems : 27th Nordic Conference, NordSec 2022 (Reykjavik, Iceland, Nov. 30 – Dec. 2, 2022) : Proceedings*. Cham : Springer, 2023. С. 101–119. DOI: 10.1007/978-3-031-22295-5\_6.
2. Srinivasa S., Pedersen J. M., Vasilomanolakis E. Towards Systematic Honeytoken Fingerprinting. *Proceedings of the 13th International Conference on Security of Information and Networks (SIN 2020)*. New York : Association for Computing Machinery, 2020. Article No. 28. P. 1–5. DOI: 10.1145/3433174.3433599.
3. Canarytokens – Open-source honeytoken service / Thinkst Applied Research. URL: <https://canarytokens.org> (дата звернення: 28.04.2026).
4. Honeytoken Protection for CrowdStrike Falcon / Acalvio Technologies. URL: <https://www.acalvio.com/solutions/honeytokens-for-crowdstrike> (дата звернення: 28.04.2026).
5. Understanding Honeytokens: A Key to Proactive Cybersecurity / SecurityHive. URL: <https://www.securityhive.io/de/blog/honeytokens-in-cybersecurity> (дата звернення: 28.04.2026).
6. ExifTool – Online Investigation Toolkit / Bellingcat. URL: <https://bellingcat.gitbook.io/toolkit/more/all-tools/exiftool> (дата звернення: 28.04.2026).
7. HoneyPotBuster – PowerShell Module for Honeytoken Detection / Javelin Networks. URL: <https://github.com/JavelinNetworks/HoneyPotBuster> (дата звернення: 28.04.2026).

**Стеценко Я. В.,**  
здобувач вищої освіти  
(*Національний юридичний університет  
імені Ярослава Мудрого*)

## **ВИКОРИСТАННЯ ІНСТРУМЕНТІВ OSINT-АНАЛІЗУ ДЛЯ ВИЯВЛЕННЯ ФЕЙКОВИХ ДОКУМЕНТІВ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ: ПОРУШЕННЯ СТАНДАРТІВ ДІЛОВОДСТВА ТА ЛІНГВІСТИЧНІ МАРКЕРИ**

В сучасних умовах постійних гібридних конфліктів інформаційний простір перетворився на повноцінне поле бою, де маніпуляція суспільною свідомістю здійснюється поряд із класичними збройними операціями. Серед численних форм інформаційно-психологічного впливу особливу небезпеку становить фальсифікація офіційних документів органів державної влади. На відміну від фейкових публікацій у соціальних мережах або відеоматеріалів на YouTube, які можуть бути відносно швидко ідентифіковані критично налаштованим користувачем, підроблені накази, постанови та розпорядження від імені українських міністерств і відомств експлуатують глибинний психологічний механізм — апеляцію до інституційного авторитету держави. Він суттєво знижує поріг критичного сприйняття навіть у підготовленої аудиторії, що обумовлює підвищену суспільну небезпечність такого виду інформаційно-психологічних операцій (ІПСО).

Актуальність дослідження посилюється стрімким розвитком генеративних нейромереж і великих мовних моделей, які дозволяють відтворювати бланки, реквізити та підписи посадовців із фотореалістичною точністю, що суттєво ускладнює виявлення підробок традиційними методами. За таких умов інструменти розвідки на основі відкритих джерел (OSINT) набувають критичного значення як засіб оперативної верифікації офіційних документів.

З огляду на тему доповіді, на мою думку, є доцільним розглянути реальні кейси застосування даних методів для ідентифікації фейкових нормативно-правових актів через виявлення порушень стандартів діловодства та лінгвістичних помилок.

Зокрема, наприкінці серпня 2024 року безпосередньо напередодні початку нового навчального року через мережі проросійських медіа та Telegram-каналів було розповсюджено скан-копію нібито офіційного наказу Міністерства освіти і науки України № 498 від 19 серпня 2024 року з назвою «Про скорочення бюджетних навчальних місць для чоловіків призовного віку» [1]. Вибір теми документа був не випадковим: апеляція до болісних для суспільства питань мобілізації та права на освіту мала спровокувати широке емоційне поширення матеріалу. Верифікація документа засобами OSINT дозволила встановити низку беззаперечних ознак підробки.

По-перше, зміст документа є юридично нікчемним. Пункт 1 фейкового наказу зобов'язує міністра одноосібно скоротити кількість бюджетних навчальних місць, що суперечить чинному законодавству: обсяг державного замовлення на підготовку фахівців затверджується виключно постановою Кабінету Міністрів України, тоді як Міністерство освіти і науки наділене лише правом внесення відповідних пропозицій до Уряду, але не правом самостійного перегляду зазначених показників.

По-друге, у тексті преамбули «наказу» міститься посилання на Указ Президента України № 69/2022, тоді як введення воєнного стану було закріплено Указом № 64/2022 [2]. Некоректне цитування базового нормативного акта є характерним маркером документа,

підготовленого особою, яка не має практичного досвіду роботи з правовою системою України та, ймовірно, спиралася на неперевірені вторинні джерела.

По-третє, документ не відповідає вимогам ДСТУ 4163:2020 «Уніфікована система організаційно-розпорядчої документації». Відповідно до п. 5.32 цього стандарту, розпорядчі акти органів виконавчої влади мають містити відмітку про наявність примірника документа в електронній формі – QR-код або штрих-код Системи електронного документообігу (СЕД), розміщений у нижньому лівому куті лицьового боку першого аркуша [3]. Відсутність такого коду однозначно свідчить про те, що документ ніколи не проходив процедури офіційної реєстрації.

По-четверте, пошук наказу № 498 від 19.08.2024 у законодавчій базі Верховної Ради України не дав жодного результату, що обґрунтовано ставить під сумнів можливість його офіційного існування.

По-п'яте, застосування методу зворотного пошуку зображень у поєднанні з моніторингом Telegram-каналів через сервіс TGStat дозволило встановити першоджерела поширення. Серед каналів, які першими опублікували фейковий документ, були «Медведь», «Шаман Раху», «Кот Костян – офіційний канал» – ресурси, безпосередньо пов'язані з проросійськими пропагандистськими мережами.

Для підтвердження системності та актуальності досліджуваної проблематики, вважаю доцільним розглянути ще один схожий, але не менш цікавий випадок. У липні 2024 року подібна кампанія була спрямована проти Міністерства охорони здоров'я України – через ті самі канали розповсюджувався документ, нібито виданий під № 476 від 15 липня 2024 року, що нібито передбачав переобладнання єдиної дитячої лікарні у Краматорську на військовий шпиталь [3]. Цільова аудиторія була свідомо обрана з урахуванням максимального емоційного резонансу – тема охорони здоров'я дітей в умовах воєнного конфлікту здатна спровокувати некритичне поширення навіть серед осіб, які в іншій ситуації перевіряли б джерело.

Верифікація виявила той самий набір ознак підробки, що й у першому випадку. Пошук наказу № 476 від 15.07.2024 у базі «Законодавство України» та на офіційному вебсайті Міністерства охорони здоров'я підтвердив, що такий акт ніколи не видавався. Порівняльний аналіз бланка з офіційними документами МОЗ знову продемонстрував відсутність QR-коду або штрих-коду СЕД, що унеможливорює будь-яку версію про «витік» офіційного документа.

Особливу доказову цінність у цьому випадку мали лінгвістичні маркери. Текст документа містив скорочення «г. Краматорськ» замість нормативного «м. Краматорськ», де «г.» є аббревіатурою від російського «город». Крім того, використана конструкція «переформатувати дитячу лікарню до військового шпиталю» є прямою граматичною калькою з російської мови: нормативний відповідник в українській — «переформатувати лікарню у військовий шпиталь». Подібні синтаксичні та лексичні аномалії є надійними індикаторами того, що текст підготовлено носієм російської мови або машинно перекладено без редакторської правки. Аналіз мережі поширення підтвердив, що первинний «вкид» відбувся через ту саму мережу проросійських інформаційних ресурсів.

Порівняльний аналіз обох випадків дозволяє констатувати відтворення єдиної структурної моделі інформаційної операції: вибір теми з максимальним потенціалом соціального резонансу (мобілізація, здоров'я дітей) → виготовлення документа з імітацією офіційних реквізитів → одночасне масоване поширення через мережу анонімних і

псевдоанонімних Telegram-каналів. Уніфікованість цієї схеми свідчить систематичне й скоординоване її застосування як інструменту ІІСО.

Водночас аналіз демонструє стабільно низький рівень якості підробок із точки зору відповідності нормам вітчизняного діловодства. Це може пояснюватися двома чинниками: по-перше, розрахунком на аудиторію, необізнану з вимогами ДСТУ 4163:2020 та порядком реєстрації розпорядчих актів; по-друге, необхідністю швидкого виготовлення матеріалу в умовах інформаційної кампанії, що не залишає часу на ретельне опрацювання деталей. З огляду на розвиток генеративних нейромереж, зокрема таких інструментів, як Stable Diffusion і DALL-E 3, здатних відтворювати печатки та підписи з фотореалістичною точністю, якість підробок у найближчій перспективі неминуче зростатиме, що підвищуватиме вимоги як до інструментів верифікації, так і до кваліфікації аналітиків.

На мою думку, існує наступні основні причини необхідності протидіяти цьому методу дезінформації: 1) використання слабких місць у суспільстві – держава-агресор використовує повагу до державних інституцій і хоча публікація в соціальних мережах може не викликати довіри, «офіційний документ з підписом міністра» або будь-якого іншого посадовця високого рангу стане більш актуальним і більш достовірним для людей; 2) порушення єдиного правового поля держави – кожний фейковий нормативний акт спотворює правову реальність у свідомості громадян.

Проведений аналіз засвідчує, що навіть базове застосування OSINT-методів – перевірка нормативних реєстрів, порівняльний аналіз офіційних бланків, лінгвістична і правова експертиза тексту – дозволяє однозначно ідентифікувати ознаки підробки, які не витримують фахового нормативного і мовознавчого аудиту.

Таким чином, OSINT є не лише інструментом ретроспективного фактчекінгу, а й дієвим механізмом системної протидії ІІСО, що ґрунтуються на використанні фальсифікованих офіційних документів. Опанування базових методів OSINT-верифікації є необхідною компетентністю як для представників державних органів, так і для громадянського суспільства в умовах триваючого гібридного конфлікту.

### **Список використаних джерел**

1. Гук Л. Фейк: МОН скорочує кількість бюджетних навчальних місць для чоловіків призовного віку. *Бахмут IN.UA*. 2024. 23 серп. URL: <https://bahmut.in.ua/fejk-mon-skorochuye-kilkist-byudzhethnyh-navchalnyh-misz-dlya-cholovikiv-pryzovnogo-viku/> (дата звернення: 30.04.2026).
2. Про введення воєнного стану в Україні : Указ Президента України від 24 лют. 2022 р. № 64/2022. *Законодавство України*. URL: <https://zakon.rada.gov.ua/laws/show/64/2022> (дата звернення: 30.04.2026).
3. Державна уніфікована система документації. Уніфікована система організаційно-розпорядчої документації. Вимоги до оформлення документів : ДСТУ 4163:2020. Київ : ДП «УкрНДНЦ», 2020. 25 с. URL: [https://zakon.help/files/article/11494/%D0%94%S0%A1%D0%A2%D0%A3%204163\\_2020.pdf](https://zakon.help/files/article/11494/%D0%94%S0%A1%D0%A2%D0%A3%204163_2020.pdf) (дата звернення: 30.04.2026).
4. Гук Л. Фейк: МОЗ переобладнає єдину дитячу лікарню в Краматорську на військовий шпиталь. *Бахмут IN.UA*. 2024. URL: <https://bahmut.in.ua/moz-pereobladnaeye-dyynu-dytyachu-likarnyu-v-kramatorsku-na-vijskovyj-shpytal/> (дата звернення: 30.04.2026).

**Тищенко С. С.,**  
курсант 2 курсу факультету № 1  
з підготовки фахівців для органів досудового  
розслідування Національної поліції  
(*Львівський державний університет внутрішніх справ*)

## **РОЛЬ OSINT-ДОСЛІДЖЕНЬ У ВИЯВЛЕННІ, АНАЛІЗІ ТА ПРОТИДІІ ПРОПАГАНДИ ТА ДЕЗІНФОРМАЦІЇ В УМОВАХ ВІЙНИ В УКРАЇНІ**

Сучасна війна в Україні є прикладом гібридного конфлікту, у якому інформаційна складова відіграє системну роль поряд із військовими, політичними та економічними чинниками. Інформаційний простір став окремим полем протистояння, де активно використовуються пропаганда, дезінформація та різноманітні інформаційні операції, спрямовані на вплив на суспільну думку, дестабілізацію ситуації та підрив довіри до офіційних джерел інформації.

На тлі воєнної агресії роль пропаганди зростає настільки, що людина під її впливом втрачає здатність аналізувати інформацію і сприймає всі факти тільки під кутом зору, сформованим пропагандою [1, с. 526]. У таких умовах поширення неправдивої або маніпулятивної інформації набуло масового характеру. Як свідчать сучасні дослідження, інформаційні кампанії у межах російсько-української війни включають системне створення фейкових новин, викривлення фактів та поширення альтернативних наративів, що формують спотворену картину подій. Подібні дії ускладнюють розуміння реальної ситуації навіть для професійних аналітиків та журналістів.

Відкрита розвідка (Open Source Intelligence) – OSINT-дослідження, – є одним з ключових інструментів протидії інформаційним війнам, дезінформаційним кампаніям та гібридним загрозам у сучасному цифровому середовищі [2, с. 273]. Ці дослідження базуються на зборі, перевірці та аналітичній обробці інформації з відкритих джерел. До таких джерел належать соціальні мережі, медіа-ресурси, супутникові знімки, державні реєстри та інші публічно доступні дані. Сучасна практика показує, що OSINT перетворився на важливий елемент як журналістських розслідувань, так і аналітики безпеки.

Значення OSINT у контексті війни в Україні полягає передусім у можливості оперативного отримання та перевірки інформації з місць подій. Методи OSINT передбачають збір та аналіз загальнодоступної інформації з широкого кола онлайн-джерел для перевірки точності та достовірності заяв. Для проведення OSINT-аналізу можна використовувати широкий спектр обчислювальних інструментів шляхом збору та обробки контенту, отриманого з різних онлайн-платформ, таких як веб-сайти соціальних мереж, новинні статті, форуми, онлайн-карти та веб-архіви [3, с. 1]. Проводяться дослідження фото- та відеоматеріалів, геолокацій, аналіз часових характеристик інформаційних повідомлень та їх порівняння із іншими джерелами. Це дає змогу ефективно виявляти випадки маніпуляцій та дезінформації.

Безумовно, вагомим значенням набуває функція OSINT у виявленні пропаганди. Пропагандистські матеріали зазвичай мають системний характер і спрямовані на формування певного емоційного або політичного ефекту. За допомогою аналізу відкритих джерел можна визначати закономірності поширення таких матеріалів, виявляти першоджерела та встановлювати мережі їх розповсюдження. Як показують дослідження інформаційних кампаній у соціальних мережах, OSINT дозволяє не лише фіксувати окремі випадки дезінформації, але й досліджувати структуру інформаційних атак, зокрема шляхом застосування методів виявлення спільнот, які дають змогу ідентифікувати окремі кластери партійності, теми та дезінформацію, підкреслюючи складну динаміку поширення інформації в соціальних мережах [4, с. 1].

Важливою є також аналітична функція OSINT, яка полягає у системному дослідженні інформаційного середовища. Зокрема, аналіз великих масивів даних із відкритих джерел дає змогу виявляти інформаційні патерни, визначати активність певних інформаційних каналів та оцінювати рівень впливу дезінформаційних кампаній. OSINT сьогодні використовується не лише для збору інформації, але й для її структурованого аналізу у межах інформаційної війни.

У контексті війни в Україні OSINT набув особливого значення як інструмент документування подій. Аналітичні спільноти та дослідницькі організації активно використовують відкриті дані для фіксації воєнних злочинів, перевірки інформації з поля бою та документування руйнувань. Саме OSINT став одним із ключових інструментів формування доказової бази у межах розслідувань воєнних злочинів.

Крім того, OSINT відіграє важливу роль у протидії інформаційним операціям, спрямованим на міжнародну аудиторію. Поширення фейків та маніпуляцій у глобальному інформаційному просторі часто має на меті вплив на політичні рішення, зниження підтримки України та формування альтернативних інтерпретацій подій.

Фахівці OSINT ретельно досліджують онлайн-дані, вони можуть надати перспективи та факти про конфлікт, які часто залишаються непомітними для журналістів. Це допомагає проникнути крізь туман війни, встановлюючи правду про окремі інциденти, що відбуваються на місцях. Ретельне вивчення кожної події важливе для побудови загальних наративів про успіх та легітимність війни, особливо враховуючи, що росія прагне сфабрикувати новини, щоб ескалювати свій наступ. Провідні OSINT-організації у таких країнах як Велика Британія, Нідерланди, Україна співпрацюють, щоб підтримувати живу картину на основі понад 1000 інцидентів – від військових втрат до жертв серед цивільного населення та бомбардувань – використовуючи зображення з соціальних мереж та геолокацію [5]. Відкриті джерела дають змогу оперативно спростовувати подібні твердження та надавати перевірену інформацію.

OSINT виступає як один із найбільш ефективних підходів до протидії інформаційним загрозам. Його перевага полягає у відкритості, можливості швидкої перевірки даних та залученні широкого кола аналітиків, включаючи журналістів, дослідників та громадські ініціативи. Як свідчить практика, саме колективний характер OSINT-аналізу підвищує точність та надійність отриманих результатів.

Таким чином, OSINT-дослідження виконують комплексну функцію у сучасному інформаційному просторі: вони дають можливість виявляти пропаганду та дезінформацію, здійснювати їх аналітичну обробку та забезпечувати ефективну протидію інформаційним загрозам. В умовах війни в Україні їх роль постійно зростає, оскільки інформаційний фронт стає невід'ємною складовою загального протистояння.

### **Список використаних джерел**

1. Варга Т. М. Дезінформація та пропаганда як інструменти ведення гібридної війни Росії проти України. *Аналітично-порівняльне правознавство*. 2024. С. 526–531. URL: <https://journal-app.uzhnu.edu.ua/article/view/317216/307740>
2. Думчиков М. О. Відкрита розвідка (OSINT) у протидії інформаційним війнам: аналітичні інструменти та правові межі. *Аналітично-порівняльне правознавство*. 2025. Вип. 6. Ч. 2. С. 273–277. URL: <https://journal-app.uzhnu.edu.ua/article/view/346448/333429>
3. Khan S. A. et al. Online Multimedia Verification with Computational Tools and OSINT: Russia-Ukraine Conflict Case Studies. 2023. 18 p. URL: <https://arxiv.org/pdf/2310.01978>
4. OSINT or BULLSHINT? Exploring misinformation dynamics in the Russo-Ukrainian war. 2025. 8 p. URL: <https://arxiv.org/pdf/2508.03599>
5. Freear M. OSINT in an Age of Disinformation Warfare. *Royal United Services Institute*. 2022. URL: <https://www.rusi.org/explore-our-research/publications/commentary/osint-age-disinformation-warfare>

**Токар П. Т.,**  
начальник ГУНП в Харківській області,  
старший викладач кафедри  
юридичних дисциплін  
(за сумісництвом), кандидат юридичних наук  
(Сумська філія Харківського національного  
університету внутрішніх справ)

**Кріцак І. В.,**  
помічник начальника ГУНП в Харківській області,  
професор кафедри права та суспільних наук  
(за сумісництвом), кандидат юридичних наук, доцент  
(Вінницький фінансово-економічний університет)

**Кобилєв О. А.,**  
начальник відділу розслідування злочинів,  
учинених в умовах збройного конфлікту  
(СУ ГУНП в Харківській області)

## **OSINT І НИНІШНЯ РОСІЙСЬКО-УКРАЇНСЬКА ВІЙНА: ВІД НАУКОМЕТРІЇ ДО ПРАКТИЧНИХ АСПЕКТІВ РОЗСЛІДУВАННЯ ВОЄННИХ ЗЛОЧИНІВ**

**Нинішня російсько-українська війна очима зарубіжних дослідників.**  
*Наукометричний зріз міжнародних наукових статей на платформі Web of Science присвячених «OSINT».* Сьогодні на платформі Web of Science розміщено понад 400 наукових статей, де зустрічається ключове слово «OSINT». Усі вони потребують свого детального перечитання/опрацювання. Нам вдалося переглянути абсолютну більшість анотацій даних наукових статей. Найбільш цікавий/важливий матеріал відображений у даній науковій праці. Водночас наступним, принципово важливим етапом дослідження стане поглиблений, системний аналіз кожної з відібраних наукових статей як ключовий крок до формування узагальнених висновків і науково обґрунтованих положень.

Розгортання російської військової агресії в Україні актуалізувало пошук додаткових джерел інформації про бойові дії. Війна показала, що офіційні прокремлівські ЗМІ поширюють відверту пропаганду. Отже, попит на незалежну та оперативну інформацію про ситуацію на фронті призвів до появи індивідуальних спостерігачів, які використовують доступні платформи для своєї діяльності. Тут важливо проаналізувати інтернет-платформи як альтернативні джерела інформації про російсько-українську війну [1].

