Міністерство освіти і науки України
Національний університет «Острозька академія»
Навчально-науковий центр заочно-дистанційного навчання
Кафедра національної безпеки та політології

Кваліфікаційна робота
на здобуття освітнього ступеня магістра
на тему: «**OSINT-аналітика як інструмент посилення воєнної безпеки України**»

Виконав студент ІІ курсу, групи ЗМНБ -2
спеціальності 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)»
Риженков Станіслав Олегович

Науковий керівник - кандидат наук з державного управління, доцент
Бондар Віталій Дмитрович

Рецензент - кандидат наук з державного управління, доцент
Шершньова Олена Володимирівна

Острог, 2026

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Повномасштабна російсько-українська війна радикально змінила характер безпекового середовища України та підтвердила, що сучасне воєнне протиборство відбувається не лише у фізичному просторі ведення бойових дій, а й у цифровому, інформаційному, кібернетичному, комунікаційному та аналітичному вимірах. За цих умов здатність держави швидко отримувати, перевіряти, систематизувати та інтерпретувати інформацію стає одним із важливих чинників забезпечення воєнної безпеки. Для України це має особливе значення, оскільки російська агресія поєднує класичне застосування військової сили з інформаційними операціями, дезінформацією, кібератаками, психологічним тиском, маніпуляцією відкритими джерелами та спробами впливу на міжнародне сприйняття війни.

У правовому полі України воєнна безпека пов’язується із захищеністю державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших життєво важливих національних інтересів від воєнних загроз [107]. У науковій літературі воєнна безпека також розглядається як складова національної безпеки, яка охоплює не лише власне оборонну діяльність, а й політичні, інформаційні, соціальні, економічні, правові та інституційні аспекти захисту держави[19, с. 367-368]. Саме тому дослідження інструментів, здатних посилювати ситуаційну обізнаність, підтримувати ухвалення рішень і забезпечувати більш якісну оцінку воєнних загроз, є актуальним як у науковому, так і в практичному вимірі.

Особливої ваги в цьому контексті набуває OSINT-аналітика, тобто робота з відкритими, доступними або комерційно доступними джерелами інформації, яка передбачає не лише пошук даних, а їхню перевірку, зіставлення, обробку, інтерпретацію та перетворення на аналітичний продукт. На відміну від простого збирання інформації в мережі Інтернет, OSINT-аналітика передбачає наявність дослідницького запиту, методичної послідовності, критичної оцінки джерел,

тріангуляції даних та формування висновків, придатних для практичного використання. У цьому сенсі OSINT є не лише технологічним інструментом, а й окремою формою аналітичної діяльності в умовах цифрового інформаційного суспільства [40; 64].

Актуальність теми посилюється кількома взаємопов'язаними чинниками. По-перше, російсько-українська війна стала одним із найбільш задокументованих збройних конфліктів сучасності, у якому значна частина інформації про події, переміщення військ і техніки, наслідки ударів, діяльність окупаційних адміністрацій, інформаційні операції та цивільний спротив фіксується через соціальні мережі, супутникові знімки, фото- і відеоматеріали, публічні реєстри, месенджери, медіа та інші відкриті цифрові джерела [63; 80; 90]. По-друге, розвиток штучного інтелекту, великих даних, автоматизованого аналізу тексту, геопросторових сервісів і комерційних цифрових платформ значно розширює можливості OSINT, але водночас створює нові ризики, пов'язані з інформаційним перевантаженням, алгоритмічними помилками, дезінформацією, непрозорістю автоматизованих рішень і порушенням приватності [35]. По-третє, європейська та євроатлантична інтеграція України актуалізує потребу у розвитку сучасних підходів до безпекової аналітики, сумісних із практиками держав-членів НАТО та ЄС, де відкриті джерела поступово стають важливою частиною розвідувальної, оборонної й аналітичної діяльності [2; 68]. По-четверте, державна політика України у сфері національної безпеки, оборони, інформаційної стійкості та протидії гібридним загрозам потребує інструментів, які дозволяють швидко реагувати на динамічні зміни безпекового середовища.

Значення OSINT-аналітики для України полягає в тому, що вона може використовуватися для підвищення ситуаційної обізнаності, виявлення загроз, аналізу відкритої інформації про противника, перевірки фото- й відеоматеріалів, документування воєнних злочинів, моніторингу тимчасово окупованих територій, оцінки інформаційних операцій РФ, аналізу цифрових слідів, підтримки стратегічних комунікацій і доповнення традиційних видів розвідки

[23; 24; 45; 63]. Водночас її використання потребує обережності, оскільки відкрите джерело не гарантує достовірності інформації, а цифровий простір у воєнний час може бути насичений маніпулятивними повідомленнями, повторюваними інформаційними сигналами, фальшивими цифровими слідами та цілеспрямованими дезінформаційними операціями [31; 42; 47; 85].

Практичний вимір актуальності теми особливо помітний у діяльності державних, волонтерських, громадських і дослідницьких ініціатив, які використовують відкриті джерела для аналізу російсько-української війни. У цьому контексті важливими є приклади роботи Bellingcat, InformNapalm, Molfar, DeepState, Cyber Resistance, OSINT-спільнот, журналістів-розслідувачів, аналітичних центрів і волонтерських проєктів, які здійснюють верифікацію даних, геолокацію фото- й відеоматеріалів, ідентифікацію російських військових, аналіз супутникових знімків, документування наслідків атак і дослідження інформаційного середовища війни [70; 83; 89; 91; 98; 100]. Саме тому OSINT-аналітика може розглядатися як один з інструментів посилення воєнної безпеки України, але лише за умови методично організованого, відповідального та професійного застосування.

Стан наукової розробленості теми дослідження. Проблематика OSINT-аналітики у сучасній науковій літературі розглядається на перетині кількох дослідницьких напрямів: теорії розвідки, національної та воєнної безпеки, інформаційної безпеки, кібербезпеки, цифрової верифікації, аналізу соціальних мереж, міжнародних відносин і дослідження сучасних збройних конфліктів. Така міждисциплінарність є одночасно перевагою і проблемою для дослідження. З одного боку, вона дозволяє розглядати OSINT як комплексний інструмент збору, перевірки та інтерпретації відкритої інформації. З іншого боку, у науковій літературі досі немає повної єдності щодо того, чи слід розуміти OSINT як окремий вид розвідки, як метод аналітичної роботи, як технологічний інструментарій або як ширшу практику взаємодії державних і недержавних акторів у цифровому інформаційному середовищі [42; 64; 65].

Вагомий внесок у теоретичне осмислення OSINT зробили американські дослідники цифрового інформаційного середовища М. Ґлассман і М. Дж. Канґ, які пов’язують виникнення OSINT із трансформацією інформаційного середовища в епоху Інтернету [40]. Історичний розвиток OSINT досліджували фахівці з історії розвідки та відкритих джерел: нідерландський дослідник Л. Блок, американський розвідувальний теоретик Р. Стіл, дослідник відкритої розвідки Дж. Голдер-Роудс, американський фахівець з розвідувальних досліджень А. Гулнік, а також історик журналістики та відкритих джерел М. Фульхаге [29; 37; 43; 44; 59]. У їхніх працях показано, що використання відкритих джерел у розвідувальній і безпековій діяльності має довшу історію, ніж лише цифрова доба, однак саме Інтернет, соціальні мережі та цифрові платформи суттєво змінили масштаб, швидкість і доступність такої інформації.

Сучасні підходи до визначення OSINT і його ролі в міжнародній безпеці розробляють дослідники розвідки та міжнародної безпеки Д. Ван Пуйвелде і Ф. Табарес Рієнзі, фахівці з безпекової аналітики С. Култхарт і Б. Нуссбаум, дослідники оборонного середовища Г. Вільямс та І. Блум, а також польська дослідниця військової розвідки А. Зьолковська [32; 64; 65; 66]. У їхніх працях OSINT розглядається як елемент сучасної розвідувальної архітектури, проте водночас підкреслюється, що відкриті джерела стають аналітично значущими лише після професійної обробки, перевірки та включення в процес ухвалення рішень.

Критичний підхід до OSINT представлений у працях дослідників розвідувальної діяльності та інформаційної безпеки Дж. М. Гетфілда, Г. Хрібара, І. Подбрегара, Т. Івануші, А. Гулніка, а також фахівців із міжнародної безпеки Т. Коллі та Г. Ділана [30; 31; 42; 44]. Ці автори звертають увагу на ризики інформаційного шуму, етичні та правові обмеження, складність верифікації, можливість маніпуляції відкритими джерелами та обмеженість уявлення про OSINT як універсальний засіб подолання “туману війни”. Їхні підходи є важливими для цього дослідження, оскільки дозволяють уникнути надмірно оптимістичного трактування OSINT і розглядати його як інструмент,

ефективність якого залежить від методики, якості джерел, професійної підготовки аналітиків і контексту застосування.

Окремий напрям досліджень присвячений технологічному виміру OSINT. Британські дослідники безпеки та великих даних К. Елдрідж, К. Гоббс і М. Моран аналізують поєднання алгоритмів і людської аналітики в умовах великих даних [35]. Фахівці з кібербезпеки А. Ядав, А. Кумар і В. Сінґх розглядають OSINT у сфері виявлення кіберзагроз, цифрової криміналістики та моніторингу атак. Аналітики Центру дослідження нових безпекових технологій Ч. Вінтер, Дж. Галлачер і А. Гарріс досліджують взаємозв'язок штучного інтелекту, OSINT і російського інформаційного середовища [104]. У цих працях і звітах обґрунтовується, що сучасна OSINT-аналітика потребує поєднання технологічних інструментів із людською експертизою, оскільки алгоритми здатні пришвидшувати обробку великих масивів інформації, але не замінюють критичного мислення, контекстного аналізу та професійної інтерпретації.

Особливе значення для цього дослідження мають праці, присвячені використанню OSINT у російсько-українській війні. Дослідники воєнних студій Г. Ван Бік і С. Ріт'єнс аналізують роль відкритих джерел у висвітленні та розумінні війни в Україні, зокрема зміну ролі недержавних акторів, журналістів-розслідувачів, волонтерів та OSINT-спільнот [63]. Дослідники міжнародної безпеки О. Крпец, М. Чованчик та А. Ілавська розглядають можливості й обмеження OSINT на стратегічному рівні в умовах невизначеності війни [47]. Британські аналітики і журналісти-розслідувачі, зокрема автори Bellingcat та інших дослідницьких платформ, розкривають значення відкритих джерел для геолокації, верифікації фото- і відеоматеріалів, аналізу супутникових знімків і встановлення фактів у контексті російсько-української війни [80; 83; 89; 90; 91].

Українська наукова література також поступово розширює дослідження OSINT. Українські дослідники військово-спеціальних наук Я. М. Жарков і А. О. Васильєв розглядали питання визначення суті розвідки з відкритих джерел [9]. Українські правники Н. В. Жмур і М. П. Землянікіна досліджували історію становлення та сучасний стан технології OSINT [10]. Дослідники у сфері

інформаційних технологій і прикладного аналізу Б. В. Ліцук і В. В. Стрелков аналізували галузі застосування розвідки відкритих джерел даних [15]. Українські науковці у сфері права та правоохоронної діяльності М. О. Думчиков, Р. І. Радейко, С. А. Басалик, О. С. Туз, В. В. Тищук розглядали використання OSINT-технологій у правоохоронній, юридичній та антикорупційній діяльності [4; 8; 20]. Їхні праці важливі для розуміння того, що OSINT в українському науковому полі розглядається не лише як інструмент розвідки, а й як метод роботи з інформацією в різних сферах публічної безпеки, права та державного управління.

Питання воєнної безпеки України як складової національної безпеки досліджували українські науковці В.О. Іваха, М.В. Ковалів, Р. П. Лаврьонов, О. Пархоменко-Куцевіл, Р. М. Скриньковський та інші автори [11; 12; 14; 19; 21]. У їхніх працях розкриваються теоретичні засади воєнної безпеки, її зв’язок із національною безпекою, обороноздатністю, стійкістю держави, захистом суверенітету і територіальної цілісності, а також протидією воєнним загрозам. Для цього дослідження ці праці мають значення як теоретична основа для розмежування понять “воєнна безпека”, “військова безпека”, “оборонна безпека” та “національна безпека”.

Попри наявність значної кількості праць, тема OSINT-аналітики як інструменту саме посилення воєнної безпеки України залишається частково розробленою. У науковій літературі достатньо активно досліджуються окремі аспекти OSINT: його історія, поняття, джерела, інструменти, застосування в кібербезпеці, розвідці, журналістиці та документуванні воєнних злочинів. Водночас бракує цілісного дослідження, у якому OSINT-аналітика розглядалася б як комплексний інструмент посилення воєнної безпеки України з урахуванням теоретико-методологічних засад, організаційної послідовності, практичних кейсів російсько-української війни, можливостей штучного інтелекту, обмежень комерційних інструментів і перспектив їх інтеграції в безпекову систему держави.