25 лютого 2022 року російські війська взяли під контроль Чорнобильську АЕС після тривалих боїв у Чорнобильській зоні відчуження. Впродовж березня відбувалися постійні події, що підвищили ризик потенційного забруднення раніше незабруднених територій та можливого впливу на здоров'я людей і стан довкілля. Війна призвела до переривання звичайних профілактичних заходів, а датчики радіаційного моніторингу не працювали. Відкриті джерела інформації можуть бути корисними, коли офіційні звіти та дані недоступні. Дані з відкритих джерел можуть надати цінну інформацію та раннє попередження про потенційні радіаційні небезпеки в умовах війни, де може бракувати офіційних повідомлень та заходів щодо їхнього пом'якшення, що дозволить вчасно вжити заходів з реагування на надзвичайні ситуації та охорони громадського здоров'я [2].

Останніми роками кібератаки стають дедалі поширенішими в усьому світі. Зокрема, у триваючій війні між росією та Україною активно використовуються технологічні засоби. Росіяни застосовують різні види атак з різних причин, наприклад, для розвідки з метою збору інформації про критично важливі системи України. Вкрай важливо вміти скласти профілі таких атак для їхньої ідентифікації та розробки інших стратегій, спрямованих на запобігання подібним атакам у майбутньому. Техніки аналізу даних можуть використовуватися для профілювання хакерів як державами, так і правоохоронними органами та організаціями. Профілювання хакерів може допомогти краще підготуватися до кібератак та реагувати на них. Тут важливим є використання технік аналізу даних для профілювання російських хакерів. Іншим важливим аспектом є набір даних, який буде використовуватися, – OSINT. Набір даних з відкритим кодом було обрано через його безплатність, придатність для досліджень та широку доступність. Для навчання запропонованих предикторів використовуються різні алгоритми класифікації з метою обрання найнадійнішої та найточнішої моделі. Сьогодні надважливим є краще розуміння відомих російських хакерських угруповань, що може сприяти кращій підготовці та реагуванню на кіберінциденти за участю таких суб'єктів загрози. Уряди держав, дослідники та правоохоронні органи можуть використовувати розроблену модель у поєднанні з іншими методами для швидкого виявлення атак з боку російських АPT-груп, надання рекомендацій щодо заходів контролю та розробки детальної стратегії протидії таким атакам, що покращить безпеку та конфіденційність даних [3].

*Прогнозування соціальної напруги в Україні (2026–2027): байєсівське моделювання, OSINT та аналітика великих даних.* М. Згуровський, М. Слюсаревський наголошують, що у період війни та глибоких суспільних перетворень українське суспільство засвідчує значну мінливість соціально-психологічних реакцій, що підкреслює необхідність кількісного вимірювання соціальної напруги як показника суспільної рівноваги. В умовах стрімких змін традиційні соціологічні методи не забезпечують своєчасного прогнозування кризових процесів, адже не враховують нелінійність соціальної динаміки та вплив емоційних та інформаційних чинників. Це створило нагальну потребу в когнітивно-аналітичній моделі, здатній інтегрувати великі масиви даних, експертні оцінки та байєсівські методи прогнозування в режимі реального часу. Автори пропонують міждисциплінарний підхід до прогнозування соціальної напруги в Україні на середньострокову перспективу (2026–2027 рр.) з використанням байєсівського моделювання, аналізу прогнозних сценаріїв, моніторингу відкритих джерел інформації (OSINT) та інструментів штучного інтелекту. Вченими розроблено цифрову аналітичну платформу N-SH для розрахунку показника соціальної напруги в режимі реального часу, проведення сентиментного та емоційного аналізу публічних комунікацій, а також формування часових рядів суспільних настроїв. Модель виявила циклічну динаміку соціальної напруги в Україні у 2000–2025 рр., з піковим значенням SH, близьким до 9, у 2022 році та тенденцією до стабілізації на підвищеному рівні у 2025–2027 рр. Аналіз прогнозних сценаріїв визначив три базові траєкторії розвитку – контрольований мир, тривала стагнація та ескалація й розлад – з оцінкою їхніх ймовірностей за допомогою байєсівського апостеріорного розподілу [4].

**OSINT та важливість його ефективної реалізації за нинішніх умов.** З огляду на наміри ООН щодо глобальної взаємодії до 2030 року, кіберрозвідка стає основною сферою людського виміру, здатної впливати на зміни в геополітичній динаміці. У кіберпросторі новим полем бою є свідомість людей, де застосовуються такі нові засоби, як зловживання соціальними мережами з метою маніпулювання інформацією, обман з боку активістів та дезінформація. Автори пропонують систему аналізу настроїв із функцією виявлення аномалій (SAAD).

Ця масштабна та модульна система використовує підхід OSINT-Deep Learning для дослідження настроїв у соціальних мережах з метою прогнозування підозрілих аномальних тенденцій у публікаціях Twitter. Виявлення аномалій досліджується за допомогою нового напівнаглядного процесу, здатного виявляти потенційно небезпечні ситуації в критичних сферах [5].

Р. Шет, Ч. Пареха наголошують, що у сучасному мінливому цифровому світі отримання точної та актуальної інформації має вирішальне значення для кібербезпеки, аналізу конкуренції та наукових досліджень. Завдяки технологіям відкритого розвідувального аналізу (OSINT) соціальні мережі та цифрові платформи стали важливими джерелами даних. Важливо порівнювати різні системи OSINT для збору даних, різноманітні інструменти OSINT, класифікувати їх за функціональністю, зручністю використання та ефективністю, зокрема веб-скрейпери, засоби аналізу соціальних мереж, аналізатори доменів та пошукові системи. Кожен інструмент оцінюється на основі можливостей збору даних, точності результатів, доступності модулів та зручності використання. Основна мета – допомогти особам, зокрема потерпілим, науковцям, практикам у прийнятті обґрунтованих рішень під час вибору інструментів розвідки з відкритих джерел (OSINT) для вилучення необхідної інформації [6].

Файли даних, фотографії та відео в мережі Інтернет є величезними джерелами інформації про особу, яка їх опублікувала. Ці файли містять відомості про зовнішність, поведінку, погляди та матеріальний стан. Аналіз цих файлів допомагає перевірити достовірність змісту та спосіб їхнього створення. Таку інформацію часто публікують соціальні мережі, такі як Facebook, Twitter та Instagram. Публічні бази даних надають інформацію про підприємства, корпорації та громадських діячів, забезпечуючи доступ до даних про поїздки урядовців, наукових статей та репутації компаній. Ці ресурси допомагають зрозуміти можливості співпраці та визначити потенційних партнерів. Відкриті джерела інформації (OSINT) – це сукупність інструментів та методів для вилучення інформації з загальнодоступних джерел. Вони допомагають перевірити точність та автентичність інформації, як це було засвідчено під час розслідування ФБР у 2020 році щодо жінки з Філадельфії, яка брала участь у протестах та готувала цілеспрямовані атаки, такі як спірфішинг [7].

Автори Р. Гіоні, М. Таддео, Л. Флоріді відзначають, що сьогодні розвідка на основі відкритих джерел (OSINT), тобто інформація, отримана з загальнодоступних джерел, становить від 80 до 90 відсотків усієї розвідувальної діяльності, що здійснюється правоохоронними органами (LEA) та розвідувальними службами на Заході. Розвиток у сферах аналізу даних, машинного навчання, візуальної криміналістики та, що найважливіше, зростання обчислювальної потужності, доступної для комерційного використання, дозволили фахівцям з OSINT пришвидшити, а іноді навіть автоматизувати збір та аналіз розвідданих, отримуючи точніші результати швидше. У міру розширення інфосфери, що пристосовується до дедалі більшої присутності в Інтернеті, розширюється й масив корисної інформації OSINT. Ці зміни викликають серйозні занепокоєння щодо наслідків у сфері управління, етики, права та суспільства (GELSI). Поряд зі стандартними проблемами конфіденційності виникають нові та надзвичайно важливі питання щодо нагляду, адже деякі з більш досконалих інструментів аналізу даних майже не потребують нагляду. Вченими проаналізовано 571 публікацію з метою оцінки сучасного стану літератури щодо використання OSINT на базі штучного інтелекту (та розробки програмного забезпечення OSINT) у контексті рамки GELSI, висвітлено потенційні прогалини та запропоновано нові напрямки досліджень [8].

Сучасний збір та аналіз відкритих джерел розвідки (OSINT) стикається з такими проблемами, як низька ефективність збору та обробки інформації, обмежене охоплення та значна суб'єктивність, що ускладнює задоволення практичних потреб. Існує нагальна потреба у підвищенні рівня ефективності методів OSINT. Останнім часом дедалі більшої уваги привертає контент, створений за допомогою штучного інтелекту. Технології генеративного штучного інтелекту, завдяки таким процесам, як видобуток даних, попередня обробка, навчання моделей, генерація контенту, а також простежуваність та верифікація, можуть зробити збір та аналіз OSINT більш гнучкими та ефективними [9].

*Досвід Італії у сфері OSINT.* Революція в інформаційних технологіях робить відкриті джерела більш доступними, поширеними та цінними. Міжнародні розвідувальні спільноти за останні роки спостерігають, що відкриті джерела стають дедалі доступнішими та дешевшими. До 80 % електронних даних є текстовими, а найцінніша інформація часто міститься на сторінках, які не мають структури та не є засекреченими. Тому процес доступу до цих неопрацьованих даних, що відрізняються за мовою, та їх перетворення на інформацію нерозривно пов'язаний із поняттями текстового аналізу та синтезу, що значною мірою залежить від уміння вирішувати проблеми багатомовності. SYNTHEMA SPYWatch – це система забезпечення контенту для OSINT, яку було впроваджено в деяких оперативних структурах розвідки в Італії для підтримки циклу збору, обробки, використання, створення, поширення та оцінки інформації. За допомогою цієї системи оперативні співробітники можуть отримати загальний огляд великих обсягів текстових даних, що допомагає їм виявляти значущі подібності між документами та знаходити всю пов'язану інформацію [10].

*Словацький досвід використання OSINT.* Відкриті джерела інформації (OSINT) надають актуальні дані про нові методи кібератак, групи зловмисників, зміни в IT-продуктах, оновлення політик, останні події у сфері безпеки та багато іншого. Часто десятки аналітиків досліджують безліч джерел, збирають, класифікують, групують та ранжують новини з відкритого та даркнету, щоб підготувати найбільш релевантну інформацію для осіб, що приймають рішення. Інструментом, що підтримує цю роботу, є «Taranis NG» від словацького CERT. Це рішення збирає інформацію з багатьох типів джерел, таких як веб-сайти, RSS-канали, електронні листи та соціальні мережі, і робить її доступною для пошуку. Воно також підтримує створення звітів та щоденних підсумків. Однак кількість джерел та новин постійно зростає, що ускладнює їхній пошук виключно вручну. Ці обставини вимагають застосування нових методів обробки природної мови (NLP) для підвищення ефективності аналізу OSINT. [11].

Термін «доксинг» походить від слова «документи» і означає збір інформації про організацію чи особу за допомогою соціальних мереж, пошукових систем, методів злому паролів, інструментів соціальної інженерії та інших джерел загальнодоступної інформації. Головною метою атак доксингу є погрози, приниження, переслідування та приниження організації чи особи. Для здійснення доксингу використовуються різноманітні інструменти. Такі інструменти, як Maltego, візуалізують архітектуру організації, що допомагає визначити слабкі ланки в її структурі [12].

Проект ePOOLICE спрямований на розробку ефективної та дієвої стратегічної системи раннього попередження, що використовує аналіз зовнішнього середовища для раннього виявлення та попередження про існуючі, нові та майбутні загрози з боку організованої злочинності. Центральним елементом цієї концепції є використання сканування навколишнього середовища для виявлення «слабких сигналів» у зовнішньому

середовищі з метою моніторингу та ідентифікації нових та майбутніх загроз до того, як вони втіляться у конкретну злочинну діяльність [13].

І насамкінець важлива інформація, сьогодні масштабність кіберзагрози у вигляді зламування телефону та отримання доступу до будь-якої інформації в рази перевищує загрози від убивств, тортур, викрадення людей; сучасний тероризм надзвичайно активно використовує інформаційні можливості для своїх варварських цілей. Так, наприклад, у лютому – березні 2024 р. Франція потерпала від потужних кібератак. Понад 33 мільйони людей – трохи менше половини населення Франції – постраждали від витоку даних, які включали такі відомості, як «сімейний стан, дата народження та номер соціального страхування, назва медичного страховика та покриття, передбачене полісом» [14].

**Пошук та використання інформації із відкритих джерел. Практичні аспекти застосування OSINT при розслідуванні воєнних злочинів за О. А. Кобилєвим.** Документування військових злочинів, вчинених військовослужбовцями збройних сил російської федерації і притягнення їх до відповідальності – першочергове завдання усіх правоохоронних органів. Цього від нас очікує суспільство, родичі, близькі, знайомі усіх загиблих і постраждалих від протиправних дій окупантів.

З початку повномасштабного вторгнення російської федерації на територію України російській військові вбивали, грабували, застосовували фізичне та психологічне насильство до цивільного населення, вчиняли інші особливо тяжкі злочини. Робота з ідентифікації російських військових, причетних до вчинення злочинів на території України, – це складний і багатогранний процес. Одним із методів цього процесу є пошук і аналіз інформації із відкритих джерел, так званий OSINT.

Сам термін OSINT (Open Source Intelligence Techniques) розшифровується як розвідка серед доступних джерел. Це інформація про людину, подію, певне місце. OSINT охоплює дані, які можна шукати у різних джерелах інформації доступних широкому загалу користувачів. Такі дані збираються на законних підставах, бо доступ до них не обмежується їх володільцем.

Використовуються доступні джерела, найчастіше, це інформація з мережі Internet: книги у відкритих бібліотеках, статті у засобах масової інформації, журналістські розслідування, публікації у соціальних мережах (Facebook, Twitter, Instagram, VKontakte, OK, Telegram, Youtube тощо). Взаємодія з цифровим світом є невід’ємною частиною повсякденного життя і вона залишає цифровий слід. Це невидимий слід, який залишається з після кожного кліку, вподобайки, публікації, яка публікується в мережі Internet і його можна прослідкувати.

Це дані, які можуть бути викладені у вигляді тексту, фото-, відеоматеріалів, звіти публічних зборів, конференцій. Крім того, для дослідження можуть використовуватися супутникові зображення, експертні аналітичні матеріали та доповіді.

Однією з *ключових форм* здійснення OSINT є аналіз отриманої інформації. Методами, які використовуються для аналізу та перевірки достовірності можуть бути: - оцінка змісту джерела, виявлення пропаганди та спроб маніпуляції; - визначення місця подій за допомогою супутникових зображень або інших засобів; - виявлення даних, які можуть свідчити про місцеперебування причетних до вчинення злочинів; - відстеження активності військових російської федерації в соціальних мережах; - встановлення користувачів соціальних мереж, авторів публікацій, повних анкетних даних, іншої інформації, необхідної для проведення розслідування та ін.

Безумовно, під час досудового розслідування кримінальних проваджень в ролі *аналітиків* виступають сторони кримінального провадження, зокрема, слідчий та прокурор,

але на арені OSINT в Україні та світі OSINT-аналітиками є некомерційні організації, індивідуальні експерти, журналісти, інші дослідники-одноосібники, які активно займаються OSINT. Вони збирають та аналізують інформацію, яка згодом використовується для підтвердження фактів агресії з боку росії, виявлення військової техніки на різних локаціях, підтвердження фактів вчинення злочинів військовими зс рф на території України. Одним з аналітиків OSINT є Міжнародна група Bellingcat. Беллінгкет – незалежний міжнародний колектив дослідників, слідчих і громадянських журналістів, які використовують відкриті джерела та соціальні мережі для розслідування різноманітних тем [15].

І, насамперед, одними з основних користувачів OSINT в Україні є військові структури. Вони використовують OSINT для збору інформації про рух ворожих військ, їх кількість та розташування, що допомагає військовим командирам приймати обґрунтовані рішення, своєчасно реагувати на загрози, вибудовувати тактику ведення бойових дій, адаптувати свої дії для ефективного протистояння; виявлення таємних військових баз росії на території України та прикордонних районах та інших цілей.

Поряд з перевагами OSINT є і *недоліки*, з якими постійно стикаються аналітики. До них слід віднести такі: - ненадійність отриманої інформації, у зв'язку із чим достовірність такої інформації варто перевірити й іншими можливими способами; - інформаційний шум, що ускладнює процес фільтрації та відбору важливих даних, що може спричинити пропуск важливої інформації або прийняття помилкових рішень, у зв'язку із чим варто зважено підходити до використання виявленої інформації; - маніпуляція інформацією, яка може дезорієнтувати та вплинути на результати OSINT-аналізу; - дотримання цифрової безпеки користувачів Internet.

*Інструментарій* проведення OSINT-аналізу в умовах доступності джерел доволі широкий. Це, насамперед, соціальні мережі, публічні та закриті канали у месенджерах, публікації у ЗМІ, про які згадано вище. У більшості випадків саме завдяки соціальним мережам вдається відшукати фотознімки, номери телефонів, іншу важливу інформацію про осіб, причетних до вчинення воєнних злочинів, та надалі використати їх під час розслідування воєнних злочинів. Але застосовуються й інші інструменти, такі, як пошук людей та предметів по фотознімках, використання спеціалізованих сайтів для пошуку інформації про людей, документи, підприємства, місцевість та ін.

OSINT відіграє важливу роль у наш час. Він допомагає виявляти рухи ворожих військ, аналізувати тактику та стратегію ворога, збирати інформацію про зброю та техніку, а також ідентифікувати воєнних злочинців. OSINT став потужним інструментом у боротьбі за суверенітет, безпеку та територіальну незалежність України.

**Напрацьовані методики І. В. Кріцака щодо відшукування найбільш оригінальних наукових ідей впродовж багаторічної наукової діяльності у рамках OSINT.** Кожен має свої інструменти пошуку того чи іншого матеріалу і ті результати, яких вдається досягти. Хочемо також поділитися власним досвідом, а саме – впродовж тривалого часу здійснюємо постійний кримінологічний моніторинг наукового, соціального та Інтернет-простору. Якщо сьогодні мовиться про «ройовий» (за І. О. Ревак) чи «інтелектуальний» OSINT (за О. М. Грезіною), то ми наполягаємо на понятті наукового, а в нашому випадку – кримінологічного «OSINTу», що передбачає активний моніторинг насамперед наукових просторів національних і міжнародних бібліотек, у тому числі й ресурсів держави-агресора, аби добре/точно розуміти тактики й стратегії ворога та, водночас, відстежувати всі тенденції, вироблені сучасною науковою спільнотою. У цьому контексті особливого значення набуває

техніка скорочитання, яка дозволяє у стислі терміни переглядати значні масиви інформації, виокремлюючи саме той матеріал, що вражає/зачіпає або стимулює подальше осмислення, і доносити його до широкого загалу. Тут пропонується метод «бджоли-розвідника», який спонукає інших науковців замислитися та включитися в опрацювання тієї чи іншої проблеми. Проведений нами експеримент у *ГУНП в Івано-Франківській області* (2018-2022 рр.) засвідчив, що за допомогою цієї техніки можливо опрацювати понад 500 наукових статей за один день, і навіть, якщо щоденний обсяг становитиме 100–300 наукових фахових статей, – це вже формує потужну аналітичну базу, адже така методика дозволяє вловити/засвоїти головне, зануритися у відповідний режим і зосередитися на тих джерелах, що з різних причин резонують із дослідником. Цей кримінологічний моніторинг має ручний/людський характер і не підлягає автоматизації, адже лише людина здатна відчутти смислові акценти, розпізнати ті слова й ідеї, які справді здатні здивувати й зачепити сучасного дослідника. Така тактика, вироблялася роками й постійно вдосконалюється, забезпечує високу наукову продуктивність, що підтверджується значною кількістю публікацій (зокрема понад 250 наукових праць *І. В. Кріцака*), значна частина яких має духовно-ціннісний характер і ґрунтується на відповідній авторській духовно-ціннісній концепції праворозуміння, особливо актуальній у ХХІ столітті в умовах глобальних загроз і війни в Україні, коли знищуються території й ставиться під загрозу існування українського народу не залежно, де ти проживаєш на Заході чи Сході України. У цьому сенсі кримінологічний моніторинг постає як своєрідна інтелектуальна розвідка, яка може бути посилена командною роботою (*один дослідник здійснює пошук та генерує ідеї, інший – систематизацію, групування й інтерпретацію матеріалу*), що дозволяє у стислий час опрацьовувати значні обсяги інформації. Тут слід враховувати різні умови – психоемоційний стан, спосіб і час сприйняття інформації (*вголос чи візуально, зранку чи ввечері, що конкретно залежить від дослідника*), технічних засобів (*мобільний телефон чи ноутбук*), – чим вдасться щоразу підсилювати власний інструментарій формувати гнучкий графік дослідницької діяльності, коли у найбільші притоки сил, подібно як в операційній, відбувається інтелектуальна робота. Такий підхід має безпосереднє значення і для воєнної сфери, зокрема в межах розвитку нового напрямку – кримінології війни «*Criminology of War*», який започаткувала харківська та одеська кримінологічні школи, потребують міждисциплінарного осмислення величезні масиви інформації. Відкриття нових тем і виходу на нові рівні наукового пошуку/осмислення, особливо тих, що є релевантними для правоохоронної діяльності та функціонування Національної поліції України, сприяючи більш якісному виконанню її завдань і служінню державі та суспільству.