Мета дослідження полягає в розробленні теоретико-методологічного обґрунтування OSINT-аналітики як інструменту посилення воєнної безпеки України та визначенні напрямів її застосування в умовах російсько-української війни для підвищення ситуаційної обізнаності, виявлення загроз, перевірки інформації, документування дій противника та підтримки ухвалення безпекових рішень.

Для досягнення мети поставлено такі завдання дослідження:

- визначити генезу становлення OSINT-аналітики в системі розвідувальної та безпекової діяльності;
- узагальнити наукові й інституційні підходи до визначення OSINT і OSINT-аналітики та уточнити авторське розуміння цього поняття;
- з’ясувати методологічні проблеми дослідження й реалізації OSINT-аналітики в умовах цифровізації безпекового середовища;
- обґрунтувати зв’язок OSINT-аналітики з посиленням воєнної безпеки України та визначити організаційну й методичну послідовність її проведення ;
- проаналізувати практичні кейси застосування OSINT-аналітики в умовах російсько-української війни, зокрема діяльність державних, волонтерських, громадських і дослідницьких ініціатив;
- оцінити можливості, обмеження й перспективи використання комерційних OSINT-інструментів, лексичного, мережевого та геопросторового аналізу у сфері воєнної безпеки України.

Об’єктом дослідження є OSINT-аналітика як явище сучасної безпекової та розвідувально-аналітичної діяльності.

Предметом дослідження є теоретико-методологічні засади, організаційні підходи, інструменти та практичні напрями використання OSINT-аналітики для посилення воєнної безпеки України в умовах російсько-української війни.

Методологічну основу дослідження становить поєднання загальнонаукових і спеціальних методів. Історико-генетичний метод

використано для з’ясування еволюції OSINT-аналітики та переходу від доцифрових форм роботи з відкритими джерелами до сучасної цифрової OSINT-практики. Метод аналізу й синтезу застосовано для опрацювання наукової літератури, інституційних визначень, аналітичних звітів і практичних кейсів. Порівняльний метод використано для зіставлення різних підходів до визначення OSINT, OSINT-аналітики, відкритих джерел, доступної інформації та комерційно доступних даних. Поетапний підхід дав змогу розглядати OSINT-аналітику не як набір окремих інструментів, а як елемент ширшої системи забезпечення воєнної безпеки України. Інституційний підхід застосовано для аналізу організаційних моделей інтеграції OSINT у діяльність державних структур, військових інституцій, аналітичних центрів, волонтерських і громадських ініціатив.

У роботі також використано метод контент-аналізу для дослідження відкритих повідомлень, публікацій, медіаматеріалів, соціальних мереж і цифрового контенту, пов’язаного з російсько-українською війною. Метод кейс-стаді застосовано для аналізу практичного використання OSINT-аналітики на прикладах Bellingcat, InformNapalm, Molfar, DeepState, Cyber Resistance, OSINT-спільнот, волонтерських і громадських ініціатив, а також цифрового моніторингу тимчасово окупованих територій. Метод тріангуляції використано для обґрунтування необхідності перевірки інформації шляхом зіставлення різних типів джерел: фото- і відеоматеріалів, супутникових знімків, геолокаційних даних, повідомлень у соціальних мережах, публічних реєстрів і повідомлень ЗМІ. Елементи геопросторового, мережевого та лексичного аналізу використано для оцінки інструментального потенціалу OSINT-аналітики. Прогностичний метод застосовано для визначення перспектив розвитку комерційних OSINT-інструментів і штучного інтелекту у сфері воєнної безпеки України.

Хронологічні межі дослідження охоплюють період від становлення сучасного поняття OSINT у другій половині XX століття до сучасного етапу російсько-української війни. Основна увага приділяється періоду після 2014 року, коли внаслідок російської агресії проти України відкриті джерела набули

особливого значення для моніторингу воєнних, інформаційних і безпекових процесів, а також періоду після 24 лютого 2022 року, коли повномасштабне вторгнення РФ суттєво розширило практичну роль OSINT-аналітики. Географічні межі дослідження зосереджені насамперед на Україні, включаючи тимчасово окуповані території, а також на міжнародному середовищі, у якому функціонують OSINT-спільноти, аналітичні центри, державні структури та волонтерські проєкти, що працюють із даними про російсько-українську війну.

Наукова новизна дослідження полягає в уточненні теоретико-методичного розуміння OSINT-аналітики як інструменту посилення воєнної безпеки України. У роботі обґрунтовано, що OSINT-аналітика не зводиться до пошуку інформації у відкритих джерелах, а становить методично організований процес збору, перевірки, зіставлення, аналізу та інтерпретації відкритої, доступної або комерційно доступної інформації для підготовки аналітичного продукту, придатного для підтримки рішень у сфері воєнної безпеки. Уточнено зв’язок між OSINT-аналітикою та воєнною безпекою України, який полягає у підвищенні ситуаційної обізнаності, виявленні загроз, документуванні дій противника, протидії дезінформації, аналізі окупованих територій, підтримці стратегічних комунікацій та доповненні традиційних видів розвідки. Удосконалено підхід до класифікації практичних напрямів використання OSINT-аналітики у сфері воєнної безпеки через виокремлення організаційного, тактичного, локального, інструментального та технологічного рівнів її застосування. Набули подальшого розвитку положення щодо ролі комерційних OSINT-інструментів, штучного інтелекту, лексичного, мережевого та геопросторового аналізу в умовах сучасної війни.

Практичне значення одержаних результатів полягає в тому, що висновки й положення дослідження можуть бути використані в діяльності органів державної влади, структур сектору безпеки і оборони, аналітичних підрозділів, дослідницьких центрів, волонтерських ініціатив і громадських організацій, які працюють із відкритими джерелами інформації в умовах війни. Матеріали роботи можуть бути корисними для підготовки навчальних курсів із

національної безпеки, воєнної безпеки, інформаційної безпеки, OSINT-аналітики, цифрової верифікації та протидії дезінформації. Окремі положення можуть бути застосовані під час розроблення методичних рекомендацій щодо перевірки відкритої інформації, організації OSINT-досліджень, роботи з комерційними інструментами та оцінки ризиків поширення чутливої інформації у цифровому середовищі.

Структура роботи. Кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та літератури і додатків. У першому розділі розкрито теоретико-методологічні засади дослідження OSINT-аналітики, проаналізовано її генезу, наукові та інституційні підходи до визначення OSINT і OSINT-аналітики, а також методологічні проблеми дослідження цього явища в умовах цифровізації безпекового середовища. У другому розділі досліджено OSINT-аналітику як інструмент посилення воєнної безпеки України, визначено організаційну та методичну послідовність її проведення, проаналізовано переваги, можливості штучного інтелекту, а також тактичний і локальний рівні застосування OSINT-аналітики в умовах російсько-української війни. У третьому розділі розглянуто інструменти OSINT-аналітики у сфері воєнної безпеки, проблеми використання комерційних OSINT-інструментів, можливості лексичного, мережевого й геопросторового аналізу, а також перспективи інтеграції комерційних інструментів у систему посилення воєнної безпеки України.

РОЗДІЛ І
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ АСПЕКТИ ДОСЛІДЖЕННЯ OSINT-АНАЛІТИКИ

У цьому розділі розглянуто теоретичну основу дослідження OSINT-аналітики. Перший підрозділ присвячено генезі OSINT-аналітики в системі розвідувальної та безпекової діяльності. У ньому показано, що робота з відкритими джерелами має довшу історію, ніж цифрова епоха, однак саме розвиток Інтернету, соціальних мереж, відкритих реєстрів, супутникових сервісів і великих масивів даних радикально змінив масштаби та значення цього напряму. У другому підрозділі проаналізовано наукові й інституційні підходи до визначення OSINT та OSINT-аналітики. Особлива увага приділяється тому, що OSINT не зводиться лише до відкритих джерел як таких. Відкрита інформація набуває аналітичної цінності лише тоді, коли вона зібрана за певною логікою, перевірена, зіставлена з іншими даними та інтерпретована відповідно до конкретної дослідницької або безпекової потреби. У третьому підрозділі розглянуто методологічні проблеми дослідження OSINT-аналітики в умовах цифровізації безпекового середовища. Йдеться про достовірність джерел, інформаційний шум, дезінформацію, тріангуляцію даних, межі використання відкритої та комерційно доступної інформації, а також про складність інтеграції OSINT-аналітики в практику ухвалення безпекових рішень.

1.1. Генеза становлення OSINT-аналітики в системі розвідувальної та безпекової діяльності

Інтенсивний прогрес в сфері інформаційних технологій, який полягав в появі Інтернету, соціальних мереж та інших пов’язаних з ними феноменів, привів до трансформації усіх вимірів життя людей. Змінились як способи поширення інформації, так і методи її збору та аналізу. Інформаційна революція, що триває з середини XX століття, але особливо інтенсивною стала з 1990-х років, призвела

до вибуху цифрової доступності знань. Web 2.0 значно розширив можливості отримання та обміну величезними обсягами інформації одним натисканням кнопки.

Оскільки все більша кількість інформації стала доступною з відкритих джерел, то поступово все більша кількість зацікавлених осіб стала намагатись використовувати ці можливості. Українські дослідники, Ліцук Б.В. та Стрелков В.В. наводять широкий перелік організацій, що можуть використовувати розвідку з використанням відкритих джерел даних (з англ. - Open Source Intelligence, далі - OSINT): уряд, комерційні структури, наукові установи, ЗМІ та інші [15, с. 136].

Якщо спочатку ці технології використовувались переважно державними структурами, то протягом останніх років OSINT дійсно все частіше почав використовуватись різноманітними організаціями приватного сектору, оскільки він може допомогти в конкуренції, в запуску нової продукції, отриманні нових ринків. За його допомогою можна отримати якусь важливу інформацію про конкурентів, партнерів, клієнтів, ринки; він може допомогти виміряти рівень лояльності клієнтів, відстежити коливання громадської думки та оцінку споживачами продукції. Розширились і коло державних структур, що використовують ці технології, наприклад правоохоронні органи почали використовувати ці методи для удосконалення своїх слідчих дій та покращення своєї здатності виявляти кримінальні загрози та реагувати на них. Проте OSINT почав також використовуватись і для зловмисних цілей, таких як шпигунство, крадіжка даних тощо. З огляду на все перелічене, дослідження теми OSINT почало викликати велику зацікавленість у вчених, які працюють у різних галузях: безпековій, політичній, соціологічній, психологічній та ін., і з’явилось чимало праць присвячених вивченню OSINT як явища, його значення та технологій його застосування. Проте не зважаючи на велику кількість досліджень цієї теми, продовжуються дискусії як про поняття OSINT, так і про час його виникнення.

Чимало іноземних дослідників історії розвідки та відкритих джерел, зокрема автори оглядових праць про еволюцію OSINT, вказують, що інституційна історія цієї дисципліни починається напередодні Другої світової війни зі створенням Служби моніторингу BBC у Великій Британії в 1939 році та Служби моніторингу іноземного мовлення у 1941 році у Сполучених Штатах [83; 102]. Подібної позиції дотримуються і деякі українські дослідники OSINT, зазначаючи що саме тоді США та Великобританія почали використовувати інформацію з загальнодоступних газет та радіопередач для підтримки інформації отриманої в результаті класичних розвідувальних дій. Втім інші дослідники, зокрема нідерландський фахівець з історії відкритої розвідки Л. Блок, стверджують, що OSINT має набагато довшу інституційну історію [29, с. 95] . У своїй статті «Довга історія OSINT» він, як свідчення використання цих технологій, вказує ще події Громадянської війни в Америці 1861-1865 років. Події, які він описує, свідчать, що технології OSINT починають застосовуватись, як тільки для цього з'являється відповідна матеріальна база, тобто доступна інформація, яку хтось помічає і починає використовувати. Сама ідея використання доступних джерел інформації для того, щоб передбачити поведінку, рішення суперника, не є такою вже новаторською. Саме прагнення використовувати доступні відомості для передбачення дій суперника має давню історію, однак у різні періоди змінювалися джерела, обсяг інформації та способи її систематизації. Головна заслуга - побачити ці нові джерела інформації, зрозуміти, що ж може бути в цій якості використане.

Під час Громадянської війни в Америці 1861-1865 років таким джерелом стала журналістська інформація. Це був час бурхливого розвитку преси, зростання кількості преси й журналістів підвищення й якості їх публікацій, серед в яких почало з'являтись чимало інформації, щодо стану армій, і це значно розширило можливості отримання інформації про сили суперника. Американський дослідник історії журналістики та відкритих джерел М. Фульхаге проаналізував публікації в 18 газетах, що були опубліковані між 13 і 28 грудня 1860 року, і 1423 статті з них визначив як корисні для ворожої армії,

розсортувавши їх на політичні, економічні, військові, культурні та технологічні [37, с.82-83]. Завдяки цим статтям можна було отримати інформацію про чисельність, організацію та пересування військ суперника, проблеми з виробництвом зброї та боєприпасів, забезпечення війська тощо. Підтвердженням дослідження М. Фульхаге можуть бути мемуари американського генерала часів Громадянської війни Е. Александера, що воював на стороні Південних штатів, який зазначав, що військова інформація з щоденних газет, які видавались у Північних Штатах, щодо чисельності та організації їх військ була кращою, ніж інформація від його власних агентів [25, с. 55]. Тобто газети, що видавались у Північних штатах давали більш точну інформацію про чисельність і поповнення війська, призначення командного складу, моральний дух військ ніж класичні варіанти розвідувальної діяльності. Наявність такої кількості інформації, що потребувала аналізу, в підсумку привела до створення перших спеціальних підрозділів. У 1863 році було створено Бюро військової інформації Потомакської армії, яке почало систематично шукати, опрацьовувати і використовувати інформацію з преси [37, с. 224].

Поширення друкованої преси привело до появи великої кількості публічної інформації, яку варто було досліджувати, а також до появи практик, близьких до сучасної OSINT-аналітики, та відповідних організаційних структур. У подальшому поява радіо й телебачення теж приводили до появи нових джерел інформації. Проте звісно що жодне з цих джерел не може порівнятись за обсягами інформації з Інтернетом.

Науковець М.О. Думчиков вказує, що соціальні мережі, онлайн-видання, державні реєстри, форуми та багато інших джерел стали доступними для аналізу, і це дозволило ефективно отримувати інформацію про різні аспекти діяльності осіб чи організацій [8, с.4]. Саме з настанням сучасної інформаційної ери, розвитком Інтернету та цифрової сфери для виробництва та зберігання інформації, характер та обсяг загальнодоступної інформації докорінно змінилися. Американський фахівець із досліджень розвідувальної діяльності А. Халнік наводить дані, що інформація з відкритих джерел становить близько 80%

матеріалів, доступних аналітику розвідки, який займається подіями за кордоном [44, с. 229]. Це, разом із розвитком нових технологій та методів, революціонізувало OSINT. Швидке розширення онлайн-даних з моменту появи Інтернету значно розширило можливості державних та недержавних суб'єктів по збору та аналізу доступної інформації з усе зростаючого кола питань безпеки, від зміни клімату до тероризму та розповсюдження зброї. Зростання популярності соціальних мереж та смартфонів, оснащених камерами, прискорило цю тенденцію і спричинило помноження загальнодоступних даних у геометричній прогресії. Ці технологічні зміни призвели до інтенсифікації збору та використання інформації з відкритих джерел спочатку розвідувальною спільнотою а потім і багатьма іншими суб'єктами. Після цього розвитку якраз і з'явилася підвищена увага до відкритих джерел і набуло популярності саме поняття «розвідка з відкритих джерел» та абревіатура «OSINT».

Українські дослідники також по різному бачать часові рамки виникнення та розвитку OSINT в світі, оскільки підходять до цього питання з різних методологічних позицій. До речі, у Польщі не тільки по своєму розуміють часові рамки OSINT, але й запропонували власну назву - «Біла розвідка». Що стосується українських вчених, то Український дослідник у сфері застосування OSINT-технологій М.О. Думчиков, вказує в якості початку еволюції OSINT як інструменту розвідувальної діяльності, час наприкінці 1980-х років, і вважає важливим етапом становлення цієї технології, рішення Комісії з питань ролей та можливостей розвідувального співтовариства США (яка ще має коротку назву Комісія Аспіна-Брауна (Aspin-Brown)) у 1996 році, яка офіційно визнала необхідність активного використання відкритих джерел для покращення розвідувальної діяльності [8, с. 3-4].

Українські правники Н.В. Жмур та М.П. Землянікіна вважають, що сучасну історію OSINT умовно можна розділити на декілька етапів. Перший етап, починається наприкінці 1941 р., і починається з створення у США Служби моніторингу зарубіжних трансляцій задля дослідження радіо програм. Другий етап (2005-2009 роки) відзначається виникненням центрів аналізу відкритих

джерел на фоні стрімкого зростання обсягу даних в Інтернеті, що заклало фундамент сучасних інструментів OSINT. Третій етап (2009-2016 роки) характеризується встановленням нових стандартів доступності інформації завдяки швидкому розвитку цифрових технологій, а з 2017 року почався четвертий, і відбувається активна інтеграція не лише в оборонну, але й у політичну, економічну та правоохоронну сфери за допомогою впровадження інструментів Business Intelligence, Knowledge Management та інтегрованих процесів типу JISR, що забезпечують своєчасне збирання, обробку та поширення аналітичних даних для підтримки прийняття рішень [10, с. 96].

Таблиця 1.1

Етапи становлення OSINT-аналітики

Етап	Хронологічні межі	Основна характеристика
Перший етап	кінець 1941 р. - початок 2000-х рр.	Створення у США Служби моніторингу зарубіжних трансляцій, розвиток системного моніторингу радіопрограм, друкованої преси та інших відкритих повідомлень для розвідувальних і безпекових потреб.
Другий етап	2005-2009 рр	Виникнення центрів аналізу відкритих джерел на тлі швидкого зростання обсягів інформації в мережі Інтернет. У цей період закладається основа сучасних інструментів OSINT.
Третій етап	2009-2016 рр.	Формування нових стандартів доступності інформації внаслідок розвитку цифрових технологій, онлайн-платформ, соціальних мереж і нових способів обробки відкритих даних.
Четвертий етап	з 2017 р. - дотепер	Активна інтеграція OSINT в оборонну, політичну, економічну та правоохоронну сфери, а також використання Business Intelligence, Knowledge Management та інтегрованих процесів типу JISR для підтримки прийняття рішень.

Джерело: складено автором на основі [10, с. 96].

Як бачимо і вище зазначені автори, а також українські дослідники військово-спеціальних наук Я.М. Жарков та А.О. Васильєв сходяться в тому, що «Сполучені штати Америки є першою країною, яка почала активно використовувати джерела відкритої інформації в розвідувальних цілях» [9, с. 39].

Проте, якщо провести пошук у спеціалізованих академічних журналах, то першу згадку про поняття «розвідка з відкритих джерел» і абревіатуру «OSINT» у спеціалізованій літературі з розвідки можна знайти у статті американського теоретика розвідки та колишнього офіцера Центрального розвідувального управління Р. Стіла, виданій у 1990 році в American Intelligence Journal [59]. У статті під назвою «Розвідка в 90-х роках: переосмислення національної безпеки у світі, що змінюється» визнавалось, що контекст національної безпеки та виклики, які постають перед розвідувальними службами, суттєво змінилися. У ній було сформульовано шість критичних змін, на які слід було звернути увагу, щоб розвідувальні служби змогли адаптуватися до нових умов.

У згаданій статті абревіатура OSINT згадувалась лише двічі при обговоренні адаптації розвідки до нових викликів, і її конкретне визначення не надавалось. Можна припустити, що термін уже використовувався у внутрішній професійній комунікації, оскільки Р. Стіл не запроваджував його у статті як нове поняття, не пропонував окремого визначення, а згадував про нього як про щось уже наявне в розвідувальному середовищі. Акронім OSINT також нагадує інші абревіатури, поширені в американській розвідувальній спільноті, також пов’язані з різними способами збору інформації, такими як HUMINT (HUman INTelligence) - агентурна розвідка, що добуває відомості за допомогою агентів, SIGINT (SIGnal INTelligence) - радіо- та радіотехнічна розвідка, здійснює збір інформації шляхом перехоплення сигналів, MASINT (Measurement And Signature INTelligence) - вимірювально-сигнатурна розвідка, заснована на зборі розвідданих шляхом виявлення, відстеження, ідентифікації або опису відмінних характеристик (сигнатур) фіксованих або динамічних цільових джерел та IMINT (IMagery INTelligence) - візуальна розвідка, що забезпечує отримання фотографічного зображення об’єкта[3, с. 45-47; 6, с. 135-136].

Про поширеність терміна в США вже на початку 1990-х років свідчить і те, що «Спільна доктрина розвідувальної підтримки операцій» Міністерства оборони США 1993 року вже містила поняття OSINT. У тому ж 1993 році вийшов спеціальний випуск American Intelligence Journal, присвячений розвідці з відкритих джерел. Він складався з доповідей, представлених на першій конференції з розвідки з відкритих джерел, організованій роком раніше, у 1992 році. Подібні події мають важливе значення і мають бути враховані при визначенні етапів розвитку OSINT-аналітики. Представник американської розвідувальної спільноти В. Студеман в одній із публікацій спеціального випуску American Intelligence Journal звертав увагу на поширені міфи щодо можливостей OSINT [60, с. 19-24]. В іншій публікації цього випуску американський дослідник відкритих джерел Дж. Голдер-Роудс запропонував одне з ранніх публічних визначень цього поняття. Він визначав OSINT як несекретний розвідувальний продукт, отриманий у результаті аналізу, що відображає доступ до якомога ширшого кола мультимедійних джерел [43, с. 67-71].

Технології OSINT розвивались, в першу чергу, через появу нових масивів інформації, яку робили ці технології можливими, проте ще однієї групою причин їх розвитку був запит, поява відповідної потреби. Це пояснює, наприклад, пізню появу цих технологій в Україні, хоча вони були відомі, не було мотивації до їх активного засвоєння та застосування. Вище згадуваний нідерландський дослідник історії відкритої розвідки Л. Блок запропонував дві основні умови для виникнення практик OSINT, які частково пояснюють і ситуацію в Україні. Перша умова - існування критичної маси новин та інших відкритих матеріалів, доступних громадськості. Окрім засобів масової інформації, сюди традиційно належать журнали, матеріали конференцій, аналітичні дослідження, академічні та урядові бази даних, а також архівні фотографії [61]. Друга умова - наявність конкретних інформаційних потреб щодо супротивників [29, с. 98].

Інтернет породив нові можливості OSINT які вийшли за рамки традиційних уявлень про цю діяльність, тому в цілому, генезу розвитку OSINT

можна ділити на два етапи: доцифровий і цифровий. Проте повторимо, що подієвий вимір був другою лінійкою причин. В Україні розвиток OSINT-аналітики був значною мірою зумовлений російсько-українською війною, коли її результати стали практично потрібними для державних структур, журналістів, волонтерських ініціатив, аналітичних центрів і громадянського суспільства. З'явилися конкретні інформаційні потреби: перевірка повідомлень про дії противника, встановлення місця подій, аналіз переміщення техніки, моніторинг окупованих територій, виявлення інформаційних операцій і документування наслідків війни [63; 80; 90; 105]. Російсько-українська війна породила величезний масив відкритих даних, які постійно з'являються в Інтернеті. Частина цієї інформації поширюється через соціальні мережі та месенджери, зокрема Telegram, TikTok, Facebook, YouTube та Twitter/X. Окреме значення мають сервіси, які спочатку не створювались саме для розвідки, але в умовах війни стали корисними для OSINT-аналітики, наприклад, Google Earth, Sentinel Hub, Planet Labs, Maxar, NASA FIRMS, Flightradar24, ADS-B Exchange, MarineTraffic, VesselFinder, Google Maps, OpenStreetMap та Wikimapia. Через такі платформи можна перевіряти місце події, співставляти фото й відео з мапами, відстежувати окремі переміщення, бачити теплові аномалії або уточнювати географічний контекст. Водночас сама наявність великої кількості відкритих даних ще не означає, що вони автоматично є достовірними. Тому для OSINT-аналітики важливими залишаються перевірка, зіставлення кількох джерел і обережність у висновках.

Що стосується США, країн Європи та НАТО як військово-політичного блоку, то причиною більшої уваги до технологій OSINT стала трансформація біполярного світу, розпад Радянського Союзу і Організації Варшавського договору та виникнення нового типу загроз. Інформаційні потреби стали набагато більш динамічними, технології OSINT дали можливість надавати інформацію важливу не тільки при прийнятті стратегічних рішень, але й на тактичному рівні, на полі бою. Наявність сталого суперника по біполярному протистоянню давало багато часу на агентурну роботу, час на те, щоб дати

можливість своїм агентам під прикриттям зробити кар'єру і добратись до цінних джерел, час на вербування місцевих інформаторів, навіть на формування мережі «сплячих агентів». Це було логічним, оскільки на десятиліття вперед було зрозуміло, хто буде твоїм ворогом. Проте в 1990-х роках усе почало змінюватись. В 1994 році, в рамках ЦРУ, було створено Управління програми відкритого коду спільноти (Community Open Source Program Office-COSPO). У 1996 році, згадувана українським дослідником OSINT-технологій М.О. Думчиковим, Комісія Аспіна-Брауна оприлюднила свій висновок, що розвідувальному товариству слід докласти більше зусиль для використання величезного простору інформації, доступної зараз з відкритих джерел, розвиток OSINT-аналітики набув структурного виміру [8, с. 3-4].