*Ідея 1.* Так, тут ми говоримо про OSINT як про зовнішню розвідку, однак маємо чітко усвідомлювати, що OSINT – це також і внутрішні емоційно-вольові процеси, які відбуваються/протікають всередині нас у ході здійснення зовнішньої розвідки в результаті читання тисяч і тисяч наукових статей та різних матеріалів, адже у дослідника неминуче виникають власні внутрішні генераційні процеси, які він осмислює, піддає аналітиці та зрештою видає певний продукт – конкретний плід мисленнєвої діяльності у процесі пошуку. Тому слід пам'ятати, що хоча OSINT це зовнішня розвідка, ми настільки нею захоплюємося, що часто забуваємо про наші внутрішні емоційно-вольові процеси, що протікають у свідомості, на рівні нашого ества, умовно кажучи, навіть на внутрішньомолекулярному рівні у взаємодії з усім тим, що ми бачимо, що нас оточує і чим ми живемо. Звідси, надзвичайно важливо розглядати OSINT і в іншому аспекті – як причину і наслідок глибинних

мисленневих процесів, притаманних людині, створеній за образом і подобою Божою, адже людина є також творцем за природою, що здатна продукувати унікальні речі та народжувати унікальні/геніальні плоди. Тому ми наголошуємо на духовно-чуттєвій стороні OSINT як інструменту зовнішньої розвідки, який неодмінно приносить свої плоди, генерує численні ідеї та продукти, здатні переосмислити навколишню реальність і, можливо, змінити вектор нашого життя і світу у кращий бік – щоб поспішати жити, творити й робити все для вдосконалення світу, аби народжувалися діти, щоб вони не були голодними, і щоб ми допомагали бідним, знедоленим і всім, хто такої допомоги потребує.

Ідея 2. Ми вже неодноразово писали про ідею гостей професорів, тобто сьогодні кожна вища школа ЗВО має таких самородків, так сказати, тих, на кому тримається, Університет/Академія чи інший заклад освіти, які є кісткою колективу. І це не є секрет, хто чого вартий, тобто є прості викладачі, які проводять заняття на нормальному рівні, але, відповідно, віднаходити кращих із кращих серед цих усіх викладачів ЗВО є дуже важливим, і засобом такого відбору можуть бути науково-практичні заходи, де можна побачити, хто чого вартий, у кого яка доповідь яка, хто як спілкується, чи здатен доводити матеріал так, щоб він засвоювався максимально слухачем/аудиторією. Подібно як сьогодні існує національна школа суддів України, де викладають кращі з кращих і проводиться суворий відбір, так на рівні поліцейської системи доречно створити Школу кращих викладачів системи МВС і загалом ЗВО за персональною згодою викладача, які увійдуть у плеяду кращих із кращих та залучати їх як гостей професорів у різні ЗВО системи МВС, або створити єдину онлайн-площадку для усіх ЗВО системи МВС, де читатиме лекцію, проводитиме тренінг відповідний професор чи викладач. Причому, щоб потрапити туди повинен бути серйозний відбір, і повинні бути відповідні презентаційні лекції, відеолекції того чи іншого викладача у ЮТуб, щоб видно було, як професор спілкується, як він подає матеріал і як підносить його, і наскільки цей матеріал буде корисний для аудиторії, тобто відповідна презентабельність має бути, і створити комісію, яка визначатиме, хто увійде до цієї Школи поліцейстики на рівні всієї системи МВС, коли той чи інший професор буде читати серйозну лекцію/курс для всіх, і ті, хто забажають його послухати, відповідно отримають таку можливість. На наукових заходах ми відразу бачимо, хто чого вартий, у кого яка доповідь, хто як уміє спілкуватися, як він доносить матеріал, і водночас можна бути прекрасним науковцем, дослідником, але не лектором, можна бути хорошим викладачем, але не лектором, а вміння донести до аудиторії матеріал, уміння володіти й оперувати матеріалом – це дуже важлива річ, якої треба навчитися, і відповідно в цьому напрямку потрібно системно працювати. Для прикладу: серед кандидатур, які покликані прочитати хоча б одну лекцію у такій Школі поліцейстики на рівні МВС можна сміло запросити таких професорів як: Ю. В. Орлов (ХНУВС); В. К. Грищук (ЛьвДУВС), Е. В. Рижков (ДДУВС).

Ідея 3. Ми повинні готувати нового фахівця – кримінолога-політехнолога, поліцейського кримінолога-політехнолога, і це означає, що кращих із кращих ми повинні залучати до підготовки доповідей найвищого рівня, які ґрунтуються на опрацюванні тисяч і тисяч наукових статей, адже сьогодні ми чітко бачимо: у поліцейського керівника (*шефа поліції окремого регіону*) об'єктивно немає часу читати весь цей масив, тому поруч із ним має діяти команда радників, яка працює зранку до ночі 24\*7, відбираючи, осмислюючи та доносячи найбільш цікавий і важливий матеріал. Наша ідея полягає в тому, що один із радників повинен мати потужну наукову складову – це особистості, які вміють писати та публікувати необхідний матеріал, узагальнювати, шукати/віднаходити глибинний зміст і

формувати інтелектуальний продукт, який щоденно подається керівнику/управлінцю для виступів на різних рівнях, для формування позиції, для впевненого й аргументованого публічного виступу. Кримінолог-політтехнолог виступає своєрідним помічником керівника, подібно до помічника народного депутата, він формує образ шефа поліції, вкладає всі інтелектуальні ресурси в підготовку виступів, шліфує риторичку, допомагає уникати прорахунків і прогалин, водночас, тонко відчуваючи, що можна покращити, що змінити, що підсилити для того, щоб керівник поліції залишався на своєму місці, користувався авторитетом і повагою серед колег та всіх, хто з ним взаємодіє, і саме тому цей напрям – підготовка кримінолога-політтехнолога – є надзвичайно важливим й тим, який ми повинні започаткувати вже сьогодні.

**Висновки.** Розгортання російсько-української війни актуалізувало значення відкритих джерел інформації, адже в умовах пропаганди та обмеженості офіційних даних саме OSINT забезпечує оперативність, альтернативність і верифікацію відомостей, зокрема щодо бойових дій, кіберзагроз і соціальної напруги. Сучасні дослідження переконливо засвідчують, що OSINT у поєднанні з аналітикою великих даних, штучним інтелектом і байєсівським моделюванням здатен не лише фіксувати події, а й прогнозувати суспільні процеси, виявляти аномалії інформаційних потоків, профілювати кіберзагрози та формувати стратегічні рішення у сфері безпеки. Водночас, OSINT постає не лише як зовнішня розвідка, але й як внутрішній інтелектуально-емоційний процес дослідника, що супроводжується генерацією ідей, аналітичним осмисленням і створенням нового знання, особливо в умовах постійного кримінологічного моніторингу наукового та інформаційного простору. Запропонований підхід «кримінологічного OSINTу» передбачає системне, інтенсивне опрацювання великих масивів інформації через використання технік скорочитання, командної аналітики та формування інтелектуального продукту, орієнтованого на практичні потреби правоохоронної діяльності. У цьому контексті обґрунтовується необхідність інституційних новацій, зокрема створення Школи кращих викладачів системи МВС та підготовки нового типу фахівця – кримінолога-політтехнолога, який здатен інтегрувати наукові знання, аналітику та комунікаційні навички для забезпечення ефективної діяльності шефа поліції окремого регіону, ректора Університету, цим самим й багатотисячні колективи, громадськість загалом. OSINT за сучасних умов війни виступає ключовим інструментом національної безпеки, поєднуючи функції збору, аналізу та прогнозування інформації. Його ефективність визначається інтеграцією технологій, аналітичних підходів і людського інтелекту, що потребує подальшого розвитку як на науковому, так і практичному рівнях.

### Список використаних джерел

1. Horska K., Dosenko A., Iuksel G., Yuldasheva L., Solomatova V. Internet platforms as alternative sources of information during the Russian-Ukrainian war. *Amazonia Investiga*. 2023. Vol. 12. No. 62. P. 353–360. DOI: <https://doi.org/10.34069/AI/2023.62.02.36>
2. Stone H., Heslop D., Lim S., Sarmiento I., Kunasekaran M., MacIntyre C. R. Open-Source Intelligence for Detection of Radiological Events and Syndromes Following the Invasion of Ukraine in 2022: Observational Study. *JMIR Infodemiology*. 2023. Vol. 3. e39895. DOI: <https://doi.org/10.2196/39895>
3. Ehiorobo E., Pournouri S., Ghazaani S. J., Toms J. M. Profiling Cyber Attackers by Classification Techniques: A Case Study on Russian Hackers. Y: Jahankhani H. (ed.).

*Cybersecurity in the Age of Smart Societies*. Cham: Springer, 2023. (Advanced Sciences and Technologies for Security Applications). DOI: [https://doi.org/10.1007/978-3-031-20160-8\\_11](https://doi.org/10.1007/978-3-031-20160-8_11)

4. Zgurovsky M., Sliusarevsky M. Bayesian-Foresight Approach to the Prediction of Social Tension in Ukraine in the Medium Term. *Science and Innovation*. 2026. Vol. 22. № 1. P. 51–69. DOI: <https://doi.org/10.15407/scine22.01.051>

5. Maisano R., Foresti G. L. A Sentiment Analysis Anomaly Detection System for Cyber Intelligence. *International Journal of Neural Systems*. 2023. Vol. 33. № 2. URL: <https://doi.org/10.1142/S012906572350003X>

6. Sheth R., Parekha C. A proposed framework for the detection of cyber threats using open-source intelligence tools in real-time. *International Journal of Electronic Security and Digital Forensics*. 2025. Pp. 725–747. DOI: <https://doi.org/10.1504/IJESDF.2025.149329>

7. Szymoniak S., Foks K. Open Source Intelligence Opportunities and Challenges – A Review. *Advances in Science and Technology Research Journal*. 2024. Vol. 18. No. 3. P. 123–139. DOI: <https://doi.org/10.12913/22998624/186036>

8. Ghioni R., Taddeo M., Floridi L. Open source intelligence and AI: a systematic review of the GELSI literature. *AI & Society*. 2024. Vol. 39. P. 1827–1842. DOI: <https://doi.org/10.1007/s00146-023-01628-x>

9. Zhou L., Qin Y., Yan S., Zhang G., Hu W. Application Analysis of Generative Artificial Intelligence in the Field of Open Source Intelligence. *Y: Proceedings of the 39th Youth Academic Annual Conference of the Chinese Association of Automation (YAC 2024)*. Dalian, China, 2024. P. 1603–1608. DOI: <https://doi.org/10.1109/YAC63405.2024.10598766>

10. Neri F., Geraci P. Mining Textual Data to Boost Information Access in OSINT. *Information Visualization, IV 2009, Proceedings: 4th Information Visualization Conference*. 2009. P. 427–432. DOI: [10.1109/IV.2009.99](https://doi.org/10.1109/IV.2009.99)

11. Skopik F., Akhras B. Taranis AI: Applying Natural Language Processing for Advanced Open-Source Intelligence Analysis. *ERCIM News*. 2024. № 136. P. 50–51.

12. Khanna P., Zavarsky P., Lindskog D. Experimental analysis of tools used for doxing and proposed new transforms to help organizations protect against doxing attacks *Future Networks and Communications (FNC 2016) / Mobile Systems and Pervasive Computing (MobiSPC 2016): Proceedings of the 11th International Conference and the 13th International Conference*. 2016. Vol. 94. P. 459–464. <https://doi.org/10.1016/j.procs.2016.08.071>

13. Brewster B., Andrews S., Akhgar B. Environmental Scanning and Knowledge Representation for the Detection of Organised Crime Threats. *Graph-Based Representation and Reasoning*. 2014. Vol. 8577. P. 275–280. Proceedings of the 21st International Conference on Conceptual Structures (ICCS).

14. Data of half the population of France stolen in its largest ever cyberattack. This is what we know. URL: [https://www.euronews.com/next/2024/02/08/data-of-33-millionpeople-in-france-stolen-in-its-largest-ever-cyberattack-this-is-what-we-know?utm\\_source=flipboard&utm\\_content=curiouscurator%2Fmagazine%2FDigitech+](https://www.euronews.com/next/2024/02/08/data-of-33-millionpeople-in-france-stolen-in-its-largest-ever-cyberattack-this-is-what-we-know?utm_source=flipboard&utm_content=curiouscurator%2Fmagazine%2FDigitech+) (Last accessed: 03.05.2024).

15. Беллінгкет українською мовою. URL: <https://uk.bellingcat.com/>

**Фігура В. О.,**  
ад'юнкт відділення докторантури і ад'юнктури  
(*Національна академія Державної прикордонної  
служби України імені Богдана Хмельницького*)

## **ЗАСТОСУВАННЯ OSINT ДЛЯ ПОСИЛЕННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ МОЖЛИВОСТЕЙ ПЕРСПЕКТИВНОГО ПІДРОЗДІЛУ ОБРОБКИ ДАНИХ ПАСАЖИРІВ (PIU)**

Стрімкий розвиток інформаційних технологій докорінно змінив підходи до збору та аналізу персональних даних, що зумовило формування принципово нового середовища у сфері правоохоронної діяльності. Великі масиви даних, які раніше були фактично недоступними або потребували складних процедур отримання, сьогодні перебувають у вільному доступі. У цьому контексті ефективність протидії сучасним загрозам значною мірою залежить від здатності державних інституцій не лише акумулювати інформацію, а й забезпечувати її якісну інтерпретацію та практичне використання.

Іструменти OSINT є ключовими для реалізації цього завдання є. OSINT дедалі глибше інтегрується у практику правоохоронних органів, відіграючи важливу роль у зміцненні національної та прикордонної безпеки України.

З урахуванням цього зазначені інструменти є важливими з огляду на особливе місце перспективного органу - Центру обробки попередніх даних (Passenger Information Unit - PIU) у майбутній структурній конфігурації системи забезпечення прикордонної безпеки. Його діяльність буде спрямована на аналіз інформації, отриманої з систем API (попередня інформація про пасажирів)/PNR (запис імені пасажирів) [1]. Ці дані містять базові відомості про пасажирів авіаційних рейсів: установчі дані, маршрути подорожей, деталі бронювання та контактну інформацію. Проте варто зауважити, що самі по собі ці відомості є обмеженими та не завжди дозволяють повноцінно виявляти приховані загрози на державному кордоні.

Застосування OSINT дозволить суттєво розширити аналітичний потенціал PIU через залучення відкритих джерел: соціальних мереж, медіа-ресурсів, судових рішень та публічних реєстрів. Це дасть змогу доповнити базовий масив API/PNR відомостями про професійну діяльність, зв'язки та публічну активність особи. Такий комплексний підхід сприятиме формуванню об'єктивного профілю пасажирів, що має вирішальне значення для якісної оцінки ризиків та запобігання транскордонній злочинності. Зокрема, цей підхід дозволяє виявити осіб, причетних до терористичних організацій або суб'єктів, що намагаються обійти санкційні обмеження.

Як зазначає дослідник Лібор Бенеш, у минулому OSINT вважався менш затребуваним через низьку надійність джерел, що зумовлена дезінформацією та викривленими даними. Водночас сьогодні його належне використання є важливим для збору інформації. Тобто найважливішою функцією методу можна вважати здатність системи надавати обґрунтовані оцінки особам, які приймають рішення [2].

Зауважимо, що впровадження OSINT у діяльність підрозділу PIU забезпечить перехід від лінійного аналізу даних до глибокого аналітичного опрацювання інформації. Як правило, дані PNR трансформуються у багатовимірний профіль, який дозволяє виявити нетипові зв'язки між особами, встановити потенційну причетність до кримінальних правопорушень, протидія яким регулюється Директивою Європейського Парламенту і Ради ЄС № 2016/681 [3].

Наголосимо, що для ефективного використання OSINT можуть бути застосовані спеціалізовані аналітичні інструменти. За допомогою сучасного програмного забезпечення аналітик може візуалізувати зв'язки між об'єктами (особами, номерами телефонів, електронними адресами тощо). Такий підхід дає правоохоронним органам можливість виявляти небезпечні контакти. Таким чином, аналіз відкритих джерел дозволяє отримати ширший контекст щодо діяльності особи, її соціального оточення та публічної активності.

Через інструменти OSINT здійснюється автоматизований збір інформації, яка надалі систематизується та інтегрується з даними API/PNR. Це дозволяє значно підвищити якість аналітичної діяльності підрозділу PIU. Однією з ключових переваг OSINT є раннє виявлення потенційних загроз. Особливе значення має комплексний підхід до верифікації осіб, що передбачає поєднання масивів внутрішніх баз даних із методами OSINT [4, с. 386].

На нашу думку, саме поєднання даних API/PNR із доступною інформацією з відкритих джерел надасть можливість виявляти підозрілу поведінку пасажирів, зокрема: часті переміщення, нетипові маршрути або зв'язки з особами, які вже перебувають у полі зору правоохоронців. Крім того, це створить умови для превентивного реагування. Важливим аспектом є також кореляція отриманих відомостей із міжнародними та внутрішніми базами даних, санкційними списками тощо. Такий підхід дозволяє сформуванню цілісної аналітичної картини.

Отже, практична цінність OSINT для PIU полягає у можливості ефективної пріоритизації об'єктів аналізу. Це дозволяє оптимально розподіляти ресурси, акцентуючи увагу на найбільш ризикованих пасажирів. Головним є і те, що OSINT сприяє підтвердженню або спростуванню первинних аналітичних гіпотез, що знижує рівень помилкових результатів.

Окрему увагу слід звернути на підготовку аналітичних матеріалів. OSINT дозволяє формувати змістовні звіти для зацікавлених державних органів, що підвищує ефективність міжвідомчої взаємодії. Такі матеріали містять не лише «сухі» факти, а й аналітичні висновки щодо потенційних загроз.

При цьому майбутнє застосування OSINT у системі API/PNR потребує суворого дотримання правових норм. Обробка персональних даних повинна відбуватися згідно з GDPR та іншими актами для забезпечення належного рівня захисту інформації. Підсумовуючи, зазначимо, що використання OSINT у роботі PIU є стратегічно важливим елементом системи забезпечення прикордонної безпеки України.

### **Список використаних джерел**

1. Крутік Ю. В. Національний центр обробки попередніх даних як елемент системи API/PNR. *Науковий вісник Ужгородського Національного Університету*. 2025. № 88. Т. 3. С. 285–290.
2. Libor Benes, OSINT, New Technologies, Education: Expanding Opportunities and Threats. A New Paradigm, *Journal of Strategic Security* 6. № S3 2013. S. 24. URL: <http://dx.doi.org/10.5038/1944-0472.6.3S.3>. (дата звернення: 20.04.2026).
3. Про використання даних системи бронювання (PNR) для запобігання, виявлення, розслідування і кримінального переслідування злочинів терористичної спрямованості та тяжких злочинів : Директива Європейського парламенту та Ради Європейського Союзу від 27 квітня 2016 р. № 2016/681/ЄС. URL: <https://itd.rada.gov.ua/billInfo/Bills/pubFile/1437637> (дата звернення: 25.04.2026).
4. Філіппов С., Фігура В, Дзюба М. Використання інструментів OSINT в інтересах розбудови доброчесності. *Law & Border*. 2025. № 6(2). С. 370–394. [https://doi.org/10.32453/law\\_border.v6i2.2085](https://doi.org/10.32453/law_border.v6i2.2085).

**Форос Г. В.,**  
завідувачка кафедри кримінального аналізу  
та інформаційних технологій,  
кандидат юридичних наук, доцент  
(*Одеський державний університет внутрішніх справ*)

**Калугін В. Ю.,**  
професор кафедри кримінального аналізу  
та інформаційних технологій,  
кандидат юридичних наук, доцент  
(*Одеський державний університет внутрішніх справ*)

## **КЛЮЧОВІ НАПРЯМИ ЗАСТОСУВАННЯ МЕТОДОЛОГІЇ OSINT У СФЕРІ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ**

В умовах інтенсивної цифрової трансформації суспільства та розвитку інформаційних технологій відкриті джерела інформації перетворилися на масштабне інформаційне середовище. У зв'язку з цим методологія OSINT, що ґрунтується на системному зборі, обробці, верифікації, аналізі та подальшому використанні даних із відкритих джерел, посідає одне з ключових місць у діяльності правоохоронних органів. Її застосування спрямоване на забезпечення інформаційно-аналітичної підтримки процесів ухвалення управлінських, оперативно-службових рішень, а також виступає дієвим інструментом досягнення інформаційної переваги в умовах сучасних безпекових викликів.