У західних розвідувальних служб виникли нові географічні та тематичні пріоритети, такі як Африка та Азія, у полі їх уваги з'явились різного роду недержавні суб'єкти, різноманітні політичні та релігійні терористичні угруповання, партизанські рухи тощо, замість класичних війн актуальними стали конфлікти низької інтенсивності. Зросла значимість таких проблем як розповсюдження зброї масового знищення та зростання значимості і вразливості комп'ютерних мереж, що у сумі призвело до більшого акценту на відкритих джерелах. Технології OSINT почали активно використовуватись в ході військових операцій, наприклад в ході операцій в Косово та Сербії і Герцеговині. Косово не було в зоні уваги розвідувальної спільноти країн НАТО включно до початку там операції Альянсу, тому традиційні методи не давали належного ефекту. Тож сили НАТО активно використовували OSINT, включаючи комерційні супутникові знімки та новини з відкритих джерел, для моніторингу переміщень югославських військ та перевірки цілей для бомбардувань, для моніторингу динаміки конфлікту.

Терористичні атаки 11 вересня 2001 року стали ще одним важливим моментом у розвитку OSINT. Після цих подій у США посилилося розуміння того, що традиційні розвідувальні методи не завжди дають змогу швидко реагувати на загрози, які походять не від класичних державних структур, а від

мережевих і транснаціональних організацій. Національна комісія з питань терористичних атак на Сполучені Штати, відома як Комісія 11 вересня, у 2004 році рекомендувала створити окрему структуру для роботи з відкритими джерелами. Уже наступного року було створено Open Source Center, що стало одним із показників подальшої інституціоналізації OSINT у розвідувальній системі США [1]. У цьому випадку важливо не лише те, що було створено нову структуру, а й те, чому в ній виникла потреба. У період Холодної війни головним об'єктом уваги розвідки були держави, їхні армії, політичні еліти, військово-промисловий потенціал і довгострокові стратегічні наміри. Після 2001 року все більшого значення почали набувати недержавні актори, терористичні мережі, цифрові комунікації, фінансові потоки та інформаційна активність у відкритому середовищі. Такі загрози складніше відстежувати лише класичними агентурними методами, тому відкриті джерела почали розглядатися як важливе доповнення до традиційних способів отримання інформації.

Отже, історія становлення OSINT показує, що ця практика розвивалася не тільки через появу нових технологій. Не менш важливим був запит на інформацію, який виникав у конкретних політичних, військових або безпекових умовах. Спочатку відкриті джерела використовувалися радше як допоміжний ресурс, але з часом навколо них почали формуватися окремі підходи, структури й методи аналізу. Тому OSINT варто розглядати не як випадковий наслідок появи Інтернету, а як напрям діяльності, що поступово виріс із практичної потреби працювати з великими масивами доступної інформації. Для України ця логіка є особливо помітною. Російсько-українська війна створила і значний масив відкритих цифрових даних, і гостру потребу в їхньому аналізі. Саме тому OSINT-аналітика в українському контексті має значення не лише як технологія пошуку інформації. Вона може допомагати у перевірці повідомлень, виявленні загроз, документуванні дій противника, аналізі інформаційних операцій і підтримці рішень у сфері воєнної безпеки України.

1.2. Наукові та інституційні підходи до визначення OSINT і OSINT-аналітики

Поняття OSINT потребує окремого аналізу, оскільки в науковій літературі й інституційних документах воно трактується неоднаково. В одних підходах OSINT розуміється як інформація, отримана з відкритих джерел; в інших - як розвідувальний продукт, створений після збору, перевірки й аналізу даних; ще в інших - як практична діяльність або набір методів роботи з відкритою, доступною чи комерційно доступною інформацією.

У межах цього підрозділу розглядаються визначення OSINT, запропоновані державними структурами, міжнародними організаціями та академічними дослідниками. Такий підхід дає змогу порівняти інституційне розуміння OSINT як елементу розвідувальної діяльності з ширшими науковими підходами, у яких OSINT розглядається не лише як джерело інформації, а і як процес її збору, перевірки, аналізу та поширення. Саме після цього можна перейти до поняття OSINT-аналітики як складнішого явища, що передбачає не просто отримання даних, а їхнє методичне опрацювання для підготовки аналітичного продукту. Наприклад, у публікації Міністерства оборони США «Спільна розвідувальна підтримка військових операцій» від 1996 року OSINT визначається як інформація потенційної розвідувальної цінності, доступна широкому загалу; Довідник НАТО з розвідки з відкритими джерелами від 2001 року визначає OSINT як інформацію, яка була навмисно виявлена, розділена, дистильована та поширена серед вибраної аудиторії, як правило, командира та його безпосереднього штабу, з метою вирішення конкретного питання.

Для систематизації основних підходів до визначення OSINT доцільно порівняти інституційні та наукові трактування цього поняття, оскільки вони по-різному визначають його зміст, межі та практичне призначення. Узагальнення таких підходів подано в таблицях 1.2 та 1.3.

Таблиця 1.2

Підходи до визначення OSINT в інституційних документах

Інституція	**Зміст підходу до визначення OSINT**	**Основний акцент**
Міністерство оборони США	OSINT розглядається як інформація потенційної розвідувальної цінності, доступна широкому загалу.	Доступність інформації та її можлива цінність для розвідки
Розвідувальне співтовариство США	OSINT визначається як розвідувальні дані, отримані з публічно доступної інформації, яка збирається, використовується та поширюється серед відповідної аудиторії для задоволення конкретних розвідувальних потреб.	Наявність інформаційної потреби, збір, використання і поширення даних
НАТО	OSINT пов'язується з розвідкою, отриманою з публічно доступної інформації, а також з іншої несекретної інформації, яка може мати обмежене публічне поширення або доступ.	Поєднання відкритої та несекретної інформації для потреб розвідки

Таблиця 1.3

Підходи до визначення OSINT у науковій літературі

Автор	**Зміст підходу до визначення OSINT**	**Основний акцент**
Дж. Голдер-Роудс	OSINT визначається як несекретний розвідувальний продукт, отриманий у результаті аналізу широкого кола мультимедійних джерел.	OSINT як результат аналітичної обробки інформації
С. Култхарт і Б. Нуссбаум	OSINT трактується як законно отримана публічна або комерційна інформація, яка була перевірена, проаналізована та поширена для задоволення потреб розвідки.	Законність отримання, перевірка, аналіз і потреби розвідки
Дж. М. Гетфілд	Автор наголошує, що відкриті джерела самі по собі ще не є розвідкою; розвідувального значення вони набувають лише після професійної аналітичної обробки.	Розмежування відкритої інформації та розвідувального продукту
Українські дослідники OSINT	У більшості українських підходів OSINT розглядається як діяльність з отримання розвідувальної інформації з відкритих джерел або кіберпростору.	Відкритість джерел і отримання розвідувальної інформації

Джерело: складено автором на основі [3; 9; 32; 42; 43; 68; 72]

Як видно з таблиць 1.2 та 1.3, у більшості визначень OSINT повторюються три ключові ознаки: відкритість або доступність джерел, наявність конкретної інформаційної потреби та подальша обробка зібраних даних. Водночас між підходами є помітна різниця. Інституційні документи США і НАТО переважно пов’язують OSINT із потребами розвідки, тоді як частина науковців звертає увагу на ширший процес перетворення відкритої інформації на аналітичний продукт. Саме ця відмінність є важливою для подальшого розмежування понять OSINT і OSINT-аналітики.

Після узагальнення інституційних підходів можна побачити, що американське та натівське розуміння OSINT поступово зміщується від простого акценту на відкритості інформації до акценту на її цільовому використанні. У документах американського розвідувального співтовариства OSINT розглядається як інформація, отримана з публічно доступних джерел, яка збирається, використовується і поширюється серед відповідної аудиторії для задоволення конкретних розвідувальних потреб [3]. У документах НАТО також підкреслюється, що OSINT може охоплювати не лише повністю публічну інформацію, а й іншу несекретну інформацію з обмеженим доступом або поширенням [68]. Отже, вже на інституційному рівні OSINT не зводиться до простого пошуку у відкритих джерелах, а передбачає зв’язок між джерелом, інформаційною потребою, обробкою даних і подальшим використанням результату.

Що стосується академічних дослідників, то визначення поняття OSINT залишається предметом постійних дискусій та інтерпретацій. У дослідженнях OSINT добре відомо, що саме явище є невловимим терміном, а запропоновані визначення, як правило, є широкими та неконкретними [65, с. 87]. Його можна розглядати як кінцевий продукт, тобто OSINT - це дані, що отримані з загальнодоступної інформації і збираються серед відповідної аудиторії з метою задоволення конкретної потреби, а можна як певну практику, тобто OSINT - це збір та аналіз інформації, зібраної з відкритих джерел, для отримання практичних даних.

Українські дослідники звернули увагу на OSINT порівняно пізніше, ніж західна наукова та розвідувальна спільнота. Українські дослідники військово-спеціальних наук Я. М. Жарков та А. О. Васильєв у 2013 році опублікували статтю «Наукові підходи щодо визначення суті розвідки з відкритих джерел», яка стала однією з перших спроб науково осмислити поняття OSINT в українській літературі. Аналізуючи стан розробки проблеми, автори зазначали, що у працях вітчизняних науковців термін «розвідка з відкритих джерел» у прямій інтерпретації майже не використовувався [9, с. 40]. Зараз ситуація змінилась і, наприклад, Дикий О.В. та Сидорчук В.В. виділяють чотири типи визначення поняття OSINT, що були запропоновані українськими дослідниками:

- діяльність по отриманню розвідувальної інформації з відкритих джерел кіберпростору;

- діяльність по отриманню розвідувальної інформації з відкритих джерел;

- розвідка на основі аналізу відкритих джерел інформації;

- діяльність по отриманню розвідувальної інформації з відкритих джерел кіберпростору, розвідка на основі аналізу відкритих джерел інформації [72, с. 332].

Усі ці визначення доволі однотипні, акцент зроблено на відкритості джерел і отриманні розвідувальної інформації. Проте OSINT- це інструмент, який, як ми вже вище писали, можуть використовувати дуже різні структури, від ЗМІ до правоохоронців і вимоги до результатів використання цих інструментів дуже різні. Український дослідник у сфері юридичної методології Радейко Р.І. в статті «Інструментарій OSINT у юридичній методології: теоретичні основи та практичне застосування» [20], а також українські дослідники правоохоронної діяльності Басалик С.А., Туз О.С. і Тищук В.В. в статті «Генезис інструментів OSINT та окремі аспекти їх використання у правоохоронній діяльності» [4] описують як ці інструменти використати так, щоб отримана інформація могла бути використана в судовому процесі, і її звісно не можна назвати «розвідувальною». Так само антикорупційні активісти, для яких теж написано

чимало методологічних робіт по проведенню OSINT-аналітики, не мають на меті отримання саме «розвідувальної інформації».

Ця обставина, тобто акцент на розвідці, притаманна не тільки українським дослідникам. Наприклад, фахівці з безпекової аналітики С. Култхарт і Б. Нуссбаум пропонують таке визначення OSINT: «законно отримана публічна або комерційна інформація, яка була перевірена, проаналізована та поширена для задоволення потреб розвідки» [32, с. 1]. У цьому визначенні важливою є вказівка на легальність отримання інформації, її перевірку, аналіз і подальше поширення. Саме ці ознаки дозволяють відрізнити OSINT від випадкового пошуку даних в Інтернеті або від таємних методів збору інформації.

Водночас це визначення також має певне обмеження, оскільки знову прив’язує OSINT насамперед до потреб розвідки. Як було показано вище, OSINT може використовуватися не лише розвідувальними структурами, а й журналістами, правоохоронними органами, антикорупційними активістами, дослідниками, аналітичними центрами та приватними структурами. Тому визначення С. Култхарта і Б. Нуссбаума є цінним для розуміння класичного безпекового підходу до OSINT, але воно не повністю охоплює сучасне різноманіття сфер його застосування.