У правоохоронній діяльності OSINT використовується як допоміжний, а в окремих випадках і як базовий, механізм для своєчасного виявлення, попередження, документування та розслідування кримінальних правопорушень, а також для встановлення зв'язків між подіями, особами, об'єктами та явищами. Зокрема, аналіз відкритих джерел дозволяє ідентифікувати осіб, причетних до злочинної діяльності, встановлювати їхні зв'язки, визначати маршрути переміщення, фінансові операції, а також фіксувати цифрові сліди їхньої активності. [1] Особливого значення набуває моніторинг соціальних мереж, де користувачі добровільно публікують значні обсяги персональної інформації, що може бути використана в інтересах досудового слідства.

Одним із пріоритетних напрямів використання методології OSINT є протидія організованій злочинності, екстремізму та терористичній діяльності. Шляхом комплексного аналізу інформації, отриманої з відкритих джерел, правоохоронні органи набувають можливості своєчасно виявляти підготовчі процеси, відстежувати тенденції розвитку протиправної активності, встановлювати канали фінансування незаконних збройних формувань і злочинних угруповань, а також ідентифікувати осіб, причетних до їх функціонування.

У зазначеному контексті OSINT виступає дієвим інструментом превентивної діяльності, оскільки забезпечує можливість раннього виявлення потенційних загроз, прогнозування ризиків та вжиття своєчасних заходів реагування ще на початкових стадіях формування протиправних намірів.

Сучасні інформаційні трансформації створюють для правоохоронних органів нові можливості організаційного, правового та технологічного характеру. Відкриті джерела містять значний потенціал для отримання відомостей щодо кримінальних зв'язків, можливих

місць зберігання зброї, боєприпасів чи наркотичних засобів, а також характеру й інтенсивності діяльності терористичних груп [2].

Саме процеси цифровізації та глобальної інформатизації зумовлюють докорінну зміну характеру сучасної правоохоронної діяльності. Динамічний розвиток цифрового середовища, стрімке зростання обсягів даних і поява нових каналів комунікації істотно трансформують підходи до виявлення, документування та припинення протиправної діяльності. У зв'язку з цим традиційні методи оперативно-розшукової діяльності дедалі частіше поєднуються з інноваційними технологічними рішеннями, орієнтованими на пошук, збір, обробку та аналіз інформації з відкритих джерел.

У зазначеному контексті простежується поступова еволюція оперативно-розшукової діяльності у формат кримінальної розвідки - системної, аналітично керованої моделі діяльності, що ґрунтується на використанні алгоритмічних інструментів аналізу даних, міжвідомчій кооперації, ризик-орієнтованому підході та превентивному виявленні потенційних загроз. Такий підхід не лише суттєво розширює функціональний інструментарій правоохоронних органів, а й формує нову парадигму реагування на злочинність.

Окремої уваги потребує питання допустимості доказів, отриманих із відкритих джерел, у кримінальному провадженні [3]. Для того щоб такі дані могли бути використані як доказ, необхідно забезпечити їх належну фіксацію, перевірку достовірності та дотримання процесуальних процедур. У цьому контексті важливим є розвиток методичних рекомендацій та стандартів роботи з OSINT для правоохоронних органів.

Не менш вагоме значення має належне технічне забезпечення процесів реалізації методології OSINT. Сучасні програмно-аналітичні комплекси та спеціалізовані цифрові інструменти надають можливість автоматизувати процедури пошуку, збору, систематизації й аналізу даних, здійснювати візуалізацію соціальних та комунікаційних зв'язків, проводити геопросторовий аналіз, а також виявляти приховані закономірності у значних масивах інформації.

Особливого значення набуває процедура верифікації даних, яка передбачає застосування комплексу методів перевірки достовірності інформації. До таких методів належать перехресне зіставлення відомостей із різних джерел, технічна експертиза фото- та відеоматеріалів, аналіз метаданих, оцінка репутації та надійності інформаційних ресурсів, а також встановлення логічної узгодженості отриманих даних.

### **Список використаних джерел**

1. Федчак І. А. Основи кримінального аналізу : навчальний посібник. Львів : Львівський державний університет внутрішніх справ, 2021. 288 с.
2. Бондаренко С. В. Використання OSINT-технологій у протидії незаконному обігу зброї в Україні. *Криминологія та соціальна інтеграція*. 2022. № 3. С. 45–59.
3. Кульчицька Л. О. Матеріали OSINT як джерела доказів у кримінальних провадженнях за ознаками злочину агресії та воєнних злочинів : матеріали наук.-практ. круглого столу Цифровізація кримінального провадження: стан та перспективи, м. Харків, 19 верес. 2024 р. С. 97–102.

**Франчук В. І.,**  
старший науковий співробітник,  
доктор економічних наук, професор  
(Львівський державний університет внутрішніх справ)

## **КОНЦЕПТУАЛЬНА МОДЕЛЬ OSINT ЯК ВИДУ БЕЗПЕКОВОЇ ДІЯЛЬНОСТІ**

Життєве середовище людини, організації чи держави в силу різних обставин та причин містить загрози, кризи та небезпеки, які руйнують, наносять шкоду тощо та яким потрібно протидіяти. Для цього застосовують безпекову діяльність, яка використовується як збірне загальне поняття та містить безпекові механізми: попередження, виявлення, ліквідації загроз, а також відновлення чи відшкодування збитків. Зазначені безпекові механізми, один чи більшість є у багатьох видах діяльності, зокрема й в OSINT.

Ідея використання OSINT (відкритої розвідки) в різних видах діяльності набула інтенсивного наукового осмислення упродовж останнього десятиліття. Дискусії торкаються як теоретико-методологічної природи OSINT, так і практичних аспектів. Узагальнюючи контент-аналіз наукових досліджень(1, 2, 3, 4, 5, 6, 7, 8, 9, 10, , та інш) можна констатувати, що OSINT розглядається під різними кутами наукового зору та використовується в якості інструменту збору й аналізу інформації для використання її в тих чи інших видах діяльності для прийняття рішень. Отримані власні наукові результати розширюють усталене розуміння OSINT, виходячи за межі його традиційного трактування як інструменту чи методу розвідки та дозволяють вперше в науці розглядати як вид безпекової діяльності. Концептуальну модель структури OSINT як виду безпекової діяльності подано на рисунку 1.

Науково обгрунтовано, що сучасний OSINT як вид безпекової діяльності це цілісний технологічний процес, що має складну структуру з обов'язкових елементів, які поділяються на: організаційно-технологічні та алгоритм дій, а також безпекові інформаційно-виявляючі механізми (рис. 1).

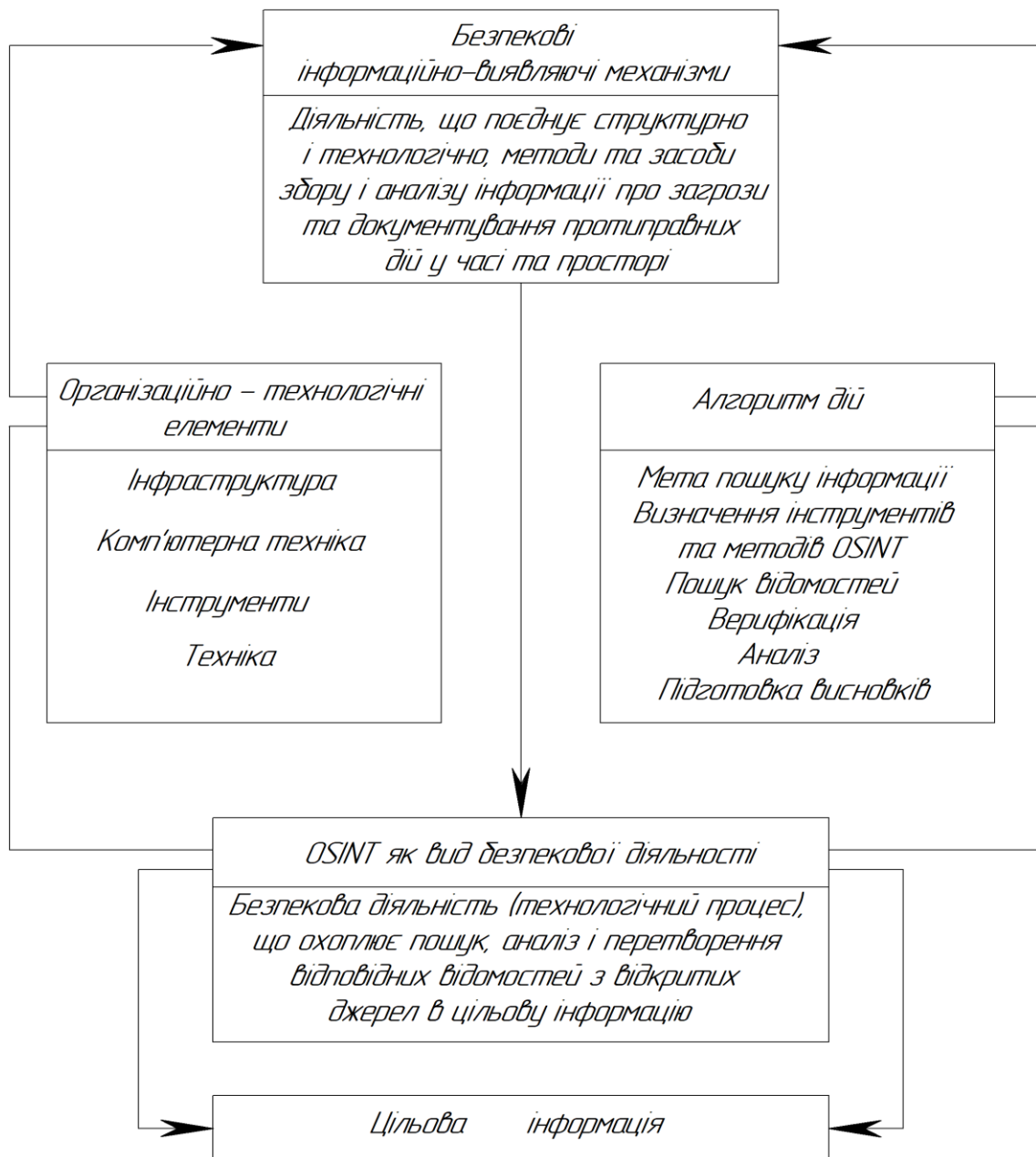


Рис.1 Концептуальна модель структури OSINT як виду безпекової діяльності

Джерело: розроблено автором.

З огляду на це OSINT за змістом є технологією, що поєднує алгоритм дій, інфраструктуру, компетентності, методи та інструменти, необхідні для пошуку, аналізу і перетворення відповідних відомостей з відкритих джерел в цільову інформацію. а за формою є безпековою діяльністю, бо містить інформаційно-виявляючі механізми та реалізується безпосередньо людиною-фахівцем, а також може використовуватися у межах різних видів безпекової діяльності для отримання цільової інформації з відкритих джерел. Зокрема інформацію про розповсюдження наркотичних речовин, зброї, небезпечні групи чи особи, кіберзагрози, про порушення комерційної таємниці співробітниками компанії тощо. Слід наголосити, що ця та інша цільова інформація враховується під час прийняття рішень для вирішення завдань в різних видах безпекової діяльності: оперативно-розшуковій діяльності,

правоохоронній діяльності, детективній діяльності, слідчій діяльності, службових розслідуваннях, журналістських розслідуваннях, фінансових розслідувань, пошуках зниклих людей, пошуках викрадених речей тощо.

Таким чином OSINT – це безпекова діяльність (технологічний процес), що охоплює пошук, аналіз і перетворення відповідних відомостей з відкритих джерел в цільову інформацію. Використання OSINT як виду безпекової діяльності дозволяє посилити спроможності відповідних суб'єктів щодо отримання інформації про загрози (виявлення загрози), або тих хто їх зреалізував, а відтак і щодо їх попередження чи ліквідації (припинення), або притягнення винуватця до відповідальності.

### **Список використаних джерел**

1. Hayes D. R., Cappa F. Open-source intelligence for risk assessment. *Business Horizons*. 2018. Т. 61. № 5. С. 689–697. DOI:
2. Konieczny, M. (2025). Anti-OSINT methods ensuring protection of personal data in the context of cybercrime. *RAIP*, 1(XXV), 127–144. DOI: <https://doi.org/10.5604/01.3001.0055.1100>
3. Lakomy M. Open-source intelligence and research on online terrorist communication: Identifying ethical and security dilemmas. *Media, War & Conflict*. 2023. № 17(1). P. 23–40. URL: <https://doi.org/10.1177/17506352231166322>
4. Sampson F. Intelligent evidence: Using open source intelligence (OSINT) in criminal proceedings. *The Police Journal: Theory, Practice and Principles*. 2017. Т. 90. № 1. С. 55–69. DOI: <https://doi.org/10.1177/0032258X16671031>
5. Van Beek H., Rietjens S. Open-source intelligence in the Russia–Ukraine war. Reflections on the Russia–Ukraine War / eds. M. Rothman, L. Peperkamp, S. Rietjens. Leiden: Leiden University Press, 2024. С. 57–76.
6. Van Puyvelde D., Tabárez Rienzi F. The rise of open-source intelligence. *European Journal of International Security*. 2025. First View. С. 1–15. DOI: <https://doi.org/10.1017/eis.2024.61>
7. Wagner T. D., Mahbub K., Palomar E., Abdallah A. E. Cyber threat intelligence sharing: Survey and research directions. *Computers & Security*. 2019. Vol. 87. DOI: <https://doi.org/10.1016/j.cose.2019.101589>
8. Yamin M., Ullah M., Ullah H., Katt B., Hijji M., & Muhammad K. (2022). Mapping Tools for Open Source Intelligence with Cyber Kill Chain for Adversarial Aware Security. *Mathematics*, 10(12):205
9. Zaporozhchenko M. M. Місце OSINT в життєвому циклі кібератаки. *Телекомунікаційні та інформаційні технології*. 2023. № 1 (78). С. 53–60. DOI: <https://doi.org/10.31673/2412-4338.2023.015360>.
10. Главацька А., Ангельська О., Опірський І. Дослідження технології використання OSINT як нової загрози з деанонізації особи в Інтернет просторі. *Кібербезпека: освіта, наука, техніка*. 2024. № 1 (25). С. 19–50. DOI: <https://doi.org/10.28925/2663-4023.2024.25.1950>.

**Фуртес О. О.,**  
старший науковий співробітник  
науково-дослідного відділу Наукового центру  
сухопутних військ, кандидат історичних наук, працівник ЗСУ  
(*Національна академія сухопутних військ*)

**Кудимов С. М.,**  
заступник начальника науково-дослідного відділу  
Наукового центру сухопутних військ  
(*Національна академія сухопутних військ*)

**Дорота А. С.,**  
доцент кафедри тактики інституту піхоти  
(*Національна академія сухопутних військ*)

## **OSINT У РОЗКРИТТІ ВОЄННИХ ЗЛОЧИНІВ В УКРАЇНІ**

В умовах, яких знаходиться Україна на сьогоднішній день одержання вчасно достовірної інформації та в найкоротші терміни є важливим і необхідним для Збройних Сил України, підрозділів Національної поліції, Служби безпеки України, Державної прикордонної служби України, та інших підрозділів, які здійснюють підслідність (здійснення розслідування).

Сучасний OSINT сформувався з появою мережі інтернет, соціальних мереж та супутникових знімків, що дозволило перетворити збір інформації на високотехнологічну діяльність.

В Україні OSINT набув особливого значення з 2014 року, коли волонтерські групи збирали докази присутності російських військ через відкриті фото і пости. У 2022 році команди Molfar, Oguh та українці ідентифікували тисячі одиниць техніки, воєнних злочинців і логістику ворога.

Станом на кінець січня 2026 року в Україні зафіксовано понад 212 тисяч військових злочинів, що робить OSINT (розвідка на основі відкритих джерел) – розслідування критично важливою та допомагає перетворювати цифрові сліди на юридичні докази, забезпечуючи нести відповідальність та покарання за вчиненні воєнні злочини. Джерелами для OSINT слугують численні ресурси, зокрема сайти, платформи соціальних мереж, новини та інформація.

Отже, за допомогою OSINT здійснюється військова та безпекова розвідка, фільтрація інформації, військові та правоохоронні розслідування воєнних злочинів рф в Україні. До цієї групи з розслідування злочинів долучилися 14 країн. Її метою є сприяння розслідуванням злочинів росії в Україні, допомогти виявляти підозрюваних та їхню причетність за допомогою збору та аналізу розвідувальних даних з відкритих джерел. Використання та розповсюдження перевіреної інформації з відкритих джерел сприяє вільному обміну даними, адже в такому разі не використовуються закриті методи. OSINT методологією та технологічним комплексом, які забезпечують отримання та застосування воєнних, політичних, економічних та інших даних з відкритих джерел без порушення чинного законодавства та знаходить застосування у процесах ухвалення рішень у сфері національної оборони та безпеки.

OSINT передбачає збір інформації, її фіксацію, облік та аналіз обробку первинних відомостей, збереження та поширення даних, забезпечення інформаційної безпеки та представлення результатів досліджень. В результаті обробки, вихідна інформація перетворюється на цінне знання, що може бути засекречене.

Переваги використання розвідки з відкритих джерел (OSINT):

1. Доступ до зібраних даних є відкритим для всіх.
2. Здатність збирати інформацію з широкого спектра джерел. Дані можна отримати з соціальних мереж, новин, офіційних урядових документів, наукових публікацій.

Роль OSINT- спеціаліста полягає у зборі та аналізі відомостей з багатьох джерел. Головне завдання такого фахівця - складання правдивої картини подій на підставі віднайдені інформації. Прикладом є українські OSINT-фахівці ідентифікували пілота літака А-50, він спрямовував запуски ракет з території Білорусії (військовий аеродром смт.Мачулищі). Вони здійснюючи моніторинг відкритої інформації, встановили його місце проживання, освіту, місце служби. Українські OSINT – експерти виявляють російських військових, які вчиняють військові злочини, навіть за фотографіями у їхніх телефонах, які вони гублять.

Розвідка з відкритих джерел у всесвітній мережі сприяє виявленню цілих підрозділів під час боїв, а також тих, які перетинають кордони нашої держави. Діяльність наших OSINT-фахівців активно займається пошуком колаборантів, збору інформації про контроль росією українських підприємств, оборонної промисловості, а також про наявність російської агентури на нашій території. Метою таких фахівців є перемогти ворога.

Кожна OSINT – спільнота розробляє та функціонує за власною розробленою стратегією, має чіткий план та вносить свій внесок у перебіг бойових дій. Метою є протистояти російській дезінформації, підтримувати та допомагати українським захисникам для наближення перемоги.

Для здійснення всебічного дослідження з використанням методології OSINT, існує велика кількість спеціалізовано інструментарію, що здатне збільшити продуктивність діяльності.

Основними інструментами, що застосовують в процесі розкриття воєнних злочинів є:

Maltego – програмне забезпечення для збору інформації в відкритим вихідним кодом. За допомогою Maltego визначають геолокацію кіберзлочинців, де об'єктом є люди.

Shodan – це пошукова система, фокусується на індексації метаданих, що називають банерами, які передаються пристроями клієнтам. Роль таких інструментів важлива для розвідки та захисту.

OSINT Framework – це інтерактивна мапа-каталог для розвідників, яка допомагає розвідникам впорядкувати процес збору даних, аналізу воєнних злочинів та ідентифікації ворога: від пошуку людей IP-адрес до соціальних мереж і державних реєстрів.

Recon-ng – це потужний фреймворк для проведення веб-розвідки та збору даних з відкритих джерел. Використовується фахівцями з кібербезпеки для аналізу уразливостей, збору інформації про ціль та конкурентної розвідки.

Coogole Dorks – у розкритті воєнних злочинів та OSINT- розслідувань (розвідка на основі відкритих джерел) є потужним інструментом для пошуку доказів, які були «заховані» на веб-сайтах, але проіндексовані Coogole.

OSINT сприяє задумів противника, надаючи змогу українським військовим корегувати власні дії задля результативної протидії.

Одним із напрямів застосування OSINT під час розслідування воєнних злочинів є залучення соціальних мереж з метою виявлення та ідентифікації осіб, котрі були учасниками бойових дій чи стали свідками злочинів. Фотографії та відеоматеріали, розміщені в соціальних мережах, здатні містити цінну інформацію про конкретних осіб, місце їх перебування та вчинки, що дають змогу правоохоронцям.

Основні напрямки використання OSINT у війні:

1. Ідентифікація та пошук – OSINT-фахівці, використовують доступну інформацію для виявлення російських солдатів, техніки та позицій.

2. Фіксація воєнних злочинів – фіксування фактів злочинів, вчинених росією, що важливо для міжнародного правосуддя.

3. Георозвідка та аналітика – створено спеціалізовані аналітичні платформи, які дозволяють отримувати дані з російських гаджетів для подальших досліджень.