Окремою проблемою є те, що в умовах війни OSINT часто працює не лише з класично відкритою інформацією, а й з даними, які вже опинилися у відкритому доступі внаслідок витоків, несанкціонованого оприлюднення або діяльності третіх осіб. Такі дані не можна автоматично прирівнювати до легітимних відкритих джерел, однак повністю ігнорувати їх у дослідженні сучасної OSINT-практики також складно. Вони створюють так звану “сіру зону” між публічно доступною інформацією, обмежено доступними даними, правовими вимогами та безпековою доцільністю. У цьому контексті важливо розрізняти саме отримання інформації і подальший аналіз уже оприлюднених даних. OSINT-аналітика не повинна ототожнюватися з незаконним доступом до інформаційних систем або здобуттям даних прихованими методами. Водночас на практиці журналісти-розслідувачі, правозахисні організації та аналітичні спільноти можуть

аналізувати вже оприлюднені масиви даних, якщо вони мають суспільне, доказове або безпекове значення. Саме тому для OSINT-аналітики принциповими є не лише технічні навички пошуку, а й оцінка правового статусу джерела, способу появи інформації у відкритому доступі та допустимості її подальшого використання.

Прикладом складності таких меж є діяльність журналістських і розслідувальних OSINT-спільнот, які працюють з відкритими цифровими слідами, реєстрами, фото- і відеоматеріалами, супутниковими знімками, архівними даними та вже оприлюдненими витоками. Їхня робота показує, що сучасний OSINT не обмежується простим пошуком у Google або переглядом соціальних мереж. Ідеться про складний процес зіставлення різних типів інформації, перевірки джерел, реконструкції подій і формування висновків, які можуть мати журналістське, правове, безпекове або міжнародно-політичне значення.

Для подальшого аналізу важливо розмежувати доступну інформацію, відкриті джерела та загальнодоступну інформацію. Одним із найбільш вдалих є визначення доступної інформації як загального терміна для позначення даних або інформації, до яких може отримати доступ широка громадськість з обмеженими технічними та економічними ресурсами і які не вимагають членства в певній організації [65].

Водночас відкрите джерело не завжди тотожне загальнодоступній інформації. Відоме визначення відкритих джерел описує їх як джерела інформації, що надають її без вимоги щодо збереження конфіденційності, тобто без спеціальних обмежень для публічного доступу [69]. Такі джерела належать до сфери відкритої інформації, однак спосіб фактичного доступу до них може бути різним. Загальнодоступна інформація - це інформація, яка вже оприлюднена або розміщена для широкого використання і не потребує додаткової дії, наприклад написання інформаційного запиту. Натомість частина відкритої інформації може бути формально доступною, але вимагати запиту, реєстрації, оплати, спеціального пошуку або технічних навичок. Саме тому для

OSINT-аналітики важливо не лише те, чи є інформація відкритою, а й те, яким способом вона отримується, які обмеження має доступ до неї та чи може вона бути використана для підготовки аналітичного продукту.

Існує широка згода, що традиційні форми медіа, такі як газети, радіопередачі, телевізійні матеріали, урядові звіти та офіційні публікації, відповідають уявленню про відкриту інформацію. Проте в цифрову епоху межі цього поняття стали менш очевидними. Поява онлайн-баз даних, соціальних мереж, комерційних платформ, супутникових сервісів, закритих або частково платних архівів створила ситуацію, у якій інформація може бути відкритою за своїм правовим статусом, але не завжди простою для фактичного доступу [64, с. 4]. Саме тому серед дослідників немає повної єдності щодо того, яку інформацію вважати загальнодоступною. Частина даних справді перебуває у вільному доступі й може бути отримана без спеціальних умов. Інша частина потребує оплати, реєстрації, технічних навичок, спеціального програмного забезпечення або вміння працювати з великими масивами даних. Наприклад, платний доступ до онлайн-газет, академічних журналів, комерційних супутникових знімків або спеціалізованих баз даних уже не повністю відповідає простому уявленню про “загальнодоступність”, хоча така інформація може залишатися несекретною і придатною для OSINT-аналізу [65, с.88]. У цьому полягає одна з методологічних проблем визначення OSINT: відкритість інформації не завжди означає її легку доступність. Відкрите джерело може вимагати додаткових дій для отримання інформації, а доступна інформація може мати різний рівень надійності, повноти й придатності для аналізу. Тому в межах цього дослідження важливо розглядати OSINT не лише як роботу з “усім, що є в Інтернеті”, а як методично організовану діяльність із відбору, перевірки та інтерпретації інформації, яка має значення для конкретної безпекової потреби.

Проблема з визначенням джерел полягає в тому, що існує небагато усталених підкатегорій для розрізнення типів інформації, а наявні визначення не завжди точно відображають зміну характеру публічної інформації в цифрову епоху. Наприклад, українські дослідниці Д. Дрижакова та Р. Волинець у доповіді

на тему «Використання відкритих джерел інформації (OSINT) у сфері безпеки держави: технології та перспективи» визначали перелік джерел OSINT, які згрупували в п’ять типів:

1) Інтернет, куди входять: веб-сайти, соціальні мережі, форуми, блоги, новинні портали, бази даних.

2) ЗМІ: телебачення, радіо, газети, журнали.

3) Державні документи: офіційні звіти, закони, постанови, реєстри.

4) Комерційні джерела: бази даних компаній, фінансова інформація, звіти про ринок.

5) Академічні джерела: наукові статті, дослідження, конференції [7].

Більш універсальним є, наприклад, поняття «сіра література». Міжвідомча робоча група уряду США з питань сірої літератури (The U.S. Government’s Interagency Gray Literature Work Group) у 1995 році визначила сіру літературу як «іноземні або вітчизняні матеріали з відкритих джерел, які зазвичай доступні через спеціалізовані канали та можуть не потрапляти до звичайних каналів або систем публікації, розповсюдження, бібліографічного контролю або придбання книгарнями чи агентами з передплати» [65, с.10]. Це визначення може включати широкий спектр типів інформації: доповіді на конференціях, корпоративні документи, дисертації, урядові звіти, інформаційні бюлетені, галузеву літературу, звіти про поїздки. Зазвичай такі матеріали публікуються дослідницькими установами, національними урядами, приватними видавництвами, корпораціями, торговими асоціаціями, спілками, аналітичними центрами та академічними колами.

Найскладнішим аспектом роботи з «сірою літературою» в минулому була її доступність. Значна частина таких матеріалів існувала поза звичайними каналами поширення, тому знайти їх було складніше, ніж традиційні публікації в медіа, наукових журналах або офіційних збірниках. Після появи Інтернету ця інформація стала більш помітною і частіше присутньою онлайн, однак це не зняло повністю проблему її пошуку, перевірки та правильного використання.

Дослідницька служба Конгресу у 2007 році описала чотири категорії відкритої інформації: широкодоступні дані та інформація; цільові комерційні дані; окремі експерти; та «сіра» література [1].

Проте ці категорії не враховують контент, що міститься в соціальних мережах. Дослідники RAND Corporation запропонували поділ доступної інформації на чотири категорії: дві з них є основними, і кожна поділена ще на два рівні. Перша диференціація визначається генератором контенту: інституційно згенерований контент протиставляється індивідуально згенерованому контенту. Інституційно згенерований контент складається з новинних медіа та іншого інституційного контенту, значна частина якого раніше могла бути визначена як «сіра література». Індивідуально згенерований контент, або контент соціальних мереж, поділяється на довгий і короткий, які мають важливі відмінності в обробці та використанні [65, с.11].

У підсумку ми маємо чотири типи відкритої інформації

1) Контент новинних ЗМІ, результат діяльності мультимедіа - газет, журналів (як друковані, так і онлайн), телебачення та радіо, сайтів-агрегаторів новин, які також можуть публікувати оригінальний контент.

2) «Сіра» література, тобто контент, що надходить від немедійних установ та організацій, як державних, так і приватних. Це матеріали дослідницьких установ, національних урядів, приватних видавництв, корпорацій, торгових асоціацій та профспілок, аналітичних центрів та академічних кіл.

3) Тривалий контент соціальних мереж - це матеріал, що містить багато тексту, від окремих осіб або невеликих груп. Він включає матеріали з блогів та сайтів, на зразок колишнього Живого Журналу.

4) Короткий контент соціальних мереж. Це матеріал з таких платформ, як Facebook, Twitter тощо. Зазвичай має невелику цінність окремо; цінність зазвичай отримується шляхом агрегації такої інформації. Однак існує виняток, коли короткий контент соціальних мереж отримується з конкретних акаунтів, що становлять великий інтерес, наприклад, акаунтів відомих осіб, таких як високопоставлені урядовці. Цінний короткий контент також може включати

акаунти осіб, які входять до окремих груп, наприклад представників якогось військового підрозділу або їх родичі.

Крім традиційних відкритих джерел, у сучасному інформаційному середовищі з’являються масиви даних, які потрапляють у публічний простір унаслідок витоків, хакерських операцій або діяльності третіх осіб. Для OSINT-аналітики це створює окрему методологічну і правову проблему. З одного боку, такі дані вже можуть бути доступними для аналізу у відкритому просторі. З іншого боку, спосіб їхнього первинного отримання може бути спірним, а іноді й незаконним, тому аналітик повинен враховувати не лише зміст інформації, а й її походження, надійність, можливі маніпуляції та допустимість подальшого використання.

В українському контексті прикладом такої ситуації є діяльність хакерських та розслідувальних спільнот, зокрема Cyber Resistance та InformNapalm, які працюють з інформацією про російську агресію, військові структури РФ, окупаційні адміністрації та пов’язані з ними інформаційні мережі. Їхні матеріали можуть посилювати можливості OSINT-аналізу, оскільки виводять у публічний простір нові дані, які потім можуть перевірятися, зіставлятися з іншими джерелами та використовуватися для документування діяльності противника. Водночас такі приклади ще раз показують, що OSINT-аналітика не може обмежуватися механічним збором відкритої інформації: вона потребує оцінки джерела, контексту появи даних і ризиків їхнього використання. Окремим різновидом даних, важливих для сучасної OSINT-практики, є комерційно доступна інформація. Йдеться про дані, які збираються, агрегуються або продаються різними компаніями, платформами чи брокерами даних. Частина таких даних може бути отримана легально через відкриті реєстри, офіційні сервіси, аналітичні платформи або комерційні підписки. Водночас існують і сумнівні ринки даних, використання яких створює правові, етичні та безпекові ризики. Тому в межах наукового аналізу важливо не романтизувати такі практики, а розглядати їх як проблемну зону сучасної OSINT-аналітики, особливо в умовах війни.

Дослідник у сфері технологічного права та національної безпеки С. Дж. Аранго описує цю дилему в контексті США і звертає увагу на те, що брокери даних можуть одночасно створювати як можливості, так і ризики для національної безпеки [26]. З одного боку, агреговані комерційні дані можуть допомагати державним структурам швидше отримувати інформацію, виявляти зв'язки, оцінювати ризики та посилювати ситуаційну обізнаність. З іншого боку, використання таких даних порушує питання приватності, контролю за обігом інформації, прозорості походження даних і допустимості їх застосування в безпековій діяльності. Сучасна "економіка спостереження" створює умови, за яких значні масиви персональних, фінансових, поведінкових, геолокаційних та інших даних збираються приватними компаніями, платформами, сервісами й посередниками. Дослідники проблем ринку даних і цифрової нерівності Л. Палк та К. Муралідхар звертають увагу на те, що ринки даних можуть посилювати нерівність доступу до інформації та формувати ситуацію, коли окремі суб'єкти отримують перевагу завдяки можливості купувати або агрегувати великі масиви даних [53]. Для OSINT-аналітики це важливо, оскільки частина інформації, яка формально є несекретною, фактично може бути доступною лише за наявності фінансових, технічних або організаційних ресурсів.

Враховуючи вище сказане, ми повинні визнати, що OSINT, внаслідок своєї поширеності, став доволі різноманітним. Первинно ці технології були зорієнтовані на здобуття розвідувальної інформації, однак згодом вони були запозичені іншими сферами діяльності. Сьогодні результат, на який спрямований OSINT, може бути різним: розвідувальна оцінка, журналістське розслідування, правовий доказ, антикорупційний матеріал, бізнес-аналітика, безпекова довідка або аналітичний звіт. Це накладає відбиток і на умови його здійснення, і на вимоги до якості, законності, перевірки та оформлення отриманої інформації. OSINT у правоохоронній або юридичній сфері висуває більш жорсткі вимоги до легальності походження даних, оскільки зібрані матеріали потенційно можуть бути представлені в суді. Натомість OSINT у сфері безпеки, особливо воєнної безпеки, може працювати з ширшим колом

інформації: відкритими джерелами, комерційно доступними даними, супутниковими знімками, соціальними мережами, реєстрами, витоками, архівами та іншими цифровими слідами. Проте в усіх випадках принциповим залишається не сам факт доступу до інформації, а її перевірка, зіставлення з іншими джерелами і подальше аналітичне осмислення.

У межах цього дослідження, з урахуванням підходів С. Култхарта і Б. Нуссбаума до визначення OSINT як законно отриманої публічної або комерційної інформації, а також підходу дослідників RAND Corporation Г. Дж. Вільямса та І. Блум до розуміння доступної інформації, OSINT доцільно визначити як сукупність законних і методично впорядкованих способів пошуку, збору, отримання та первинної перевірки інформації з відкритих, доступних або комерційно доступних джерел для задоволення конкретної інформаційної потреби [32; 65]. Таке визначення дозволяє не зводити OSINT лише до розвідувальної діяльності, але водночас зберігає його зв’язок із безпековою практикою, оскільки ключовими залишаються інформаційна потреба, джерело, спосіб отримання даних і можливість їх подальшого використання.

OSINT як метод збору інформації може бути інструментом в руках окремого журналіста-розслідувача, антикорупційного активіста, дослідника, приватного аналітика або невеликої волонтерської групи. Проте OSINT у сфері безпеки, особливо воєнної безпеки, не може зводитися лише до діяльності окремих ініціативних осіб. На основі зібраної інформації можуть ухвалюватися рішення, що мають суспільну, безпекову або військову вагу, тому вимоги до такої інформації є вищими. Вона має бути не просто знайдена, а перевірена, зіставлена з іншими даними, правильно інтерпретована і подана у формі, придатній для подальшого використання.

Саме тут виникає потреба розмежувати OSINT і OSINT-аналітику. OSINT у вузькому розумінні можна розглядати як спосіб пошуку, збору й первинної перевірки інформації з відкритих, доступних або комерційно доступних джерел. Натомість OSINT-аналітика є ширшим процесом, який включає не лише отримання даних, а й постановку інформаційної потреби, відбір релевантних

джерел, оцінку їхньої надійності, перевірку інформації, тріангуляцію, інтерпретацію та підготовку аналітичного продукту.

У межах цього дослідження OSINT-аналітику доцільно визначити як методично організовану діяльність зі збору, перевірки, зіставлення, обробки та інтерпретації інформації з відкритих, доступних або комерційно доступних джерел, що здійснюється відповідно до конкретної інформаційної потреби з метою підготовки аналітичного продукту для підтримки рішень у сфері безпеки. На відміну від простого пошуку інформації, OSINT-аналітика передбачає наявність мети, процедури, критеріїв оцінки джерел, тріангуляції даних і практичного результату у вигляді висновку, довідки, звіту, оцінки загрози або іншого аналітичного матеріалу.

Однією з ключових ознак OSINT-аналітики є тріангуляція, тобто перевірка інформації через поєднання кількох джерел, методів, дослідницьких підходів або аналітиків. Це потрібно для того, щоб зменшити ризик помилки, упередження або залежності від одного джерела. У сфері безпеки така вимога має особливе значення, оскільки хибний висновок на основі неперевіреної відкритої інформації може призвести до неправильного розуміння загрози або до помилкового рішення. Тріангуляція відрізняє OSINT-аналітику від простого збору інформації. Якщо окреме фото, відео, повідомлення в соціальній мережі, запис у реєстрі або супутниковий знімок розглядати ізольовано, вони можуть дати лише часткове уявлення про подію. Натомість їх зіставлення між собою дозволяє уточнити місце, час, контекст, достовірність і значення інформації. Саме тому OSINT-аналітика потребує не лише доступу до джерел, а й чіткої процедури їх перевірки.

Отже, у межах цього дослідження можна виокремити чотири основні складові OSINT-аналітики: а) збір інформації, який доповнюється обробкою, перевіркою, тріангуляцією та аналізом; б) використання відкритих, доступних або комерційно доступних джерел, а не інсайдів чи неперевірених суб’єктивних повідомлень; в) спрямованість діяльності на конкретну інформаційну потребу; г)

методичність, тобто здійснення роботи за певними правилами, процедурами і критеріями оцінки джерел та інформації.

Вказані складові дозволяють розглядати OSINT-аналітику як самостійне явище в межах сучасної безпекової діяльності. Вона не зводиться лише до технічного пошуку інформації у відкритих джерелах, а передбачає перетворення розрізнених даних на перевірений аналітичний продукт. Саме ці ознаки визначають подальші методологічні проблеми OSINT-аналітики, які розглядаються в наступному підрозділі.

1.3. Методологічні проблеми дослідження OSINT-аналітики в умовах цифровізації безпекового середовища

Дослідження OSINT-аналітики ускладнюється тим, що вона перебуває на межі кількох сфер: розвідувальної діяльності, безпекової аналітики, журналістських розслідувань, цифрової верифікації, роботи з великими даними та правового аналізу. Через це її не можна розглядати лише як набір технічних інструментів для пошуку інформації. У науковому сенсі OSINT-аналітика потребує чітких критеріїв оцінки джерел, процедур перевірки інформації, правил тріангуляції, розуміння правових і етичних меж, а також пояснення того, як розрізнені відкриті дані перетворюються на аналітичний продукт. Саме тому ключові проблеми OSINT-аналітики доцільно розглядати не тільки як практичні труднощі її застосування, а як методологічні проблеми дослідження: як визначити надійність джерела, як перевірити достовірність інформації, як уникнути інформаційного шуму, як працювати з дезінформацією, як оцінити межі використання “сірих” або комерційно доступних даних і як забезпечити придатність висновків для ухвалення рішень у сфері воєнної безпеки.

Однією з ключових методологічних проблем дослідження OSINT-аналітики є відсутність загальновизнаної системи оцінки надійності відкритих джерел і достовірності отриманої з них інформації. У традиційній розвідувальній діяльності для цього використовуються формалізовані підходи, зокрема

Адміралтейський кодекс, який допомагає окремо оцінювати джерело інформації та сам зміст повідомлення. Для OSINT-аналітики така проблема є особливо складною, оскільки відкриті джерела дуже різні за походженням, рівнем перевіреності, умовами доступу, можливими упередженнями і ризиком маніпуляції. Тому в межах дослідження OSINT-аналітики важливо не лише описати джерела інформації, а й визначити, за якими критеріями можна оцінювати їхню надійність і придатність для ухвалення рішень у сфері воєнної безпеки.

Адміралтейський кодекс, або Кодекс оцінки джерел розвідки НАТО, використовується для оцінки як самого джерела інформації, так і змісту отриманого повідомлення. Спочатку він був розроблений Британським Королівським флотом під час Другої світової війни, а на початку Холодної війни був формалізований для потреб розвідувальної діяльності. Його поява була зумовлена необхідністю систематизувати оцінювання великої кількості інформації, яка надходила з різних джерел HUMINT: від досвідчених агентів до випадкових інформаторів.

Важливість Адміралтейського кодексу полягає в тому, що він дозволяє розрізняти два різні питання: наскільки надійним є джерело і наскільки достовірною є конкретна інформація. Це принципово важливо, оскільки навіть ненадійне джерело іноді може надати точну інформацію, а загалом надійне джерело може помилитися або передати неповні дані. Для дослідження OSINT-аналітики ця логіка є корисною, оскільки відкриті джерела також не можна оцінювати лише за їхньою популярністю, доступністю або формальною відкритістю. Надалі Кодекс був прийнятий і стандартизований НАТО, що призвело до появи формату подвійної оцінки розвідувальної інформації: за шкалою від A до F оцінюється надійність джерела, а за шкалою від 1 до 6 - достовірність самої інформації. При цьому важливо враховувати, що шкала Адміралтейського кодексу є не інтервальною, а порядковою. Тобто різниця між оцінками A і B не обов’язково дорівнює різниці між B і C. Це означає, що така

система не дає математично точного виміру, але допомагає впорядкувати професійне судження аналітика.

Чогось подібного у світі OSINT поки що немає, і згаданий Адміралтейський кодекс без адаптації до умов OSINT використовувати не можна, оскільки ця сфера надто специфічна. Втім все ж щодо частини сучасних цифрових джерел його використовувати можна, наприклад щодо якісних журналів та газет, супутникових знімків та прозорих урядових баз даних. Ці джерела, як правило, створюються з дотриманням конкретних методів збору інформації та установами, які несуть відповідальність за помилки. Такі авторитетні журналістські організації як BBC або ж Reuters, дотримуються редакційних стандартів та процедур перевірки фактів. Нижче від них по обом зі згаданих шкал, тобто гірше оцінюються, перебувають такі джерела, як експертні блоги або аналітичні центри - які є важливими, проте потенційно упередженими джерелами.

Окрім уваги до самого джерела, Адміралтейський кодекс нагадує ще про одну важливу методологічну проблему: сама інформація також має бути перевірена. У контексті OSINT-аналітики недостатньо встановити, звідки походить повідомлення. Потрібно з’ясувати, чи підтверджується воно іншими даними, чи можна перевірити його зміст, чи не є воно частиною інформаційної маніпуляції, а також чи не виникає ефект повторення одного й того самого повідомлення в різних джерелах. У цьому сенсі ми знову повертаємось до тріангуляції. OSINT-аналітик має зіставляти різні типи даних: фото, відео, супутникові знімки, повідомлення в соціальних мережах, геолокацію, метадані, записи польотів, карти, офіційні повідомлення та інші відкриті джерела. Наприклад, незалежна група Bellingcat використовувала зображення із соціальних мереж, супутникові дані та записи польотів для ідентифікації російського військового підрозділу, відповідального за збиття рейсу MH17 Malaysia Airlines. В інших випадках OSINT-аналітики відстежували переміщення військ під час російського вторгнення в Україну у 2022 році за допомогою геолокації відео з TikTok та інших соціальних платформ, а також

супутникових знімків. Такий підхід до OSINT-аналітики вимагає більшого, ніж просто технічних навичок пошуку. Він потребує балансу між скептицизмом і дисципліною. При цьому йдеться не про недовіру до всього, а про структурований скептицизм, коли будь-яке повідомлення спершу розглядається як попередня інформація, що потребує перевірки. Аналітик має бути готовим переглядати попередні висновки, якщо з'являються кращі докази, нові джерела або інший контекст події.

Структурований скептицизм означає не просто пошук інформації, а її подальше дослідження: перехресну перевірку, застосування логічних міркувань, готовність до повторного аналізу та використання різних методів перевірки. Наприклад, американський дослідник інформаційної культури М. Фейнберг у праці «Everyday Adventures with Unruly Data» звертає увагу на складність роботи з неструктурованими та "некерованими" даними, що є важливим для розуміння сучасної OSINT-аналітики [36]. У відкритому інформаційному середовищі дані часто є неповними, фрагментарними, повторюваними або вирваними з контексту, тому вони потребують не механічного використання, а критичної оцінки.

Одним із можливих методичних інструментів такої оцінки є CRAAP-тест. Його логіка полягає у перевірці інформації за кількома критеріями: актуальність, релевантність, авторитетність, точність і мета. Для OSINT-аналітики ці критерії мають практичне значення, оскільки дозволяють поставити до джерела і повідомлення базові контрольні питання: коли була оприлюднена інформація, чи відповідає вона дослідницькій потребі, хто є її автором або поширювачем, чи можна перевірити наведені факти, а також з якою метою ця інформація могла бути опублікована.

Особливо важливою для OSINT-аналітики є оцінка авторитетності джерела. Аналітик має з'ясувати, хто є автором, видавцем, власником або спонсором ресурсу; чи має автор кваліфікацію або доступ до теми, про яку пише; чи є контактна інформація, редакційна політика або організаційна приналежність; чи не приховує джерело свою афіліацію; що може свідчити про

походження ресурсу його домен, архів публікацій або попередня репутація. Така перевірка не дає абсолютної гарантії достовірності, але допомагає зменшити ризик використання випадкових, маніпулятивних або неперевірених даних.

У контексті воєнної безпеки CRAAP-тест і подібні методи оцінки мають значення не як формальна академічна вправа, а як спосіб дисциплінувати роботу з відкритими джерелами. В умовах війни інформація може поширюватися швидко, емоційно і з високим рівнем маніпулятивності. Тому методологічна проблема полягає не лише в тому, щоб знайти повідомлення, а в тому, щоб оцінити його актуальність, джерело, доказову силу, можливу мету поширення і придатність для подальшого аналітичного висновку.