4. Допомога полоненим – OSINT технології використовуються для підтвердження перебування військовослужбовців Збройних Сил України в полоні (ідентифіковано понад 3 тисячі осіб).

5. Боротьба у кіберпросторі – OSINT виступає як засіб протидії кіберзлочинності та збору розвідувальних даних.

У сучасних гібридних конфліктах OSINT перетворився на важливий елемент протидії гібридним загрозам, відіграє критичну роль, перетворюючись із допоміжного інструменту на стратегічний елемент національної безпеки та надає можливість діяти на випередження.

**Хізанов О. Д.,**  
курсант 3 курсу ННІПД  
(Національна академія внутрішніх справ)  
Науковий керівник: **Моргун Н. С.,**  
професор кафедри оперативно-розшукової  
діяльності та національної безпеки,  
кандидат юридичних наук, доцент  
(Національна академія внутрішніх справ)

## **МІЖНАРОДНЕ СПІВРОБІТНИЦТВО У СФЕРІ КІБЕРЗАХИСТУ ТА НАЦІОНАЛЬНА БЕЗПЕКА УКРАЇНИ: ВИКОРИСТАННЯ МЕХАНІЗМІВ ЄВРОПЕЙСЬКОГО СОЮЗУ ДЛЯ РЕАГУВАННЯ НА МАСШТАБНІ КІБЕРАТАКИ**

Національна безпека України сьогодні пов'язана не лише зі станом оборони, а й зі стійкістю цифрової інфраструктури, на якій тримається державне управління, зв'язок, енергетика, фінансові сервіси, транспортна координація та функціонування державних реєстрів. Масштабна кібератака в сучасних умовах спрямовується не просто на окремий інформаційний ресурс, а на здатність держави безперервно ухвалювати рішення, забезпечувати роботу критичних систем і зберігати довіру суспільства до інституцій. Саме тому міжнародне співробітництво у сфері кіберзахисту слід розглядати як складову системи безпеки держави. Його практичне значення полягає в доступі до зовнішніх механізмів допомоги, координації та відновлення під час великої кібератаки. 12 березня 2026 року Верховна Рада України ратифікувала Угоду у формі обміну листами між Україною та Європейським Союзом про внесення змін до статті 1(1) Угоди про участь України у програмі Європейського Союзу «Цифрова Європа» (2021–2027), що відкрило доступ до Резерву кібербезпеки Європейського Союзу [1]. У парламентському повідомленні зазначено можливість залучення експертної, технічної та технологічної підтримки у режимі реального часу, а також використання інструментів виявлення, стримування та відновлення після кібератак [1].

Європейський Союз уже сформував кілька пов'язаних між собою механізмів, які працюють у разі значних і масштабних кіберінцидентів. Правову основу для цього створив Cyber Solidarity Act, що набрав чинності 4 лютого 2025 року [2]. На його основі діє EU Cybersecurity Reserve, адміністрування якого покладено на ENISA. Цей інструмент дозволяє залучати перевірених постачальників послуг кіберзахисту для підтримки реагування та відновлення після великої атаки. Поряд із резервом функціонують CSIRTs Network та EU-CyCLONe: перша мережа забезпечує технічний обмін інформацією про інциденти, вразливості та способи реагування, а друга поєднує операційний і стратегічний рівні під час кіберкризи. У червні 2025 року Рада ЄС схвалила оновлений Cyber Blueprint, який визначає порядок дій від виявлення інциденту до відновлення після нього.

Небезпека масштабних кібератак полягає в тому, що їх наслідки виходять далеко за межі технічного збою. У документах ENISA такі інциденти пов'язуються з порушенням функціонування суспільно важливих сервісів, економіки та публічного управління. В умовах російської збройної агресії кіберпростір використовується як окремий напрям впливу на державу. Атака на енергетику, державні сервіси, реєстри, телекомунікації або фінансову систему здатна одночасно дезорганізувати управління, ускладнити роботу сектору безпеки і оборони, спричинити соціальну напругу та підірвати стійкість критичної інфраструктури.

Свіжа статистика підтверджує масштаб цієї загрози. За даними Держспецзв'язку, CERT-UA у 2025 році опрацювала майже 6000 кіберінцидентів, а кількість ворожих атак зросла на 37 відсотків. Також зазначається, що протягом року фіксувалося в середньому близько 15 кіберінцидентів на день та відстежувалося понад 150 кластерів кіберзагроз. У межах Європейського Союзу сектор публічного управління охопив 38,2 відсотка інцидентів, а 57,5 відсотка атак на цифрову інфраструктуру становили DDoS-атаки, що свідчить про однакову спрямованість загроз [33].

Закон України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» від 27 березня 2025 року сформував внутрішню правову основу для реагування на інциденти кібербезпеки, кібератаки і кіберзагрози, визначив порядок інформування про значні інциденти, а також розмежував ролі національної, галузевих і регіональних команд реагування [4]. Саме така модель дає можливість поєднувати зовнішні механізми підтримки Європейського Союзу з уже наявною системою координації всередині держави, коли міжнародна допомога включається не відокремлено, а через визначену структуру дій та відповідальності. Подальший розвиток цього напрямку пов'язаний із більш чітким узгодженням процедур ескалації інциденту, швидким обміном інформацією між технічним, управлінським і безпековим рівнями, а також із відпрацюванням практичної взаємодії під час кризових сценаріїв. У разі великої атаки саме злагодженість дій, швидка оцінка масштабу події та своєчасне включення зовнішньої підтримки визначатимуть, наскільки ефективно держава зможе зберегти стійкість інформаційних систем.

Отже, міжнародне співробітництво у сфері кіберзахисту прямо пов'язане зі стійкістю державного управління, безперервністю роботи критичних систем і здатністю зберігати керованість у ситуації, коли кібератака спрямовується на функціонування держави загалом. Ратифікація угоди та приєднання до механізмів Європейського Союзу у сфері кіберзахисту мають значення не лише як етап співпраці, а як реальний інструмент посилення стійкості держави до масштабних кібератак. Перспектива цього напрямку полягає у поступовому включенні цих механізмів у щоденну практику захисту цифрової інфраструктури, а не лише у використанні їх у виняткових випадках.

### **Список використаних джерел**

1. Верховна Рада ратифікувала Угоду з ЄС, яка надасть Україні доступ до Резерву кібербезпеки Євросоюзу. Верховна Рада України. 12.03.2026. URL: <https://www.rada.gov.ua/print/271245.html> (дата звернення: 23.03.2026).
2. EU Cybersecurity Reserve. ENISA. URL: <https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management/eu-cybersecurity-reserve> (date of access: 23.03.2026).
3. CERT-UA у 2025 році опрацювала майже 6000 кіберінцидентів: кількість ворожих атак зросла на 37 %. URL: <https://cip.gov.ua/en/news/cert-ua-u-2025-roci-oprasyuvava-maizhe-6000-kiberincidentiv-kilkist-vorozhikh-atak-zroslo-na-37> (дата звернення: 23.03.2026).
4. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27.03.2025 № 4336-IX. База даних «Законодавство України». Верховна Рада України. URL: <https://zakon.rada.gov.ua/go/4336-20>

**Цмоць У. О.,**  
старший науковий співробітник  
відділу організації наукової діяльності  
(Львівський державний університет внутрішніх справ)

## **ЗАСАДИ ПРАВОВОГО ТА ЕТИЧНОГО РЕГУЛЮВАННЯ КОЛЕКТИВНОЇ OSINT-ДІЯЛЬНОСТІ: МІЖ ЕФЕКТИВНІСТЮ ТА ЗАХИСТОМ ПРАВ ЛЮДИНИ**

Розвідка на основі відкритих джерел (OSINT) у сучасних умовах перетворилася на один із ключових інструментів аналітичної діяльності у сферах національної безпеки, кримінального правосуддя та журналістики. Вона передбачає системний збір, обробку та інтерпретацію публічно доступної інформації, включно із соціальними мережами, засобами масової інформації, цифровими архівами та геопросторовими даними. Інтеграція OSINT із технологіями штучного інтелекту суттєво підвищує ефективність аналітичних процесів, однак водночас ускладнює їх правову оцінку та створює додаткові ризики для дотримання прав людини [1].

Правове регулювання використання відкритої інформації в Україні ґрунтується на положеннях Закону України «Про інформацію», який закріплює принципи відкритості, законності, достовірності та доступності інформації [2]. Водночас відкритість даних не означає їх правової нейтральності. Процеси збору, обробки та використання інформації повинні відповідати вимогам законодавства, зокрема у сфері захисту приватного життя та персональних даних. У цьому контексті важливе значення мають європейські стандарти, сформовані Конвенцією про захист прав людини і основоположних свобод та Загальним регламентом про захист даних (GDPR), які встановлюють принципи необхідності, пропорційності та мінімізації втручання у права людини.

Сучасна OSINT-діяльність дедалі частіше набуває колективного характеру, формуючи модель розподіленої аналітики. Вона передбачає взаємодію широкого кола суб'єктів – державних органів, журналістів, дослідницьких спільнот і волонтерів. Такий підхід сприяє підвищенню оперативності та якості аналізу, однак водночас ускладнює питання відповідальності. У межах колективної OSINT-діяльності аналітичний результат формується як наслідок взаємопов'язаних дій різних учасників, які виконують функції збору, перевірки, систематизації та інтерпретації інформації. Це ускладнює застосування традиційних моделей індивідуальної відповідальності та зумовлює необхідність її функціонального розподілу залежно від ролі кожного учасника.

У цьому контексті важливим є розмежування правового статусу суб'єктів OSINT-діяльності, які діють у різних нормативних режимах. Особливої складності набуває визначення статусу волонтерів у період збройного конфлікту. Хоча загальний аналіз відкритих даних не розглядається як безпосередня участь у бойових діях, передача точної інформації для ураження цілей може змінювати правову оцінку такої діяльності та наближати її до участі у воєнних операціях.

Окремого значення набуває використання OSINT у кримінальному процесі. Матеріали, отримані з відкритих джерел, можуть визнаватися доказами лише за умови дотримання критеріїв належності, допустимості та достовірності. Ключовим аспектом є забезпечення цілісності цифрових даних і належне документування процесу їх отримання. У

цьому зв'язку важливу роль відіграє дотримання цифрового ланцюга збереження доказів, порушення якого може призвести до втрати доказової сили матеріалів [3]. Судова практика поступово формує підходи до оцінки таких доказів, однак відсутність уніфікованих методологічних стандартів зумовлює ризики неоднакового застосування права та потребує подальшого нормативного і практичного узгодження.

Важливим напрямом застосування OSINT є забезпечення інформаційної безпеки та протидія дезінформації. Відкриті джерела можуть використовуватися як для викриття маніпулятивних наративів, так і для їх поширення. У цьому контексті OSINT-спільноти виконують подвійну функцію: вони сприяють виявленню неправдивої інформації, але за відсутності належної перевірки можуть також стати каналом її ненавмисного розповсюдження. Це підкреслює необхідність розвитку медіаграмотності, впровадження стандартів фактчекінгу та відповідального ставлення до поширення аналітичних матеріалів [4].

Суттєвою проблемою залишається методологічна невизначеність у сфері верифікації OSINT-даних. Вона ускладнюється стрімким розвитком технологій штучного інтелекту, зокрема створенням синтетичного контенту та дідфейків. Хоча сучасні інструменти перевірки походження цифрових матеріалів можуть підвищити рівень довіри до інформації, вони не є універсальними. Тому ефективна верифікація потребує поєднання технічних засобів із критичним аналітичним мисленням.

Інтеграція штучного інтелекту в OSINT-процеси створює також низку правових та етичних викликів. Непрозорість алгоритмів, ризик помилок і наявність упереджень у даних можуть впливати на якість аналітичних результатів. Проблема так званої «чорної скриньки» ускладнює перевірку обґрунтованості висновків і обмежує можливість їх використання у правозастосовній діяльності. У зв'язку з цим важливим є забезпечення людського контролю над аналітичними процесами та впровадження механізмів алгоритмічної підзвітності [1; 5].

Етичний вимір OSINT-діяльності ґрунтується на принципах пропорційності, мінімізації втручання у приватне життя та доброчесності. Водночас навіть законне використання відкритих даних може призводити до вторинного порушення приватності, зокрема у випадках їх повторного використання поза первинним контекстом. У цьому аспекті актуальним є питання реалізації «права на забуття», яке передбачає можливість обмеження доступу до інформації, що втратила актуальність або створює непропорційні ризики для особи.

Додатковим етичним викликом є так званий «ефект мозаїки», коли з окремих фрагментів відкритої інформації формується цілісний профіль особи. Такий підхід може призводити до розкриття чутливих даних, які не були очевидними під час первинного оприлюднення, що вимагає додаткових гарантій захисту приватності.

З огляду на складність розподілу відповідальності у колективній OSINT-діяльності доцільним є застосування моделі функціонально диференційованої відповідальності. Вона передбачає чітке визначення ролей учасників на різних етапах аналітичного процесу (збору, перевірки, інтерпретації та поширення інформації) та встановлення причинно-наслідкових зв'язків між їх діями і наслідками використання аналітичних результатів.

У сучасних умовах можна виокремити три основні підходи до регулювання OSINT-діяльності: саморегулювання, нормативне регулювання та співрегулювання. Найбільш ефективним видається останній, оскільки він поєднує гнучкість професійних стандартів із механізмами державного контролю. Важливу роль у цьому процесі відіграють цифрові

платформи, які виступають посередниками у поширенні інформації та формують додатковий рівень регулювання через власні правила модерації та політики конфіденційності.

Окремим викликом є транскордонний характер OSINT-діяльності, що ускладнює застосування національного законодавства та може призводити до конфліктів юрисдикцій. Це зумовлює необхідність розвитку міжнародного співробітництва та вироблення узгоджених підходів до регулювання.

Перспективним напрямом є формування міжнародних стандартів використання відкритих даних, які б визначали критерії їх допустимості, вимоги до документування та принципи відповідальності. У цьому процесі важливу роль можуть відігравати міжнародні організації та професійні спільноти, здатні забезпечити баланс між потребами безпеки та захистом прав людини.

На національному рівні доцільним є впровадження спеціалізованих стандартів OSINT-діяльності, які б включали б вимоги до процедур верифікації, документування аналітичного процесу та забезпечення цілісності цифрових даних. Додатково варто розглянути можливість запровадження професійної сертифікації OSINT-аналітиків і розроблення етичних кодексів, що сприятиме підвищенню довіри до результатів аналітики.

Отже, колективна OSINT-діяльність поєднує значний потенціал підвищення ефективності аналітичної роботи з істотними правовими та етичними ризиками. Забезпечення їх збалансування потребує комплексного підходу, що інтегрує правові, етичні та технологічні механізми регулювання. Така модель повинна бути адаптивною до технологічних змін і водночас гарантувати належний рівень захисту основоположних прав і свобод людини.

### **Список використаних джерел**

1. Лукашук Ю. А., Цмоць У. О. Застосування інтелектуальних систем обробки даних у контексті сучасних воєнних дій. *Штучний інтелект у правовій практиці: межі та можливості* : збірник тез круглого столу (14 березня 2025 р.). Львів : Львівський державний університет внутрішніх справ, 2025. С. 137–139.
2. Про інформацію : Закон України від 2 жовтня 1992 року № 2657-XII (зі змінами і доповненнями). *Відомості Верховної Ради України*.
3. Радейко Р. І. Theoretical and Legal Framework for the Admissibility of OSINT Evidence from Social Networks: Procedural Requirements and Methodological Approaches (Case Study № 990/232/24). 2025. URL: <https://nzlubp.org.ua/index.php/journal/article/view/1657> (дата звернення: 1 травня 2026 року).
4. Dumchukov M. O. Відкрита розвідка (OSINT) у протидії інформаційним війнам: аналітичні інструменти та правові межі. 2025. URL: <https://journal-app.uzhnu.edu.ua/article/view/346448> (дата звернення: 1 травня 2026 року).
5. Zannettou S., Caulfield T., Blackburn J., de Cristofaro E., Stringhini G., Suarez-Tangil G. The Web of False Information: Rumors, Fake News, and OSINT Challenges. *ACM Computing Surveys*. 2023.

**Чаленко П. В.,**  
здобувач вищої освіти  
(*Національний юридичний університет  
імені Ярослава Мудрого*)

## **МЕТОДОЛОГІЯ OSINT-РОЗСЛІДУВАННЯ ВОЄННИХ ЗЛОЧИНІВ: КЕЙС-АНАЛІЗ ПОДІЙ У ІЗЮМСЬКОМУ ЛІСІ ІЗ ЗАСТОСУВАННЯМ ЦИФРОВИХ ІНСТРУМЕНТІВ ВЕРИФІКАЦІЇ ТА ГЕОЛОКАЦІЇ**

Повномасштабне збройне вторгнення російської федерації в Україну, розпочате 24 лютого 2022 року, супроводжується численними порушеннями норм міжнародного гуманітарного права, зокрема воєнними злочинами. Одним із найяскравіших подібних проявів стало виявлення після деокупації Харківської області у вересні 2022 року масових поховань у лісі поблизу міста Ізюм [1]. За даними українських правоохоронців, було встановлено понад 440 поховань, більшість із яких містили тіла цивільних осіб [2]. За інформацією голови Харківської обласної військової адміністрації Олега Синегубова, у 99% ексгумованих тіл зафіксовано ознаки насильницької смерті, зокрема сліди тортур – зв’язані за спиною руки, сліди побиття та удушення [3].

Актуальність даної теми зумовлена кількома факторами. По-перше, необхідністю документування воєнних злочинів для забезпечення принципу невідворотності покарання відповідно до Римського статуту Міжнародного кримінального суду та Женевських конвенцій 1949 року. По-друге, обмеженим доступом до окупованих територій на етапі активних бойових дій, що робить традиційні криміналістичні методи недостатніми. У таких умовах методологія OSINT (Open Source Intelligence) – збір, аналіз та перевірка інформації з відкритих джерел – набуває стратегічного значення [4]. Цифрові інструменти верифікації та геолокації дозволяють фіксувати події в режимі реального часу, встановлювати хронологію, ідентифікувати причетні військові підрозділи держави-агресора та збирати доказову базу, прийнятну для судового розгляду.

Проблема полягає в тому, що обсяг цифрових даних (відео, фото, супутникові знімки, пости в соціальних мережах) є величезним і часто містить дезінформацію. Тому ключовим завданням є розробка системної методології OSINT-розслідування, яка поєднує технічні інструменти з дотриманням стандартів доказування у міжнародному кримінальному праві. Кейс Ізюмського лісу слугує наочним прикладом ефективності такого підходу, оскільки саме завдяки відкритим джерелам вдалося задокументувати обставини поховань, ознаки тортур та можливу причетність конкретних підрозділів російських військ і колаборантів.

Методологія OSINT-розслідування воєнних злочинів базується на циклічному процесі, який включає кілька етапів – збір даних, верифікацію, аналіз, геолокацію та інтеграцію з традиційними доказами. Цей підхід відповідає рекомендаціям Berkeley Protocol on Digital Open Source Investigations, розробленим для розслідування порушень міжнародного кримінального права, та практиці організацій на кшталт Bellingcat, Human Rights Watch та Europol [4; 5].

На етапі збору даних дослідники використовують соціальні мережі (Telegram, VK, Twitter/X, Instagram), матеріали ЗМІ, супутникові знімки комерційних операторів (Maxar, Planet) і відкритих платформ (Sentinel Hub, Google Earth), а також публічні бази даних. У досліджуваному випадку важливим джерелом стали свідчення місцевих жителів, фото та відео, опубліковані після деокупації міста 10 вересня 2022 року. Журналісти та активісти фіксували дерев'яні хрести з номерами замість імен, що вказувало на масовий характер поховань, здійснених окупаційною владою [3; 6].

Верифікація є критично важливим етапом, покликаним відрізнити автентичний контент від постановного або маніпульованого. Для аналізу метаданих (час створення файлу, GPS-координати, модель пристрою) застосовуються інструменти ExifTool та InVID Verification; для встановлення першоджерела зображень – Google Reverse Image Search і TinEye. Хронолокація – встановлення часу події за положенням сонця та тіней – здійснюється за допомогою сервісу SunCalc або порівняння з архівними супутниковими знімками. Геолокація ґрунтується на зіставленні візуальних орієнтирів (архітектура, рельєф, рослинність, дорожні знаки тощо) із сервісами Google Earth, OpenStreetMap та спеціалізованими платформами GeoConfirmed і Mapillary.

У кейсі Ізюмського лісу OSINT-дослідники з Centre for Information Resilience (CIR) та суміжних громадських ініціатив здійснили геолокацію відеоматеріалів, поширених російськими пропагандистами, зокрема відео Романа Разума, яке фіксувало присутність підрозділів так званих «ЛНР» і «ДНР» у школі № 6 в Ізюмі – будівлі, де за свідченнями потерпілих функціонувала катівня. Порівняння архітектурних деталей фасадів і прилеглої забудови з відкритими картографічними даними дозволило підтвердити місцезнаходження об'єкта та встановити хронологію перебування підрозділів під час окупації [7].