Сьогодні часто можна зустріти ситуацію, коли джерелом у статтях новинних ЗМІ є інші медіа. Для OSINT-аналітики це створює ризик ехо-ефекту, коли одна й та сама інформація багаторазово повторюється різними ресурсами, але фактично походить з одного первинного джерела. У такому випадку зовнішня кількість згадок може створювати хибне враження достовірності, хоча насправді аналітик має справу не з незалежними підтвердженнями, а з повторенням одного інформаційного сигналу. У межах дослідження OSINT-аналітики важливо враховувати й еволюцію медіаландшафту. Йдеться про поширення інфотейнменту, зростання ролі соціальних мереж, прискорення новинного циклу, конкуренцію за увагу аудиторії та активне використання редакціями інструментів штучного інтелекту. Наслідком цього є не лише збільшення кількості доступної інформації, а й ускладнення її оцінки. Частина матеріалів може подаватися емоційно, фрагментарно або в надмірно спрощеній формі, що знижує її аналітичну цінність для дослідження воєнної безпеки. Сучасний штучний інтелект уже здатен автоматично створювати новинні матеріали, короткі повідомлення, огляди та аналітичні тексти. Це дає медіа змогу працювати швидше й охоплювати більше тем, але водночас створює нові ризики для достовірності інформації. Навіть якісний алгоритм залежить від джерел, які він використовує. Якщо вхідні дані містять помилки, пропаганду, неповноту або

маніпулятивні формулювання, автоматизована система може відтворити ці викривлення без достатнього критичного осмислення.

Окрему проблему становить аналіз російського інформаційного простору. У випадку РФ ідеться не просто про звичайні помилки медіа або політичну упередженість. Значна частина російського медіаландшафту функціонує в умовах державного контролю, самоцензури, пропаганди та цілеспрямованого інформаційного впливу. Тому дані, отримані з російських медіа, часто є не просто викривленими, а "отруєними" з погляду інформаційного середовища. Для OSINT-аналітики це означає, що такі повідомлення потрібно аналізувати не тільки за питанням "що сказано?", а й за питанням "навіщо це поширено?", "для якої аудиторії?", "який сигнал або інформаційну операцію це може відображати?".

Російська сторона навмисно поширює неправдиву інформацію, використовує прес-релізи, організовані витоки та дезінформаційні кампанії. За цих умов OSINT-аналітика може бути дуже корисною, проте різні автори по-різному оцінюють її перспективи у воєнному середовищі. Дослідники ролі відкритих джерел у російсько-українській війні Х. ван Бік і С. Ріт'єнс налаштовані більш оптимістично і вважають, що OSINT може допомогти частково розвіяти «туман війни» [63, с. 57]. Інші дослідники проблем OSINT у сфері стратегічного аналізу та воєнної безпеки - О. Крпец, М. Чованчик та А. Ілавська - налаштовані більш скептично. Вони розглядають питання, чи можна проводити OSINT-аналітику з методичної точки зору настільки правильно, щоб перетворити її на надійну стратегічну розвідку в умовах невизначеності воєнного часу. Відповідаючи на це питання, автори наголошують, що OSINT-аналітика має доповнювати традиційну розвідку, забезпечуючи перехресну перевірку відкритих даних з експертними оцінками та іншими джерелами інформації [47].

Іншою методологічною проблемою дослідження OSINT-аналітики є питання її інтеграції в ширшу систему розвідувального та безпекового аналізу. Йдеться не лише про те, чи можуть державні структури використовувати відкриті джерела, а про те, яке місце OSINT-аналітика займає серед інших

способів отримання й перевірки інформації. Саме тут виникає дискусія: чи є OSINT самостійним напрямом аналітичної роботи, чи лише допоміжним інструментом для уточнення, перевірки або доповнення даних, отриманих іншими засобами.

Частина дослідників критично оцінює можливості OSINT. Зокрема, дослідник проблем теорії розвідки Дж. М. Гетфілд стверджує, що саме поняття «розвідка з відкритих джерел» є проблемним, оскільки відкриті джерела самі по собі не є розвідкою і набувають розвідувального значення лише після професійної аналітичної обробки [42]. Така позиція важлива для цього дослідження, бо вона не заперечує цінність відкритих джерел, але змушує розрізняти відкриту інформацію, OSINT як спосіб її збору та OSINT-аналітику як процес створення обґрунтованого аналітичного продукту.

Прихильники ширшого використання OSINT, навпаки, звертають увагу на його здатність доповнювати традиційні розвідувальні дисципліни, особливо в умовах швидкої зміни ситуації, інформаційної відкритості та великої кількості цифрових слідів. У цьому контексті OSINT не варто розглядати як заміну секретній розвідці. Більш коректно говорити про його допоміжну та посилювальну функцію: відкриті джерела можуть швидко давати первинні орієнтири, допомагати перевіряти окремі факти, виявляти інформаційні сигнали та формувати основу для подальшого аналізу. Саме тому інтеграція OSINT-аналітики має методологічне значення. Якщо її результати використовуються ізольовано, без зіставлення з іншими джерелами, вони можуть створювати ризик помилкових висновків. Якщо ж OSINT-аналітика поєднується з іншими розвідувальними дисциплінами, експертними оцінками та внутрішніми даними організацій, її цінність зростає. Б. Міллер також наголошує, що OSINT, як правило, забезпечує найбільшу цінність саме у поєднанні з іншими дисциплінами [94]. Подібну логіку підтримують і дослідники К. Елдрідж, К. Гоббс та М. Моран, які розглядають сучасну OSINT-аналітику як поєднання алгоритмічної обробки великих масивів відкритих даних і людської аналітичної оцінки [35].

Питання інтеграції OSINT-аналітики можна розглядати на трьох рівнях: рівні розвідувальної або безпекової спільноти, рівні окремої організації та індивідуальному рівні конкретного аналітика. Такий поділ важливий не лише для опису практики, а й для дослідження OSINT-аналітики як явища, оскільки дає змогу зрозуміти, де саме виникають основні методологічні труднощі: у структурі інституцій, у процедурах роботи організацій або в підготовці окремих фахівців.

На рівні спільноти однією з дискусійних проблем є питання централізації або децентралізації OSINT-аналітики. Дослідниця американської розвідувальної спільноти Е. Зегарт, описуючи розподіл функцій між розвідувальними агентствами США, пропонує створити окреме агентство, яке займалося б виключно OSINT [105]. На її думку, спеціалізація може стимулювати інновації, посилити професіоналізацію та забезпечити кращу координацію роботи з відкритими джерелами. Водночас така модель породжує питання, чи не призведе надмірна централізація до відриву OSINT-аналітики від потреб конкретних організацій і підрозділів.

На рівні окремої організації інтеграція OSINT-аналітики означає її використання не як заміни традиційних методів розвідки або безпекового аналізу, а як додаткового інструменту, який має бути включений у загальний аналітичний цикл. У тих організаціях, де OSINT використовується системно, його результати порівнюються з іншими джерелами інформації, перевіряються, контекстуалізуються і лише після цього подаються особам, які ухвалюють рішення. Саме тому методологічною проблемою є не лише наявність доступу до відкритих даних, а й створення процедур, які визначають, як ці дані перевіряються, хто несе відповідальність за висновки і яким чином OSINT-матеріали включаються в ширшу систему аналізу.

Окремою дискусією є питання організаційної моделі: чи повинна OSINT-аналітика виконуватися внутрішніми командами, чи може частина завдань передаватися зовнішнім підрядникам і експертним мережам. Дослідник розвідувальних систем Р. Довер виступає за створення внутрішніх OSINT-

команд у структурі організацій [33]. Натомість дослідник трансформації розвідки В. Ланеман пропонує гнучкіший підхід, за якого окремі завдання можуть делегуватися надійній мережі зовнішніх підрядників [48]. Ця дискусія важлива для дослідження OSINT-аналітики, оскільки різні організаційні моделі по-різному впливають на контроль якості, безпеку даних, швидкість роботи, доступ до спеціалізованих компетенцій і відповідальність за кінцевий аналітичний продукт.

У різних країнах ці питання вирішуються по-різному. Наприклад, в Австралії одним із центрів роботи з відкритими джерелами протягом 1990-х років було Управління національних оцінок, яке належало до системи розвідувальних державних структур. В Ізраїлі у структурі воєнної розвідки «Аман» був створений спеціальний підрозділ «Хатсав», який працював саме з відкритими джерелами інформації. Крім того, з відкритими джерелами працював і Центр досліджень і політичного планування у структурі Міністерства закордонних справ Ізраїлю, який збирав і аналізував інформацію від дипломатичних представництв та з відкритих джерел, зокрема газет, телебачення й Інтернету [9, с. 38].

Поряд із державною моделлю інтеграції існує і підхід, заснований на залученні недержавних суб’єктів. Прикладами можуть бути аналітичні центри, дослідницькі організації, приватні компанії, волонтерські спільноти та спеціалізовані OSINT-проєкти. Така модель є гнучкішою і часто швидше реагує на нові інформаційні сигнали, однак вона також створює методологічні питання щодо стандартизації процедур, перевірки якості, безпеки джерел, правових меж і довіри до результатів. Тому для дослідження OSINT-аналітики важливо враховувати не лише те, хто саме здійснює аналіз, а й за якими правилами, з яким доступом до даних і з якою відповідальністю за результат.

Щодо третього, індивідуального рівня інтеграції OSINT-аналітики в діяльність, важливим є дослідження американського дослідника розвідувальної культури Д. Джентрі. Він зазначає, що в США аналітики можуть уникати використання OSINT, якщо це суперечить їхнім професійним уподобанням або

звичним підходам до роботи [38, с. 836]. Це показує, що проблема інтеграції OSINT-аналітики має не лише організаційний, а й індивідуальний вимір. Тому важливим є введення OSINT-аналітики в навчальні плани спеціалізованих навчальних закладів, а також у програми професійної перепідготовки фахівців з питань національної безпеки, воєнної безпеки та розвідувальної діяльності. Без відповідної підготовки навіть доступ до відкритих джерел і сучасних цифрових інструментів не гарантує якісного аналітичного результату.

Наступна проблема OSINT-аналітики пов’язана з тим, що не так давно зробило її особливо цінною, а саме зі стрімким зростанням кількості відкритих даних. Сьогодні доступний настільки великий обсяг інформації з різних публічних джерел, що її збір, відбір і аналіз перетворюються на трудомісткий процес, який потребує значного часу, ресурсів і чіткої методики. Один із дослідників метафорично описав спробу працювати з таким масивом даних як намагання «пити воду з брандспойта».

Українські дослідники Д. С. Зоренко та інші розглядають OSINT як процес пошукової роботи. На їхню думку, творчий підхід до вибору ключових слів, комбінування різних варіантів пошуку та критичне ставлення до надійності джерел є важливими для досягнення результату. Автори також підкреслюють проблеми роботи з великими обсягами даних, необхідність верифікації інформації та високі вимоги до кваліфікації аналітиків. Такий підхід дозволяє розкрити більш чітку картину об’єкта дослідження, що допомагає приймати обґрунтовані рішення [71, с. 6-7].

Один із можливих шляхів розв’язання цієї проблеми пропонують дослідники використання великих даних в OSINT К. Елдрідж, К. Гоббс та М. Моран [35]. На їхню думку, необхідною стає розробка програмного забезпечення, яке допомагає аналітикам збирати, фільтрувати та опрацьовувати великі набори даних за допомогою автоматизованих процесів. Автоматизацію OSINT-аналітики ці автори розглядають уже не як інновацію, а як необхідність, оскільки без неї зростання обсягу відкритих даних може суттєво обмежити потенціал OSINT.

Ефективно організований процес OSINT-аналітики має забезпечувати взаємодоповнюваність людини й технологій. Програмні продукти можуть швидко опрацьовувати великі масиви даних, виявляти повтори, закономірності, зв'язки та аномалії. Водночас саме аналітик забезпечує контекст, критичну оцінку, розуміння безпекового значення інформації та відповідальність за кінцевий висновок. Тому методологічна проблема полягає не лише у впровадженні автоматизації, а й у визначенні меж між машинною обробкою даних і людським аналітичним судженням.

Ці питання доповнюються дискусією щодо використання штучного інтелекту в OSINT-аналітиці. ШІ може зменшувати інформаційне перевантаження, допомагати у класифікації, пошуку, перекладі, узагальненні та первинному аналізі відкритих даних. Проте він також створює ризики помилкових висновків, алгоритмічної упередженості, некритичного відтворення дезінформації та надмірної довіри до автоматизованих результатів. Тому держави, що матимуть розвинені технології штучного інтелекту, аналітики великих даних і підготовлених фахівців, отримуватимуть дедалі більшу перевагу в OSINT-аналітиці.

Таким чином, ключові проблеми OSINT-аналітики у межах цього підрозділу розглядаються не лише як практичні труднощі її застосування, а як методологічні проблеми дослідження. Йдеться передусім про критерії оцінки джерел, способи перевірки інформації, тріангуляцію, роботу з інформаційним шумом і дезінформацією, правові та етичні межі використання відкритих і комерційно доступних даних, а також про інтеграцію результатів OSINT-аналітики в процес ухвалення рішень у сфері воєнної безпеки. Саме ці проблеми визначають подальшу логіку аналізу OSINT-аналітики як інструменту посилення воєнної безпеки України.