Аналіз даних передбачає крос-референсинг – це зіставлення OSINT-матеріалів зі свідченнями очевидців, результатами судово-медичних експертиз та офіційними даними правоохоронців. У Ізюмі ексгумація виявила тіла з ознаками тортур – зв'язані руки за спиною, сліди стріляних ран, удушення. За інформацією прокуратури, серед загиблих переважали цивільні особи, хоча було також поховання щонайменше 17 українських військовослужбовців [2]. Деякі тіла мали ознаки смерті від артилерійських обстрілів або відсутності своєчасної медичної допомоги, що може кваліфікуватися як воєнний злочин за статтею 8 Римського статуту – умисне вбивство, тортури та нелюдське поводження з особами, які перебувають під захистом міжнародного гуманітарного права [8].

Важливим елементом методології є ідентифікація причетних. OSINT дозволяє встановлювати ORBAT (order of battle) – структуру підрозділів противника за допомогою геолокованих відео, геотегів, постів у соцмережах та відкритих джерел щодо переміщення військ. У Ізюмі правоохоронці загалом ідентифікували 13 колаборантів (військовослужбовців 2-го армійського корпусу РФ та представників окупаційних адміністрацій «ЛНР»/«ДНР»), яким повідомлено про підозру у державній зраді та порушенні законів і звичаїв війни [3]. OSINT-дослідження допомогли пов'язати конкретні підрозділи з місцями тортур і поховань.

Цифрові інструменти також застосовуються для створення інтерактивних мап та 3D-реконструкцій, що полегшує презентацію доказів у суді. Приклади успішного використання

OSINT у документуванні воєнних злочинів в Україні включають розслідування ударів по цивільних об'єктах, катівень та масових поховань у Бучі, Ірпені, Маріуполі. У контексті досліджуваних подій поєднання порівняльного аналізу супутникових знімків (до і після окупації) з наземними фотоматеріалами дозволило встановити, що масові поховання були здійснені саме в період перебування російських військ, а не внаслідок подій після деокупації. Ця обставина має принципове доказове значення для встановлення причинно-наслідкового зв'язку між діями окупаційних структур і загибеллю людей.

OSINT як метод не позбавлений принципів обмежень: якість результатів залежить від повноти відкритих даних, існує ризик маніпуляцій (дипфейки, підроблені геолокаційні мітки), а цифрові докази самі по собі не замінюють традиційних криміналістичних висновків. Найбільш ефективною практикою є гібридний підхід, за якого OSINT виконує функцію первинного скринінгу та генератора перевірних гіпотез, а традиційні методи – ДНК-аналіз, балістична і судово-медична експертизи – забезпечують належне підтвердження й дотримання стандартів доказування, необхідні для суду. Приміром, в Україні Офіс Генерального прокурора створив спеціальний OSINT-підрозділ для розслідування воєнних злочинів, а Europol сформував оперативну робочу групу з підтримки подібних проваджень [5].

Кейс-аналіз подій в Ізюмському лісі підтверджує високий потенціал OSINT-методології у розслідуванні воєнних злочинів. Застосування цифрових інструментів верифікації, хронолокації та геолокації дозволяє оперативно документувати злочини, встановлювати причинно-наслідкові зв'язки, ідентифікувати виконавців і формувати доказову базу, придатну для використання в національних та міжнародних судових інстанціях. Це набуває особливої ваги в умовах обмеженого фізичного доступу до місць вчинення злочинів під час активної фази бойових дій.

Разом з тим, ефективність OSINT як інструменту міжнародного кримінального переслідування залежить від дотримання наукової достовірності, чіткого додержування етичних стандартів захисту персональних даних і свідків, а також інтеграції з класичними методами криміналістики. Подальший розвиток методології потребує удосконалення інструментів виявлення маніпуляцій, підготовки кваліфікованих фахівців, міжнародної технічної та правової співпраці, а також прийняття нормативно уніфікованих протоколів збору та збереження цифрових доказів.

Розслідування злочинів в Ізюмі, як і в інших звільнених територіях, є не лише питанням правосуддя для жертв, але й важливою складовою відновлення верховенства права та запобігання повторенню подібних злочинів у майбутньому. Системне застосування OSINT у поєднанні з традиційними методами суттєво посилює спроможність України та міжнародної спільноти забезпечити притягнення винних до відповідальності.

### Список використаних джерел

1. Iziium mass graves. Wikipedia. URL: [https://en.wikipedia.org/wiki/Iziium\\_mass\\_graves](https://en.wikipedia.org/wiki/Iziium_mass_graves) (дата звернення: 30.04.2026).
2. Ukraine war: Mass exhumations at Izyum forest graves site. *BBC News*. 2022. 16 September. URL: <https://www.bbc.com/news/world-europe-62931224> (дата звернення: 30.04.2026).
3. Синегубов О. Ознаки насильницької смерті мають 99% тіл, ексгумованих у лісі біля Ізюма. *Укрінформ*. 2022. 17 вересня. URL: <https://www.ukrinform.ua/rubric-ato/3573240-oznaki-nasilnickoi-smerti-maut-99-til-eksgumovanih-u-lisi-bila-izuma-sinegubov.html> (дата звернення: 30.04.2026).
4. OSINT used to collect evidence of war crimes. Berkeley Human Rights Center. URL: <https://humanrights.berkeley.edu/hrc-in-the-news/osint-used-to-collect-evidence-of-war-crimes/> (дата звернення: 30.04.2026).
5. Europol sets up OSINT taskforce to support investigations into war crimes committed in Ukraine. *Europol*. 2023. 21 November. URL: <https://www.europol.europa.eu/media-press/newsroom/news/europol-sets-osint-taskforce-to-support-investigations-war-crimes-committed-in-ukraine> (дата звернення: 30.04.2026).
6. Investigating Izyum's Mass Graves. Institute for War and Peace Reporting. 2022. 27 September. URL: <https://iwpr.net/global-voices/investigating-izyums-mass-graves> (дата звернення: 30.04.2026).
7. One year on from the discovery of mass graves in Iziium, we identify the enablers of torture. Centre for Information Resilience. 2023. 12 September. URL: <https://www.info-res.org/eyes-on-russia/reports/one-year-on-from-the-discovery-of-mass-graves-in-izium-we-identify-the-enablers-of-torture/> (дата звернення: 30.04.2026).
8. Ukraine: Mass graves in Iziium is a macabre reminder of the cost of Russian aggression. Amnesty International. 2022. 16 September. URL: <https://www.amnesty.org/en/latest/news/2022/09/ukraine-mass-graves-in-izium-is-a-macabre-reminder-of-the-cost-of-russian-aggression/> (дата звернення: 30.04.2026).
9. «Murders for the sake of Russian propaganda» – Ukraine identifies 13 soldiers committed war crimes in Iziium. *The Kyiv Independent*. 2026. 13 March. URL: <https://kyivindependent.com/murders-for-sake-of-russian-propaganda-ukraine-identifies-13-soldiers-committed-in-war-crimes-in-izium/> (дата звернення: 30.04.2026).

**Чирук Б. Р.,**  
курсант навчально-наукового інституту  
підготовки фахівців для підрозділів  
кримінальної поліції  
Національної поліції України  
*(Одеський державний університет внутрішніх справ)*  
Науковий керівник: **Калугін В. Ю.,**  
професор кафедри кримінального аналізу  
та інформаційних технологій,  
кандидат юридичних наук, доцент  
*(Одеський державний університет внутрішніх справ)*

## **OSINT ЯК ІНСТРУМЕНТ ВИЯВЛЕННЯ ТА ФІКСАЦІЇ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ: ПРИКЛАДНИЙ АСПЕКТ**

У сучасних умовах цифровізації суспільства та трансформації злочинності особливого значення набуває використання відкритих джерел інформації (OSINT - Open Source Intelligence) у діяльності правоохоронних органів. Зростання обсягів інформації у мережі Інтернет, активне використання соціальних мереж та цифрових платформ створюють нові можливості для виявлення та документування кримінальних правопорушень. Водночас це вимагає від працівників поліції належного рівня підготовки та володіння сучасними інструментами аналізу інформації.

Правові засади використання OSINT у кримінальному провадженні визначаються положеннями Кримінального процесуального кодексу України, зокрема нормами щодо джерел доказів, допустимості доказової інформації та порядку її фіксації [1]. Відповідно до чинного законодавства, інформація, отримана з відкритих джерел, може бути використана як доказ за умови її належного процесуального оформлення та перевірки на достовірність. Це узгоджується із загальними принципами кримінального процесу, зокрема законності, змагальності та забезпечення права на захист.

Сутність OSINT полягає у цілеспрямованому зборі, систематизації та аналітичній обробці інформації з відкритих джерел, до яких належать соціальні мережі (Facebook, Instagram, Telegram), відеохостинги, форуми, державні реєстри, відкриті бази даних та інші інформаційні ресурси. Як зазначає М. Баззелл, відкриті джерела є одним із найбільш недооцінених, але водночас ефективних інструментів розслідування, оскільки містять значний обсяг інформації про осіб, події та обставини. [2, с. 18–22] Особливістю OSINT є його легальність, що дозволяє уникнути застосування негласних слідчих (розшукових). Разом із тим, використання OSINT у практичній діяльності потребує чітко сформованих професійних навичок, які забезпечують ефективність збору та аналізу інформації.

Першочергове значення мають навички пошуку інформації. Працівник поліції повинен володіти техніками розширеного пошуку, зокрема використанням логічних операторів (AND, OR), спеціальних команд пошукових систем (site:, filetype:, cache:) та інструментів для пошуку в соціальних мережах. Наприклад, встановлення особи за нікнеймом може здійснюватися шляхом аналізу однакових логінів на різних платформах, що дозволяє ідентифікувати користувача. [2, с. 105].

Другим важливим елементом є верифікація інформації. Практика свідчить, що значна частина інформації в мережі Інтернет може бути недостовірною або навмисно спотвореною.

Третім компонентом є аналітичні навички. Вони передбачають здатність встановлювати причинно-наслідкові зв'язки між подіями, визначати роль окремих осіб у вчиненні кримінального правопорушення та формувати узагальнені висновки. Зазначається, що аналітичний етап є ключовим, оскільки саме він дозволяє перетворити інформацію на доказ [4, с. 118].

Окремої уваги потребують навички документування результатів OSINT. У кримінальному провадженні важливим є не лише отримання інформації, а й її правильне оформлення. Зокрема, здійснюється фіксація веб-сторінок шляхом складання протоколу огляду, збереження скріншотів із зазначенням дати і часу, а також використання спеціалізованого програмного забезпечення для архівації веб-контенту.

Практичне застосування OSINT у діяльності кримінальної поліції є надзвичайно широким. Зокрема, він використовується для:

- встановлення особи правопорушника за цифровими слідами (нікнейми, фото, контакти);
- виявлення співучасників злочину через аналіз соціальних зв'язків;
- документування фактів вчинення кримінальних правопорушень;
- збору інформації про місцезнаходження особи або об'єкта;
- фіксації воєнних злочинів та діяльності незаконних формувань.

Наприклад, у практиці розслідування воєнних злочинів активно використовується аналіз відео та фото з соціальних мереж для встановлення місця події, ідентифікації осіб та підтвердження факту вчинення протиправних дій. За даними досліджень, саме OSINT дозволяє документувати події, доступ до яких обмежений через бойові дії [3, с. 76].

Таким чином, OSINT є ефективним та сучасним інструментом діяльності правоохоронних органів, який забезпечує можливість оперативного виявлення та фіксації кримінальних правопорушень. Його використання вимагає не лише знання нормативної бази, але й сформованих практичних навичок пошуку, перевірки, аналізу та документування інформації. Подальший розвиток цієї сфери пов'язаний із удосконаленням методик роботи з відкритими джерелами, впровадженням сучасних технологій та підвищенням рівня професійної підготовки працівників поліції.

### **Список використаних джерел**

1. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI. URL: <https://zakon.rada.gov.ua/laws/show/4651-17#Text>
2. Філософія цифрової людини і цифрового суспільства: теорія і практика : монографія / В. Г. Воронкова, В. О. Нікітенко. Львів-Торунь: Liha-Pres, 2022, 460 с.
3. OSINT Open Source Intelligence. Інструменти та методи: навчальний посібник / О. Користін, С. Демедюк, К. Ісмайлов, Д. Ланде та ін. ; за заг. ред. О. Є. Користіна, С. В. Демедюка. Київ : 2025. 460 с.
4. Дудоров О. О. Використання відкритих джерел у кримінальному провадженні. *Юридичний вісник*. 2022. № 3. С. 115–120.

**Чубенко А.Г.,**  
доктор юридичних наук, професор  
(Національний університет «Полтавська політехніка  
імені Юрія Кондратюка»)

## **РОЛЬ OSINT-FORENSICS У ПРОТИДІЇ НЕЛЕГАЛЬНОМУ ОБІГУ КУЛЬТУРНИХ ЦІННОСТЕЙ ТА ЗАХИСТІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ**

Повномасштабна війна російської федерації проти України супроводжується масовим розграбуванням музеїв, приватних колекцій та знищенням об'єктів культурної спадщини. Викрадені артефакти незаконно переміщуються за кордон з метою подальшої тіньової легалізації. За таких умов традиційних методів правоохоронної діяльності стає недостатньо. Виникає гостра потреба у застосуванні інструментів розвідки на основі відкритих джерел (OSINT) для моніторингу нелегального обігу культурних цінностей. У контексті національної безпеки своєчасне виявлення таких злочинів дозволяє не лише забезпечити реституцію, але й блокувати канали відмивання коштів та фінансування ворожих мереж.

Роль OSINT у забезпеченні національної безпеки та розслідуванні воєнних злочинів стає предметом посиленої уваги як міжнародних, так і вітчизняних фахівців. Зокрема, FATF наголошує на ризиках відмивання коштів на ринку мистецтва та антикваріату. Питання застосування цифрової розвідки для відстеження культурних цінностей розглядається крізь призму концепції правової інженерії.

Метою статті є визначення можливостей інструментів OSINT-Forensics у протидії незаконному обігу викрадених культурних цінностей як складової забезпечення національної безпеки України.

Сучасний тіньовий ринок культурних цінностей характеризується високим рівнем анонімності учасників та складністю перевірки провенансу. Водночас процес легалізації викрадених об'єктів неминуче залишає «цифрові сліди». Саме тому OSINT-Forensics перетворюється на ключовий інструмент документування воєнних злочинів проти культурної спадщини.

Практичне застосування OSINT-методів у цій сфері охоплює декілька напрямів. По-перше, це моніторинг міжнародних та регіональних онлайн-аукціонів, електронних каталогів антикварних галерей, а також спеціалізованих форумів і закритих груп у соціальних мережах, де можуть пропонуватися викрадені українські артефакти. По-друге, аналіз відкритих супутникових знімків для фіксації фактів руйнування та розграбування місць археологічних розкопок на тимчасово окупованих територіях. По-третє, поєднання цифрової розвідки з фінансовим профілюванням (FININT), що дозволяє встановлювати логістичні маршрути переміщення об'єктів, підставні структури та кінцевих бенефіціарів нелегальних транзакцій.

Ефективність OSINT-досліджень суттєво зростає за умови їх інтеграції з національними та міжнародними цифровими реєстрами втрачених і викрадених культурних цінностей (зокрема, з базами INTERPOL). У цій моделі державні установи, музейні працівники, експерти-мистецтвознавці та незалежні OSINT-аналітики утворюють децентралізовану мережу верифікації.

Отже, застосування методів OSINT-Forensics є критично важливим кроком для протидії нелегальному обігу культурних цінностей. Інтеграція цифрової розвідки, фінансового моніторингу та міжнародних реєстрів формує потужну аналітичну інфраструктуру, яка суттєво ускладнює легалізацію викраденого майна і зміцнює національну безпеку України.

### **Список використаних джерел**

1. Financial Action Task Force (FATF). Money Laundering and Terrorist Financing in the Art and Antiquities Market. Paris : FATF, 2023.
2. Chubenko A. Cultural Property as an Instrument of Money Laundering: International Legal Engineering. Zenodo. 2026. DOI: 10.5281/zenodo.19389446.

**Швець Д. В.,**  
ректор,  
доктор юридичних наук, професор,  
заслужений працівник освіти України  
(Львівський державний університет внутрішніх справ)

## **СТРАТЕГІЧНІ ПРІОРИТЕТИ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ OSINT У НАЦІОНАЛЬНУ ЕКОСИСТЕМУ КІБЕРБЕЗПЕКИ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ**

У сучасному геополітичному ландшафті інформаційний простір перестав бути лише засобом комунікації, змінившись на повноцінний театр воєнних дій, де цифрова трансформація державних інституцій та критичної інфраструктури створює як нові можливості, так і критичні вразливості. Для України, яка перебуває в епіцентрі першої у світі повномасштабної кібервійни, виникає гостра потреба у впровадженні інноваційних методів моніторингу та нейтралізації загроз, серед яких найбільш перспективним напрямком є Open Source Intelligence (OSINT) – розвідка на основі відкритих джерел. Традиційні підходи до кібербезпеки, які базуються переважно на захисному периметрі, сьогодні є недостатніми без глибокої аналітичної підтримки, яка забезпечує системну діяльність із отримання та інтерпретації інформації з публічно доступних ресурсів. OSINT позиціонується як комплексна методологія збору, верифікації та аналізу даних із мереж Інтернету, соціальних медіа, супутникових знімків, офіційних реєстрів та даркнету з метою отримання розвідувальної інформації, що має екзистенційне значення для прийняття управлінських рішень у сфері національної оборони. На відміну від класичних видів розвідки, OSINT базується на легальних методах доступу до даних, але вимагає спеціальних експертів для роботи з масивами Big Data та відсіву фейків і маніпуляцій. У системі кібербезпеки відкрита розвідка виконує роль системи раннього передавання, дозволяючи ідентифікувати підготовку до нападу ще на етапі ворожого сканування, а аналіз активності на хакерських форумах чи моніторинг репозиторіїв відкритого коду дає змогу виявляти витoki облікових даних до моменту їх використання зловмисниками.

Повноцінна інтеграція OSINT вимагає, насамперед, політичного визнання цього інструменту як невід'ємного елемента національного безпекового інструментарію, який має знайти відображення в оновленій Стратегії кібербезпеки України та Національному плані реагування на кіберінциденти. Нормативно-правове регулювання в даному контексті є ключовим завданням, залишивши існуючу правову прогалину щодо статусу результатів OSINT-дослідження у судовому процесі створює значні перешкоди для притягнення кіберзлочинців до відповідальності. Необхідно ініціювати внесення змін до Кримінального процесуального кодексу України щодо визначення цифрових доказів, отриманих із відкритих джерел, та розробити чіткі кодекси регламенту взаємодії між суб'єктами кібербезпеки – ДССЗІ, СБУ та Кіберполіції. Важливою передумовою ефективності є створення єдиної інституційної архітектури, зокрема Національного центру OSINT, який міг би функціонувати як міжвідомчий координаційний хаб у структурі Ради національної безпеки і оборони України. Така установа забезпечила подолання відомчої розпорошеності, формування спільної аналітичної бази та стандартизацію методів документування цифрових слідів, що є

критичним для міжнародної атрибуції кібератак та формування доказової бази для міжнародних трибуналів.

Технологічний аспект інтеграції передбачає розбудову національної програмної інфраструктури, оскільки сучасна аналітика не може функціонувати без систем автоматизованого збору даних, інструментів цифрового профілювання та платформи для аналізу матриці суспільних зв'язків. Використання алгоритмів штучного інтелекту та адаптивного самонавчання задля моніторингу сегментів даркнету та месенджерів дозволяє в автоматичному режимі класифікувати рівні загрози та виявляти аномалії в інформаційному полі, що свідчить про підготовку дезінформаційних запитів або ПІСО. Розвиток таких технологій потребує активного залучення вітчизняного ІТ-сектора та стартапів, які вже мають успішний досвід розробки системи геопросторової розвідки та аналізу супутникових знімків для потреб оборони. Паралельно з модернізацією технічного інструментарію загострюється проблема фахового забезпечення галузі. Наразі розвиток кадрового потенціалу в сегменті OSINT стримується недостатньою адаптованістю освітніх стандартів та дефіцитом спеціалізованих сертифікаційних програм. Необхідна синергія академічної спільноти та сектору безпеки і оборони для модернізації навчальних планів за напрямками ІТ та права. Впровадження спеціалізованих модулів з OSINT-аналітики має стати невід'ємною складовою професійної підготовки офіцерів кібербезпеки та фахівців з військової розвідки. Окремим стратегічним вектором є розбудова державно-приватного партнерства та легалізація взаємодії з волонтерськими спільнотами. Діяльність вітчизняних та міжнародних структур (зокрема InformNapalm, Molfar, OSINT-UA та Bellingcat) підтвердила критичну роль громадянського суспільства в інформаційному протиборстві. Гнучкість та швидкість аналітичних процедур громадянського сектору дозволяють ефективніше виявляти ворожі активи та деанонімізувати комбатантів, ніж це забезпечують традиційні бюрократичні механізми. Держава має створити правові механізми залучення таких фахівців до офіційного моніторингу загроз, забезпечуючи їм доступ до відкритих державних реєстрів та технічну підтримку в обмін на експертну допомогу в розслідуванні кіберзлочинів. Лише за умови поєднання зусиль владних інститутів, приватного сектору та громадянського суспільства можливо побудувати стійку систему захисту, де OSINT виступатиме одночасно превентивним, аналітичним та доказовим інструментом. Перехід від реактивної моделі захисту до проактивного аналізу середовища дозволяє не тільки мінімізувати наслідки кіберінцидентів, а й здобути стратегічну ініціативу в глобальному цифровому протистоянні. Таким чином, комплексне впровадження OSINT в національну систему кібербезпеки має розглядатися як фундаментальне складування сектору безпеки, що забезпечує цифровий суверенітет та стійкість держави в умовах перманентних гібридних викликів реформ XXI століття. Це вимагає консолідації ресурсів для синхронного розвитку нормативної бази, технологічного інструментарію та інтелектуального капіталу, щоб у сукупності створити відкриту інформацію про потужну зброю захисту національних інтересів.

**Ширкунов О. Д.,**

курсант факультету безпеки державного кордону  
(*Національна академія Державної прикордонної служби України  
імені Богдана Хмельницького*)

**Фільченко С. В.,**

курсант факультету безпеки державного кордону  
(*Національна академія Державної прикордонної служби України  
імені Богдана Хмельницького*)

**Каштелян С. О.,**

доцент кафедри прикордонної служби,  
кандидат військових наук, доцент  
(*Національна академія Державної прикордонної служби України  
імені Богдана Хмельницького*)

## **ІНТЕГРАЦІЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В OSINT-МОНІТОРИНГ ЯК ЧИННИК ПОСИЛЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ**

Сьогодні, в умовах повномасштабної збройної агресії та постійних гібридних загроз, підходи до забезпечення національної безпеки суттєво трансформуються [1]. Інформація з відкритих джерел (OSINT – Open Source Intelligence) перетворилася з допоміжного інструменту на один із ключових методів розвідки та аналітики для правоохоронних органів, спецслужб та прикордонних підрозділів. Відкриті реєстри, соціальні мережі, супутникові знімки, форуми та платформи обміну повідомленнями стали повноцінним полем бою в інформаційному просторі.

Проте на сучасному етапі фахівці з безпеки зіткнулися з новою, не менш серйозною проблемою – критичним надлишком інформації (феноменом Big Data). Щодня генеруються терабайти нових даних. Вручну відслідкувати ворожі публікації, проаналізувати тисячі фотографій чи знайти зв'язки між підозрілими особами стає фізично неможливо. Людина здатна якісно опрацювати лише обмежений обсяг тексту чи відео за зміну. Традиційні методи пошуку займають надто багато часу, якого в реальних бойових чи оперативних умовах просто немає [2, с. 14]. Саме тому інтеграція алгоритмів штучного інтелекту в спеціалізоване програмне забезпечення для OSINT є не просто перспективною, а критичною необхідністю.

На практиці штучний інтелект працює як своєрідний багатошаровий «фільтр» та підсилювач можливостей аналітика. Одним із найефективніших напрямів є використання алгоритмів обробки природної мови. Сучасні мовні моделі здатні в автоматичному режимі цілодобово моніторити сотні тисяч повідомлень у Telegram-каналах, пабліках та форумах. Програма самостійно перекладає сленг або іноземні мови, визначає тональність повідомлень (негативні, радикальні чи панічні настрої) та сигналізує про загрози [3, с. 82]. Для підрозділів охорони кордону це дає змогу на ранніх етапах виявляти підготовку до провокацій на прикордонних територіях, відслідковувати роботу ворожих інформаційно-психологічних операцій або знаходити канали комунікації організаторів незаконного переправлення осіб.

Окремої уваги заслуговує робота з візуальним контентом за допомогою технологій комп'ютерного зору (Computer Vision). Інструменти на базі машинного навчання вже зараз здатні автоматично сканувати години відеоматеріалів. Вони розпізнають обличчя людей у натовпі, ідентифікують приховану або замасковану військову техніку, а також здійснюють

високоточну геолокацію. Наприклад, ШІ може порівняти контури будівель, рельєф місцевості чи навіть тіні на фотографії з відкритих джерел із супутниковими картами, видаючи точні координати зйомки за лічені хвилини. Під час документування воєнних злочинів чи фіксації присутності ворожих диверсійно-розвідувальних груп це економить сотні годин кропіткої роботи оперативників [4, с. 115].

Крім того, надзвичайно перспективним є побудова соціальних графів та предиктивна (прогнозна) аналітика. Якщо слідчий або оперативний працівник виявляє одного учасника злочинної групи (наприклад, контрабандиста), ШІ здатен блискавично проаналізувати його цифровий слід: вподобання, спільні фото, геотеги, відкриті фінансові транзакції. Програма автоматично будує схему зв'язків, виявляючи всю мережу спільників. Аналізуючи історичні дані, алгоритми навіть можуть прогнозувати найімовірніші маршрути та час незаконного перетину кордону, що дозволяє діяти на випередження.

Звичайно, у масовому впровадженні ШІ існують суттєві виклики. Найбільшою загрозою сьогодні є стрімке поширення генеративного штучного інтелекту та технологій «Deepfake» [3, с. 85]. Зловмисники здатні генерувати реалістичні, але повністю підроблені відео та голосові повідомлення (наприклад, фейкові накази командирів або компрометуючі матеріали на посадових осіб). Тому розробникам безпекового забезпечення доводиться постійно вдосконалювати зустрічні алгоритми, щоб виявляти машинне втручання в медіафайли на рівні пікселів або звукових частот.

Ще одним важливим аспектом є правове регулювання. Масовий автоматизований збір даних в інтернеті часто межує з порушенням права на приватність. Використання таких потужних інструментів правоохоронцями має бути чітко регламентоване законодавством, щоб дотримуватися балансу між інтересами національної безпеки та правами людини [4, с. 120]. Крім того, машина не несе юридичної відповідальності за помилки, тому всі висновки ШІ повинні підлягати обов'язковій верифікації.

Підсумовуючи, можна стверджувати, що штучний інтелект не замінить людину-аналітика, проте він створює колосальну перевагу у швидкості та обсягах обробки інформації. Концепція «людина-в-контурі-управління» (human-in-the-loop) залишається незмінною: ШІ виконує чорнову аналітичну роботу, а кінцеве рішення приймає офіцер.

### **Список використаних джерел**

1. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19> (дата звернення: 27.04.2026).
2. OSINT (Open Source Intelligence): Теорія та методологія : навч. посіб. Київ : Асоц. науковців та фахівців у сфері оперативно-розшукової діяльності, 2024. 156 с.
3. Роль OSINT-досліджень у підвищенні рівня національної безпеки України : матеріали Всеукр. наук.-практ. конф. (м. Львів, 7 трав. 2025 р.). Львів : ЛьвДУВС, 2025. 210 с.
4. Штучний інтелект та права людини: орієнтири та обмеження у контексті національної безпеки та оборони : аналіт. доп. Київ : Укр. Гельсін. спілка з прав людини, 2024. 132 с.

**Школьніков В. І.,**  
завідувач кафедри кримінології та  
інформаційних технологій,  
доктор філософії в галузі права, доцент  
(Національна академія внутрішніх справ)

## **АВТОМАТИЗАЦІЯ ЗБОРУ, ОБРОБКИ ТА АНАЛІЗУ ІНФОРМАЦІЇ З ВІДКРИТИХ ДЖЕРЕЛ ЗА ДОПОМОГОЮ ШІ-АГЕНТІВ**

В умовах стрімкого зростання обсягів інформації автоматизація процесів збору, обробки та аналізу Big Data (великих обсягів інформації) з відкритих джерел є необхідною умовою для якісного OSINT-дослідження. На постійній основі аналітики інформації з відкритих джерел (OSINT-аналітики) досліджують структуровані та неструктуровані дані з соціальних мереж, веб-сайтів, відкритих реєстрів, месенджерів, геоінформаційних систем тощо.

Слід зазначити, що ШІ-агенти можуть допомогти OSINT-аналітику не лише зібрати та обробити інформацію з відкритих джерел, а й створити план OSINT-дослідження та сформувані проміжні аналітичні висновки.

ШІ-агенти (англ. AI-agents) – це автономні програмні системи, керовані великими мовними моделями (LLM), які здатні міркувати, планувати та використовувати інструменти (API, браузер, поштові клієнти, пошукові системи тощо) для досягнення конкретних цілей із мінімальним втручанням людини. На сьогодні найбільш відомим ШІ-агентами є Codex від компанії OpenAI [1] та Claude Code від компанії Anthropic [2]. У той же час слід зауважити, що існує можливість використовувати ШІ-агенти локально, але для якісної організації даної роботи необхідно мати достатні обчислювальні потужності.

ШІ-агенти можуть проаналізувати поставлену OSINT-аналітиком мету, сформувані план дій та за допомогою програмного коду, який взаємодіє із інтерфейсом користувача, здійснити пошук, обробку та аналіз інформації. При цьому слід зауважити, що ШІ-агент у разі виникнення проблем самостійно може їх вирішувати без участі людини. Це дозволяє реалізовувати багаторішні завдання OSINT-дослідження.

На різних етапах OSINT-дослідження ШІ-агент може надати допомогу OSINT-аналітику в:

1) формуванні дослідницького питання, визначенні ключових джерел інформації та побудові алгоритму пошуку інформації з відкритих джерел (**на етапі планування OSINT-дослідження**);

2) перегляді веб-сайтів із подальшим копіюванням текстової, графічної чи іншої інформації та її структуризацією у зручний для OSINT-аналітика формат (наприклад, CSV, Excel, SQL, JSON тощо). Додатково ШІ-агенти можуть самостійно збирати інформацію через API – англ. Application Programming Interface (**на етапі збору даних**);

3) «очистці» даних. За необхідності ШІ-агент може забезпечити переклад тексту, визначити такі структуровані сутності як номери телефонів, адреси електронних пошт, адреси криптогаманців, домени, IP-адреси тощо (**на етапі обробки даних**);

4) групуванні знайденої інформації за темами, джерелами, особами, подіями, часовими періодами тощо (**на етапі класифікації даних**);

5) порівнянні інформації з різних джерел з метою виявлення суперечностей (**на етапі верифікації даних**);

б) виявленні зв'язків між фізичними та юридичними особами, подіями, адресами, телефонами, фінансовими операціями тощо (**на етапі аналізу даних**);

7) підготовці аналітичних довідок, таблиць, схем взаємозв'язків, коротких висновків і рекомендацій (**на етапі формування звіту**).

Головною перевагою використання OSINT-аналітиком ШІ-агентів є прискорення процесів збору, обробки та аналізу інформації з відкритих джерел, але в той же час слід пам'ятати про ризик помилкових висновків або «галюцинацій» з боку великих мовних моделей (LLM).

OSINT-аналітик може використовувати ШІ-агенти для моніторингу соціальних мереж, аналізу дезінформаційних кампаній, аналізу руху віртуальних активів, аналізу інформації про публічні закупівлі тощо.

### **Список використаних джерел**

1. Codex. Агент програмування, який допомагає створювати та розгортати рішення за допомогою штучного інтелекту (ШІ) – на базі ChatGPT. *OpenAI*. URL: <https://openai.com/uk-UA/codex/> (дата звернення 01.05.2026).

2. Claude Code. *Anthropic*. URL: <https://claude.com/product/claude-code> (дата звернення 01.05.2026).

**АНАЛІЗ РИЗИКІВ ВИКОРИСТАННЯ ХМАРНИХ ПЛАТФОРМ  
ДЛЯ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ  
У КОНТЕКСТІ OSINT-ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ  
ТА ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ**

У сучасних умовах цифровізації суспільства та трансформації інформаційного середовища діяльність правоохоронних органів дедалі більше базується на використанні відкритих джерел інформації (OSINT). Такий підхід дозволяє оперативно отримувати, систематизувати та аналізувати значні обсяги даних, зокрема персональних, що циркулюють у мережі Інтернет. Водночас ефективність OSINT-діяльності значною мірою залежить від інструментальних засобів обробки інформації, серед яких провідне місце посідають хмарні платформи.

Хмарні сервіси забезпечують масштабованість обчислювальних ресурсів, доступність даних у режимі реального часу та можливість колективної роботи, що є критично важливим для сучасних аналітичних процесів. Разом з тим їх використання супроводжується низкою ризиків, які мають комплексний характер і стосуються як технічних, так і організаційно-правових аспектів. Особливої актуальності ці ризики набувають в умовах воєнного стану в Україні, коли інформаційний простір стає об'єктом активного впливу з боку противника.

Одним із ключових викликів є обмежений рівень контролю над інфраструктурою хмарних сервісів. На відміну від локальних систем, де організація має повний контроль над апаратними та програмними компонентами, у хмарному середовищі значна частина відповідальності покладається на провайдера. Це створює потенційні вразливості, пов'язані з несанкціонованим доступом до даних, порушенням їх цілісності або доступності. Для правоохоронних органів такі ризики є критичними, оскільки оброблювана інформація може містити відомості про об'єкти оперативного інтересу, хід розслідувань або персональні дані громадян.

Особливу увагу слід приділити ризикам витоку персональних даних. У контексті OSINT-діяльності навіть часткова компрометація інформації може призвести до розкриття аналітичних методів, джерел інформації або ідентифікації співробітників. У свою чергу це створює передумови для протидії з боку противника, включаючи проведення контррозвідувальних заходів або інформаційно-психологічних операцій.

Значним фактором ризику є також юрисдикційна залежність хмарних платформ. Багато провайдерів функціонують у правових полях іноземних держав, що передбачає можливість доступу до даних відповідно до законодавства цих країн. У контексті забезпечення національної безпеки це може створювати загрози витоку інформації через правові механізми або міжнародні запити. Додатково варто враховувати ризики, пов'язані з кіберзагрозами, включаючи атаки на інфраструктуру провайдерів, що можуть призвести до компрометації великих масивів даних.

У системі OSINT-діяльності правоохоронних органів хмарні платформи використовуються не лише для зберігання інформації, але й для її обробки, аналізу та обміну між підрозділами. Це передбачає активну взаємодію користувачів із даними, що підвищує

значення контролю доступу та автентифікації. Недостатній рівень захисту облікових записів або помилки в налаштуваннях доступу можуть призвести до несанкціонованого поширення інформації або її використання третіми особами.

В умовах гібридної війни інформація стає одним із ключових ресурсів, а її захист - важливою складовою національної безпеки. Використання хмарних платформ без належного врахування ризиків може бути використано противником для збору розвідувальної інформації, аналізу поведінкових моделей та формування цільових впливів. У цьому контексті забезпечення безпеки обробки персональних даних набуває значення елемента контр-OSINT діяльності.

Окремим аспектом є інтеграція сучасних технологій, зокрема штучного інтелекту, у процеси обробки даних. Використання AI-інструментів у хмарних середовищах дозволяє автоматизувати аналіз великих масивів інформації, однак водночас підвищує ризики, пов'язані з централізацією даних та можливістю їх несанкціонованого використання. Крім того, алгоритмічні системи можуть бути вразливими до маніпуляцій або використання недостовірних даних.

З метою мінімізації ризиків використання хмарних платформ у діяльності правоохоронних органів доцільно впроваджувати комплексні заходи захисту. До них належать застосування сучасних криптографічних механізмів, багатфакторної автентифікації, сегментації доступу до даних, а також регулярний аудит безпеки. Важливим є також розроблення внутрішніх нормативних документів, що регламентують порядок роботи з персональними даними у хмарних середовищах.

Не менш важливим є підвищення рівня обізнаності персоналу щодо ризиків інформаційної безпеки. Людський фактор залишається одним із найслабших елементів системи захисту, тому навчання співробітників та формування культури безпечної роботи з інформацією є необхідною умовою ефективного функціонування OSINT-підрозділів.

Використання хмарних платформ у діяльності правоохоронних органів має як значний потенціал, так і суттєві ризики. У контексті OSINT-діяльності ці ризики пов'язані насамперед із захистом персональних даних, забезпеченням конфіденційності та недопущенням компрометації інформації. Мінімізація ризиків потребує комплексного підходу, що поєднує технічні, організаційні та правові механізми. Ефективне управління зазначеними ризиками є важливою передумовою забезпечення національної безпеки України в умовах сучасних викликів та загроз.

### **Список використаних джерел**

1. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення: 29.04.2026).
2. Grance T. and Jansen W. Guidelines on Security and Privacy in Public Cloud Computing, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD. URL: <https://doi.org/10.6028/NIST.SP.800-144> (дата звернення: 29.04.2026).
3. European Union Agency for Cybersecurity (ENISA). Cloud Computing Risk Assessment. URL: <https://www.enisa.europa.eu/sites/default/files/publications/Cloud%20Computing%20Security%20Risk%20Assessment.pdf> (дата звернення: 29.04.2026).

**Юрченко Р. В.,**  
старший науковий співробітник  
науково-дослідного відділу наукового центру  
Сухопутних військ  
*(Національна академія сухопутних військ)*

**Івахів О. С.,**  
провідний науковий співробітник  
науково-дослідного відділу наукового центру  
Сухопутних військ,  
кандидат політичних наук, працівник ЗС України  
*(Національна академія сухопутних військ)*

**Лібрук-Ліпкевич С. Я.,**  
старший науковий співробітник  
науково-дослідного відділу наукового центру  
Сухопутних військ, кандидат історичних наук,  
старший науковий співробітник,  
працівник ЗС України  
*(Національна академія сухопутних військ)*

## **ВИКОРИСТАННЯ МЕТОДІВ OSINT У РОСІЙСЬКО-УКРАЇНСЬКІЙ КІБЕРПРОСТОРОВІЙ КОГНІТИВНІЙ ВІЙНІ: ОСОБЛИВОСТІ ТА ПРОТИДІЯ**

У провідних країнах світу OSINT є одним із важливих інструментів захисту національних інтересів, а також основною складовою в діяльності профільних силових відомств. Так, у США та країнах НАТО існують окремі мережі центрів, що займаються збиранням та обробкою інформації з подальшим формуванням відповідних баз даних та практичним їх застосуванням для прийняття необхідних рішень [1].

Людство фактично постійно воює, однак щоразу в різних доменах – економічних, інформаційних, технологічних, дипломатичних, торгових, розвідувальних, кіберпростору, терактів, шпигунських та агентурних.

Протягом останніх років Україна відчуває реальну необхідність захисту своєї національної безпеки. Згідно статті 3 Закону України «Про національну безпеку України» визначено, 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 життя життєдіяльності; суспільства – його демократичних цінностей, добробуту та умов для сталого розвитку; держави – її конституційного ладу, суверенітету, територіальної цінності та недоторканості; території, навколишнього природного середовища – від надзвичайних ситуацій [3].

Переконати агресора зупинитись можна лише застосувавши всі можливі методи переконання, і лише тоді, коли агресор зрозуміє, що наступати далі безперспективно, і кожен наступний крок лише погіршує ситуацію – зупинитись – це єдиний спосіб вижити. По своїй природі поведінку людини визначає її набір ідентичностей – своєрідний код, який програмується з її народження соціальним оточенням і власне тут найбільше поле бою для когнітивної війни, оскільки тут “зламується” об’єктивне сприйняття реальності та

відбувається підміна понять. Задля цього агресор масово використовує інформаційні операції, дезінформацію, пропаганду, психологічні операції, штучний інтелект, дипфейки, бот-мережі, меми, тролінг, нейронауки.

Термін «OSINT» набув поширення наприкінці 1990-х років і є важливим компонентом системи національної безпеки України, яка перебуває в стані збройної боротьби з російським агресором кіберпросторовій війні.

Технології та методики OSINT (Open Source Intelligence) – це розвідка на основі відкритих джерел: інтернету, соціальних мереж, відкритих баз даних, супутникових знімків, засобів масової інформації, форумів, офіційної звітності, яка є загальнодоступною та легальною.

У кіберпросторовій когнітивній війні OSINT забезпечує:

- раннє виявлення загроз (включаючи кібератаки, витоки інформаційних даних, активність бот-мереж);
- прозорість джерел – інформація повинна бути доступною для громадськості без порушення законодавства та етичних норм;
- достовірність - необхідно підтвердити достовірність отриманої інформації через верифікацію джерел і співставлення даних з іншими незалежними джерелами;
- атрибуцію атак (зокрема через збір даних про групи хакерів, їх інфраструктури та цифрові відбитки);
- оцінку вразливостей критичної інфраструктури через аналіз відкритих технічних даних;
- контррозвідувальне забезпечення (виявлення дезінформаційних та фішингових кампаній та елементів інформаційно-психологічних операцій (ІПСО)).

Під час російсько-української війни застосовують такі методи та інструменти OSINT:

1. Геолокація та аналіз руху військ – включає порівняння відео/фото з картами Google Maps, Google Earth, Wikimapia для визначення координат.
2. Аналіз соціальних мереж (SOCMINT) – пошук інформації в профілях військових рф, аналіз коментарів.
3. Супутникові знімки – використання сервісів для моніторингу руйнувань, зведення фортифікацій.
4. Аналіз метаданих – вивчення EXIF-даних фотографій для визначення часу та місця зйомки.
5. Верифікація втрат техніки: Проєкти на кшталт Oгух підраховують знищену техніку обох сторін на основі фото- та відеодоказів, що забезпечує об'єктивність даних.

Особливостями використання OSINT у російсько-українській війні є:

1. Масштабність та швидкість. Завдяки соціальним мережам (Telegram, Twitter/X, TikTok) швидко поширюється інформація. Геолокація відеозаписів дозволяє визначати місце знаходження техніки за короткий проміжок часу.
2. Фіксація воєнних злочинів. OSINT – інструменти використовуються для встановлення фактів вбивств, катувань, руйнувань критичної та цивільної інфраструктури, ідентифікація російських військових, які їх вчинили.
3. Аналіз бойових дій. OSINT – дослідники (наприклад, Bellingcat, InformNapalm) аналізують супутникові знімки, (Sentinel, Maxar) та фото/відео з фронту для відстеження переміщень військ, втрат техніки та змін лінії фронту.
4. Волонтерський характер. Велику роль відіграє «цивільна розвідка» - громадяни, які передають інформацію про рух ворога, наявність його техніки, через чат-боти (публікують та фотографують в мережах) [4].

Протидія OSINT для обох сторін під час війни є критично важливим аспектом інформаційної безпеки. Оскільки OSINT дозволяє збирати інформацію з соціальних мереж, супутникових знімків, новин та геолокаційних даних, спроби обмежити цей потік інформації несуть серйозні небезпеки для обох сторін конфлікту, а саме:

- втрата реального розуміння ситуації на полі бою;
- ризик дезінформації та маніпуляцій;
- приховування військових злочинів та неефективності;
- загроза цивільному населенню та військовослужбовцям;
- зниження доказової бази на міжнародному рівні та ін.

Отже, використання методів OSINT у російсько-українській війні дозволяють оперативнику ефективно збирати, обробляти, аналізувати та інтерпретувати відкриту інформацію, перетворюючи її на корисні розвідувальні дані, оскільки збирає первинну інформацію про потенційних ворогів, їхні зв'язки, спосіб життя та активи через аналіз соціальних мереж, публічних профілів та відкритих баз даних, що є основою для подальшої розробки та виявлення нових об'єктів.

Використання методів OSINT є важливим і необхідним елементом у кіберпросторовій когнітивній війні.

### **Список використаних джерел**

1. Пащенко Т. П. Гібридна війна та соціальні мережі. *Інформаційний вимір гібридної війни: досвід України* : матеріали Міжнародної науково-практичної конференції. Київ : НУОУ, 2017. С. 62–65.

2. Щурат Т. Г., Смук А. О. Деякі аспекти розвідки з відкритих джерел інформації (OSINT). URL: <http://dspace.oduvs.edu.ua/bitstream/123456789/654/1/6.pdf> (дата звернення: 21.05.2022).

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

4. Курс «OSINT – розвідка з відкритих джерел та інформаційна безпека» на платформі Prometheus. URL: <https://prometheus.org.ua/Prometheus-free/osint-open-source-intelligence/>.

**Ярема О. Г.,**

т. в. о. завідувача кафедри  
адміністративно-правових дисциплін,  
кандидат юридичних наук, доцент

*(Львівський державний університет внутрішніх справ)*

**Єсімов С. С.,**

професор кафедри адміністративно-правових дисциплін,  
кандидат юридичних наук, професор

*(Львівський державний університет внутрішніх справ)*

## **ПИТАННЯ ВНЕСЕННЯ У НАВЧАЛЬНИЙ ПРОЦЕС ЗА СПЕЦІАЛЬНІСТЮ К9 «ПРАВООХОРОННА ДІЯЛЬНІСТЬ» ТЕХНОЛОГІЙ OSINT**

Підготовка фахівців у сфері охорони прав, свобод і законних інтересів фізичних і юридичних осіб у закладах вищої освіти передбачена за спеціальністю К9 (262) «Правоохоронна діяльність». З упевненістю можемо констатувати, що у програму підготовки фахівців за даною спеціальністю приділяє більше уваги теорії, ніж практиці. У юридичних вишах значення надається більше академічним досягненням, ніж практичним. Це не відповідає реаліям сьогодення та досвіду організації діяльності правоохоронних органів країн Європейського Союзу, оскільки практичний працівник – слідчий, оперативний уповноважений, дільничний офіцер поліції, поліцейський офіцер громади, з величезним досвідом роботи, або поліцейський, який більшу частину життя реалізує службові повноваження заслуговує на повагу не менше, ніж люди, які здобули вищу юридичну освіту, захистили дисертації, написали підручники, жодного дня не брали участь у розкритті та превенції кримінальних і адміністративних правопорушень.

Хороший правоохоронець повинен уміти знайти інформацію, необхідну для виконання повноважень, дати консультацію, мати навички оперативної роботи, знати організацію та провадження експертиз, скласти договір, захищати права громадян усіма законними способами, брати участь у кримінальному та адміністративному судочинстві.

У зв'язку з цією проблемою доцільно подовження терміну навчання за освітньою програмою бакалаврату за спеціальність К9 «Правоохоронна діяльність» до 4 років (включно). При цьому терміні навчання можливе якісне освоєння всіх галузей права та застосування інформаційних технологій у правоохоронній діяльності.

Спеціалізація здобувачів вищої освіти за окремими напрямками (профілями) має реалізовуватися в магістратурі. Випускник бакалаврату, якісно та повно освоївши галузі застосування інформаційних технологій у сфері права, зможе обрати конкретну спеціалізацію (профіль) для поглибленого практичного та теоретичного вивчення певної групи галузей права необхідних для виконання функцій у визначених напрямках правоохоронної діяльності, у тому числі з врахуванням упровадження в перспективі спеціальності «приватний детектив».

В магістратурі, термін навчання доцільно збільшити до 2 років, здобувач повинен вивчати виключно спеціалізовані курси, заглиблюватися в теорії, шукати місце і роль значення принципів, предмета і методу галузі права,, можливості застосування інформаційних технологій у процес професійної діяльності.

Упровадження інформаційно-комунікаційних технологій у правоохоронну діяльність вимагає освоєння технологій отримання інформації за допомогою Open Source Intelligence (OSINT). Дорожньою картою з питань верховенства права у контексті переговорного процесу про вступ України до Європейського Союзу за кластером 1 «Основи процесу вступу до ЄС» та планом заходів, спрямованих на виконання Комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 роки передбачено впровадження інформаційних технологій у правоохоронну діяльність [1].

Термін OSINT (Open Source Intelligence) позначає діяльність із збору, обробці і аналізу інформації, отриманої із загальнодоступних (відкритих) джерел, з метою її подальшого використання для вирішення прикладних завдань у сфері безпеки, управління та превенції кримінальних і адміністративних правопорушень.

Ефективність використання сервісів для здійснення OSINT залежить від володіння інструментарієм, що дозволяє автоматизувати збирання, обробку і аналіз інформації з відкритих джерел. У наукових публікаціях виділяють програмні засоби, вивчення яких доцільно включити у процес підготовки фахівців правоохоронної діяльності із питань OSINT:

- пошук за ім'ям користувача. Sherlock і Snoor програми з відкритим вихідним кодом, що автоматизують пошук акаунтів на ім'я користувача на сотнях онлайн-платформ;
- пошук за електронною поштою. Аналіз email-адреси дозволяє перевірити факт участі у витоках баз даних. Eriéos і Holehe надають можливість перевірки електронної пошти щодо реєстрації в різних онлайн-сервісах;
- пошук за номером мобільного телефону дозволяє визначити оператора зв'язку, регіон реєстрації, виявити акаунти в месенджерах (WhatsApp, Telegram, Viber) та соціальних мережах;
- пошук за зображенням дозволяє встановити джерело фотографії, ідентифікувати відбиті об'єкти та особи, виявити факти використання підроблених або згенерованих зображень;
- комплексний аналіз зв'язків, що сприяє у процесі вивчення Maltego формуванню системного мислення, навичок структурування великих обсягів інформації та виявлення прихованих закономірностей;
- технологій розпізнавання осіб, що ґрунтуються на методах машинного навчання.

У Європейському Союзі використовується модель формування компетенцій у галузі OSINT залежно від складності розв'язуваних завдань та необхідного рівня підготовки відповідно до професійного стандарту.

Початковий рівень (5-й рівень НПК). Бакалаврат. Вивчаються основи пошуку даних у відкритих джерелах OSINT та місце в інформаційній безпеці; розширені методи пошуку із використанням операторів; робота з метаданими зображень і документів; базові методи збирання інформації із соціальних мереж; використання простих OSINT-інструментів; етичні та правові основи роботи з відкритими даними, первинний аналіз інформації, дотримання стандартів етики та конфіденційності, базове використання ШІ-інструментів для пошуку.

Метою є оволодіння базовими методами збору і аналізу інформації з відкритих джерел, достатніми для перевірки даних і отримання інформації.

Середній рівень (6-й рівень НПК). Бакалаврат. Поглиблені навички використання розшукових методів, збору доказів, аналізу інформації, цифрового форензика, використання технічних засобів (фото- та відеоапаратура, GPSтрекери), навички планування та координації роботи, взаємодія з клієнтами й правоохоронними органами, етичне застосування ШІ. Програма включає: поглиблені методи геолокації та хронологічного аналізу; роботу із спеціалізованими аналітичними платформами (Maltego, SpiderFoot); аналіз соціальних мереж

і створення дискретних акаунтів для операційної безпеки; методи перевірки достовірності та верифікації інформації; документування результатів і підготовку аналітичних звітів.

Метою є формування навичок системного аналізу, побудови графів зв'язків та підготовки аналітичних матеріалів для підтримки прийняття рішень.

Експертний рівень (7-й рівень НРК). Магістратура. Проведення складних розслідувань із збором та фіксацією доказів, експертний аналіз цифрових даних із використанням блокчейн та штучного інтелекту (далі – ШІ), вміння будувати системи безпеки на підприємствах, установах, організація (включаючи ШІ-упередження).

Ефективне формування компетенцій щодо OSINT неможливе без широкого використання практико-орієнтованих форм навчання, що дозволяють застосовувати отримані знання за умов, максимально наближених до реальної професійної діяльності.

Практичні заняття є основною формою навчання на базовому (бакалаврат) та поглибленому (магістратура) рівнях. У ході практичних занять здобувачі під керівництвом викладача освоюють роботу з конкретними інструментами та сервісами, виконують типові завдання зі збирання та аналізу інформації.

Технології розвідки за відкритими джерелами OSINT перестають бути допоміжним інструментом і стають невід'ємним компонентом професійної діяльності фахівця в галузі правоохоронної діяльності, з навиками забезпечення інформаційної безпеки, а їхнє вивчення при підготовці фахівців стає необхідною умовою формування професіонала у цій галузі.

Доцільно внести доповнення у наказ Міністерства освіти і науки України від 22.10.2020 року № 1294 «Про затвердження стандарту вищої освіти за спеціальністю 262 «Правоохоронна діяльність» (в редакції 2024 року) [2] з погляду на Постанову Кабінету Міністрів України від 30 серпня 2024 року № 1021 «Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти» [3] (К 9 «Правоохоронна діяльність») положення щодо включення вивчення діяльності зі збирання, обробки і аналізу інформації, отриманої із загальнодоступних (відкритих) джерел OSINT.

### **Список використаних джерел**

1. Деякі питання забезпечення переговорного процесу про вступ України до Європейського Союзу за кластером 1 «Основи процесу вступу до ЄС»: Розпорядження Кабінету Міністрів України від 14.05.2025 р. № 475-р. URL. <https://zakon.rada.gov.ua/laws/show/475-2025-%D1%80#Text>

2. Про затвердження стандарту вищої освіти за спеціальністю 262 «Правоохоронна діяльність» для другого (магістерського) рівня вищої освіти: Наказ Міністерства освіти і науки України від 22.10.2020 р. № 1294. URL. <https://mon.gov.ua/npa/pro-zatverdzhennya-standartu-vishoyi-osviti-za-specialnistyu-262-pravoohoronna-diyalnist-dlya-drugogo-magisterskogo-rivnya-vishoyi-osviti>

3. Про внесення змін до переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої та фахової передвищої освіти: Постанова Кабінету Міністрів України від 30 серпня 2024 р. № 1021. URL. <https://zakon.rada.gov.ua/laws/show/1021-2024-%D0%BF#Text>

**Ящур П. О.,**  
курсант 3 курсу ННПД  
(Національна академія внутрішніх справ)  
Науковий керівник: **Моргун Н. С.,**  
професор кафедри оперативної-розшукової  
діяльності та національної безпеки,  
кандидат юридичних наук, доцент  
(Національна академія внутрішніх справ)

**РОЛЬ ПІДРОЗДІЛІВ КІБЕРПОЛІЦІЇ ТА КРИМІНАЛЬНОГО АНАЛІЗУ  
У ВЗАЄМОДІЇ ЗІ СЛІДЧИМ ПІД ЧАС ДОСУДОВОГО РОЗСЛІДУВАННЯ  
КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ПОВ'ЯЗАНИХ  
ІЗ НЕЗАКОННИМ РУХОМ ФІНАНСОВИХ РЕСУРСІВ**

Рух фінансових ресурсів у цифровому середовищі давно став однією з найбільш чутливих сфер для кримінально протиправного впливу. Електронні платежі, дистанційні сервіси, рахунки підконтрольних осіб, криптовалюти гаманці, платіжні посилання та фіктивні онлайн-платформи, які маскуються під законні сервіси, дедалі частіше використовуються для незаконного отримання коштів, їх приховування, перерозподілу та подальшої леглізації. Через це під час досудового розслідування слідство стикається не з одним переказом чи окремим рахунком, а з послідовністю дій, у якій поєднуються цифрові сліди, фінансові операції, контакт між учасниками та спроби швидко розосередити кошти [1]. Саме тому у таких провадженнях вирішальне значення має реальна взаємодія слідчого з підрозділами кіберполіції та підрозділами кримінального аналізу, що має вирішальне значення під час досудового розслідування цієї категорії проваджень.

Масштаб цього питання добре видно зі статистики. За даними Національного банку України у 2025 році кількість операцій із використанням платіжних карток перевищила 9,5 млрд, а їх загальна сума становила понад 7 трлн грн. Понад 95 відсотків таких операцій здійснювалися у безготівковій формі, значна частина – у мережі Інтернет. Оплата товарів і послуг онлайн становила понад 1,2 млрд операцій на майже 770 млрд грн, а перекази між картками перевищили 1,2 трлн грн. Водночас, у 2024 році сума збитків від незаконних дій та шахрайських операцій з використанням платіжних карток досягла 1,1 млрд грн, причому 83 відсотки таких випадків сталися саме в Інтернеті. На цьому тлі й дані кіберполіції виглядають показово: у 2025 році зареєстровано понад 2,1 тис. кримінальних правопорушень, повідомлено про підозру близько 1,5 тис. особам, до суду скеровано понад 2,7 тис. кримінальних правопорушень, а потерпілим відшкодовано понад 342,6 млн грн, що становить 70,9 відсотка від завданих збитків. Okремо зазначено, що у 2025 році до суду скеровано 58 обвинувальних актів щодо організованих груп і злочинних організацій, виявлених працівниками кіберполіції, тоді як у 2024 році таких актів було 57 [2,3]. Ці дані показують, що цифровий простір став звичним середовищем фінансової активності, а тому незаконний рух коштів легко розчиняється в масиві законних операцій.

Підрозділи кіберполіції у таких провадженнях, насамперед, працюють із цифровими слідами, які швидко зникають або змінюються. Йдеться про фішингові сторінки, платіжні

форми, акаунти, IP-адреси, логіни, криптовалютні гаманці, електронну пошту, серверні дані, телеграм-канали, рекламні оголошення та історію входів до облікових записів. Саме за письмовим дорученням слідчого підрозділи кіберполіції опрацьовують запити до банків, платіжних сервісів та інших учасників цифрового ринку, встановлюють рахунки співучасників, послідовність руху коштів, переміщення криптовалюти, акаунти користувачів криптобірж та інші технічні відомості, без яких неможливо вийти за межі одного епізоду. У провадженнях, де незаконний рух коштів відбувається через дистанційні сервіси, саме кіберполіція допомагає перейти від факту списання чи переказу до встановлення способу дії, повторюваних технічних ознак і осіб, які забезпечували функціонування цифрової частини схеми. Якщо одна й та сама адреса гаманця, вебресурс, платіжна форма чи шаблон комунікації повторюються в різних епізодах, для слідства це вже ознака системної діяльності, а не випадковий збіг [3].

Підрозділи кримінального аналізу в такому провадженні систематизують великий масив відомостей і перетворюють їх на зрозумілу аналітичну картину. Йдеться не лише про зіставлення банківських операцій, телефонних контактів, технічних ідентифікаторів, часових збігів та географії переказів, а й про підготовку аналітичних звітів, схем зв'язків, інформаційних дос'є щодо фігурантів, аналіз переміщення виконавців і відомостей про їх імовірне місцезнаходження. Саме підрозділи кримінального аналізу допомагають звести окремі контакти, рахунки, акаунти, маршрути і транзакції в єдину систему, де стає зрозуміло, хто виконує технічну роль, хто приймає кошти, хто забезпечує зв'язок між учасниками, а хто фактично керує всією послідовністю незаконних операцій [4, с. 41-43].

Практична проблематика цього питання пов'язана з тим, що на початковому етапі слідчий часто бачить лише один рахунок, одну банківську виписку або один епізод списання коштів, найчастіше надану самим потерпілим. Без кіберполіції та підрозділів кримінального аналізу цього недостатньо для повноцінного досудового розслідування, бо за межами провадження залишаються пов'язані рахунки, цифрова інфраструктура, рух криптовалюти, акаунти користувачів бірж, коло виконавців та їх зв'язки між собою. Саме тому доцільно вдосконалювати забезпечення таких підрозділів різноманітними базами даних, розширювати доступ до аналітичних систем, посилювати обмін інформацією між слідчим, кіберполіцією та підрозділами кримінального аналізу й максимально рано включати їх у провадження [4, с. 43-46]. Такий підхід дає змогу швидше встановлювати фактичні дані про особу, її контакти, маршрути переміщення, пов'язані фінансові операції та загальну послідовність дій.

Отже, роль підрозділів кіберполіції та кримінального аналізу під час досудового розслідування кримінальних правопорушень, пов'язаних із незаконним рухом фінансових ресурсів, полягає в тому, що вони дозволяють перевести провадження з рівня окремої операції або одного епізоду на рівень повної схеми, де видно шлях руху коштів, коло причетних осіб і спосіб приховування незаконних дій. Такий підхід дає змогу не обмежуватися окремими фактами, а послідовно встановлювати всі елементи правопорушення, пов'язані між собою фінансовими та цифровими зв'язками. У результаті досудове розслідування стає більш цілісним і спрямованим на встановлення реальної картини події, що створює підстави для притягнення винних осіб до кримінальної відповідальності.

### Список використаних джерел

1. Безготівкові розрахунки у 2024 році суттєво переважали серед операцій з платіжними картками. Національний банк України. 03.03.2025. URL: <https://bank.gov.ua/ua/news/all/bezgotivkovi-rozrahunki-u-2024-rotsi-suttyevo-perevajali-sered-operatsiy-z-platijnimi-kartkami> (дата звернення: 24.03.2026).

2. Кількість випадків шахрайства з картками знизилася, сума збитків за ними зросла на 37 % у 2024 році. Національний банк України. 12.05.2025. URL: <https://bank.gov.ua/ua/news/all/kilkist-vipadkiv-shahraystva-z-kartkami-znizilasya-zbitki-za-nimi--zrosli> (дата звернення: 24.03.2026).

3. Щорічний звіт. Департамент кіберполіції Національної поліції України. 16.02.2026. URL: <https://cyberpolice.gov.ua/news/shhorichnyj-zvit-7096/> (дата звернення: 24.03.2026).

4. Живко З. Б., Рудий Т. В., Сенік В. В. Технології кримінального аналізу у практиці протидії кіберзлочинності. *Соціально-правові студії*. 2018. Вип. 2. С. 40–47. URL: <https://dspace.lvduvs.edu.ua/bitstream/1234567890/2323/1/2-1018-07.pdf> (дата звернення: 24.03.2026).

РОЛЬ OSINT-ДОСЛІДЖЕНЬ  
У ПІДВИЩЕННІ РІВНЯ  
НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

*Матеріали Всеукраїнської  
науково-практичної конференції*

*7 травня 2026 року*

Укладачі:

*Пацула Ольга,*

*кандидат економічних наук, доцент*

*Ірина Ревак,*

*доктор економічних наук, професор*

Макетування

*Марта Левкович*

---

Формат 60×84/8. Умовн.-друк. арк. 28,4.

Зам. 38-26.

Львівський державний університет внутрішніх справ  
вул. Городоцька, 26, Львів, 79007, Україна

Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру  
видавців, виготівників і розповсюджувачів видавничої продукції  
ДК № 2541 від 26 червня 2006 р.