Висновки до розділу 1

У першому розділі було розглянуто теоретичну основу дослідження OSINT-аналітики. Головний висновок полягає в тому, що OSINT не варто

розуміти спрощено - лише як пошук інформації в Інтернеті або використання відкритих джерел. Це значно складніше явище, яке поєднує роботу з джерелами, перевірку інформації, аналіз, порівняння даних і підготовку висновків для конкретної потреби. Для теми цієї роботи це важливо, бо у сфері воєнної безпеки сама наявність інформації ще нічого не гарантує. Значення має те, наскільки вона перевірена, правильно зрозуміла і чи може бути використана для ухвалення рішень.

У підрозділі 1.1 було показано, що OSINT не виник раптово разом з Інтернетом. Використання відкритих джерел має довшу історію, яка пов’язана з розвитком преси, радіо, публічних повідомлень, державних документів та інших доступних матеріалів. Водночас саме цифрова епоха різко змінила масштаби OSINT. Соціальні мережі, супутникові сервіси, цифрові карти, відкриті реєстри, онлайн-медіа та комерційні бази даних створили нову ситуацію, коли відкритої інформації стало дуже багато. Для України це особливо помітно через російсько-українську війну, адже війна створила і великий масив відкритих даних, і постійну потребу в їх перевірці.

У підрозділі 1.2 було розглянуто різні підходи до визначення OSINT і OSINT-аналітики. Як бачимо, у частині джерел OSINT розуміється як інформація з відкритих джерел, в інших - як розвідувальний продукт, а ще в інших - як процес збору, перевірки й аналізу даних. Через це важливо розрізняти OSINT і OSINT-аналітику. OSINT у цій роботі розглядається як спосіб пошуку, збору та первинної перевірки інформації з відкритих, доступних або комерційно доступних джерел. OSINT-аналітика є ширшим поняттям, бо включає не тільки отримання даних, а й їх перевірку, зіставлення, інтерпретацію та підготовку аналітичного продукту.

У підрозділі 1.3 було визначено основні методологічні проблеми дослідження OSINT-аналітики. До них належать відсутність універсальної системи оцінки відкритих джерел, складність перевірки достовірності інформації, потреба в тріангуляції, ризик інформаційного шуму, дезінформації та ехо-ефекту, правові й етичні межі використання “сірих” або комерційно

доступних даних, а також проблема інтеграції OSINT-аналітики в ширшу систему ухвалення рішень у сфері воєнної безпеки. Окреме значення має проблема роботи з великими масивами даних, автоматизацією та штучним інтелектом, оскільки сучасна OSINT-аналітика потребує поєднання технологічних інструментів і людського аналітичного судження.

Отже, результати першого розділу дають змогу розглядати OSINT-аналітику як самостійний напрям сучасної безпекової діяльності, що має власну історію становлення, понятійний апарат, методологічні засади та проблеми застосування. Для подальшого дослідження важливим є висновок про те, що цінність OSINT-аналітики полягає не лише в доступі до відкритої інформації, а в здатності перетворювати розрізнені дані на перевірений, структурований і практично корисний аналітичний продукт. Саме це створює підстави для подальшого аналізу OSINT-аналітики як інструменту посилення воєнної безпеки України.

РОЗДІЛ ІІ
OSINT-АНАЛІТИКА ЯК ІНСТРУМЕНТ ПОСИЛЕННЯ ВОЄННОЇ БЕЗПЕКИ УКРАЇНИ

У цьому розділі OSINT-аналітика розглядається вже не лише як теоретичне поняття, а як практичний інструмент, який може посилювати воєнну безпеку України. Основна увага приділяється тому, як відкриті, доступні та комерційно доступні джерела можуть використовуватися для виявлення загроз, перевірки інформації, підвищення ситуаційної обізнаності та підтримки ухвалення рішень в умовах російсько-української війни. Окремо розбирається організаційна послідовність проведення OSINT-аналітики, її переваги, можливості штучного інтелекту, а також приклади застосування на тактичному й локальному рівнях. Такий підхід дозволяє перейти від загального аналізу поняття OSINT до розуміння його реального значення для системи воєнної безпеки України.

2.1. Організація та методична послідовність проведення OSINT-аналітики у сфері воєнної безпеки

У сфері воєнної безпеки рішення часто доводиться ухвалювати швидко і не завжди в умовах повної інформації. Саме тому важливо не просто мати доступ до відкритих джерел, а розуміти, як з ними працювати. OSINT-аналітика в цьому випадку має значення не як випадковий пошук у мережі, а як послідовна робота з інформацією, яка може допомогти уточнити обстановку, перевірити повідомлення, виявити загрозу або підготувати матеріал для подальшого рішення.

Першим етапом такої роботи є задум дослідження або формулювання інформаційної потреби. Тобто потрібно чітко визначити, що саме необхідно з’ясувати, для кого готується інформація, у який строк і для якого рішення вона може бути використана. Без цього OSINT швидко перетворюється на перегляд

великої кількості відкритих даних без зрозумілого результату. У воєнній сфері така хаотичність є небезпечною, бо неперевірена або неправильно зрозуміла інформація може створити хибне уявлення про ситуацію.

Як уже зазначалося в першому розділі, OSINT-аналітика може інтегруватися на трьох рівнях: рівні безпекової спільноти, рівні окремої організації та рівні конкретного аналітика. Для цього підрозділу важливо не стільки повторити ці рівні, скільки показати, як вони проявляються в практичній послідовності роботи. На рівні організації мають бути визначені правила збору, перевірки й передачі інформації. На рівні аналітика важливими є навички пошуку, критичної оцінки джерел, тріангуляції та підготовки зрозумілого аналітичного висновку.

У загальному вигляді проведення OSINT-аналітики у сфері воєнної безпеки можна подати як послідовність кількох етапів: визначення інформаційної потреби, добір джерел, збір даних, первинна фільтрація, перевірка достовірності, зіставлення з іншими джерелами, аналітична інтерпретація та підготовка кінцевого продукту. Саме така послідовність дозволяє перейти від окремих відкритих повідомлень до інформації, яка має практичну цінність для ухвалення рішень.

Цікавим прикладом організації OSINT-аналітики є досвід США. У Сполучених Штатах робота з відкритими джерелами впроваджується вже тривалий час і поступово розглядається не як другорядна діяльність, а як окремий елемент розвідувального та безпекового процесу. З метою оптимізації роботи з відкритими джерелами у 2004 році президент США Дж. Буш підписав закон «Про реформування розвідки та протидію терористичним загрозам», відповідно до якого розвідка з відкритих джерел була визнана повноцінним напрямом діяльності розвідувального співтовариства. Це важливо для теми цього підрозділу, оскільки показує: ефективна OSINT-аналітика потребує не лише окремих фахівців або інструментів, а й організаційного закріплення, процедур, відповідальних структур і місця в загальній системі ухвалення рішень.

Армія США постійно працює над оновленням своєї стратегії розвитку OSINT. В рамках написання дипломної роботи я знайшов і аналізував «OSINT стратегію на 2024-2028 роки» [2], проте тільки тому, що варіанти розраховані на більш тривалу перспективу ще не стали публічними. Ця стратегія оновлює та замінює Стратегію OSINT Міністерства оборони США на 2012-2017 роки. Рада Міністерства оборони США з питань відкритих джерел / Defense Open Source Council, DOSC є основним органом управління для OSINT Міністерства оборони та служить форумом для координації та сприяння діяльності та програмам OSINT Міністерства оборони. В структурі армії також з'явився старший радник армії з питань OSINT, на цю посаду було призначено Д. Егера. З публікацій у ЗМІ та з інтерв'ю Д. Егера відомо що у довготривалій армійській стратегії враховано потребу використання можливостей штучного інтелекту та великих мовних моделей.[97]

Армія США поставила за мету здійснити суттєві зміни у своїй структурі та навчальному процесі, зокрема створити «сили збору» (collection force), які мають працювати з відкритими даними, а також запровадити посади «збирачів OSINT» (OSINT collector).

Однією з ознак зростання уваги армії США до OSINT-аналітики є очікуване затвердження «ідентифікатора навичок» OSINT (OSINT skill identifier). Такі ідентифікатори є кодами, які армія використовує для позначення спеціальної підготовки, пройденої військовослужбовцем.

Армія США також планувала створювати команди збору OSINT у своїх основних формуваннях. З огляду на можливий дефіцит підготовлених кадрів, розглядалася можливість залучення до таких посад не лише військовослужбовців, а й цивільних працівників.

Для України цей досвід важливий не як модель для прямого копіювання, а як приклад того, що OSINT-аналітика у військовій сфері потребує організації, навчання, визначених посад і швидкого доведення результатів до тих, хто ухвалює рішення. В умовах російсько-української війни це має безпосереднє значення для воєнної безпеки України, оскільки швидка перевірка відкритих

даних, виявлення загроз і передача аналітичних висновків можуть посилювати ситуаційну обізнаність на стратегічному, оперативному й тактичному рівнях.

У цьому контексті особливого значення набуває підготовка фахівців. У першому розділі вже зазначалося, що на індивідуальному рівні інтеграція OSINT-аналітики має передбачати включення відповідних курсів до навчальних планів спеціалізованих навчальних закладів. В американській армії було розроблено базовий курс підготовки з OSINT, який пропонується проходити онлайн у партнерстві з Університетом Аризони. У планах армії США також було створення «Армійського університету OSINT», який мав би пропонувати понад 40 онлайн-курсів, включаючи курс для «лідерів» OSINT. Окремо вивчається питання інтеграції OSINT-підготовки в центри бойової підготовки армії, щоб вона стала частиною сценаріїв для військових, які проходять первинну підготовку або ротацію.

Ще однією важливою метою армії США є швидша доставка результатів OSINT-аналітики до так званого «тактичного краю», тобто до рівня безпосереднього командування бойовими діями. Д. Егер пояснював це так: «Я хотів би, щоб звіти OSINT майже миттєво надходили до тактичного краю, тобто збирач пише свій звіт, натискає кнопку, і протягом 30 секунд - хвилини він поширюється там, де командир бачить його» [97]. Г. Зелмер, директор Управління OSINT армії США (Army OSINT Office), також звертає увагу на те, що OSINT-аналітика поступово інтегрується в діяльність Міністерства оборони США як окрема спроможність. На його думку, відбувається культурний і стратегічний зсув у розумінні OSINT: його дедалі частіше розглядають не як допоміжну функцію, а як критично важливий інструмент для забезпечення ситуаційної обізнаності та швидшого ухвалення рішень командирами в різних оперативних середовищах.

У багатьох сценаріях OSINT-аналітика є однією з найбільш швидко доступних форм розвідувальної інформації, оскільки може давати первинні дані раніше, ніж інші розвідувальні дисципліни. Для командирів на полі бою та планувальників операцій така швидкість може мати практичне значення,

особливо тоді, коли потрібно швидко використати можливість або вчасно відреагувати на зміну обстановки. Щоб підвищити цінність OSINT, армія США робить акцент на професіоналізації цього напряму. Саме з цим пов’язане створення окремого Управління OSINT армії, яке має координувати стандартизацію процедур, підготовку аналітиків та інтеграцію OSINT у ширші розвідувальні процеси.

У цьому підході важливо те, що OSINT уже не сприймається як “бонусний” потік розвідувальних даних. Він дедалі частіше стає початковою точкою для багатьох оцінок, особливо в ситуаціях, де час має критичне значення. Він все частіше стає відправною точкою для багатьох оцінок, особливо у сценаріях, чутливих до часу.

У першому розділі вже йшлося про необхідність узгоджених і сталих процедур здійснення OSINT-аналітики. Дослідники, які інтерпретують відкриті дані та перетворюють їх на змістовну інформацію, постійно стикаються з труднощами, пов’язаними зі зростанням обсягу, швидкості, різноманітності та складності перевірки даних [68]. Саме тому OSINT-аналітика може бути дієвим інструментом у сфері воєнної безпеки лише за умови дотримання методичних вимог. Інакше великий масив відкритої інформації не посилює аналіз, а навпаки може створювати інформаційний шум, хибні висновки або ілюзію достатньої обізнаності.

Навіть якщо базу даних для OSINT легко отримати, вона є актуальною й обширною, саме з цих якостей виникають подальші проблеми: пошук у великому масиві даних, уникнення інформаційного шуму, ризик заплутування дезінформацією або навмисно “отруєною” інформацією, оцінка того, що справді важливо, робота із занадто загальним характером окремих відкритих повідомлень, а також поширення повторюваної інформації та ефект ехо [69, с. 235-236]. Крім того, відкриті джерела не завжди дають відповідь на найбільш чутливі питання, особливо якщо йдеться про закриті військові програми, авторитарні держави або об’єкти з високим рівнем секретності [70, с. 2].

Жоден метод розвідки не є ідеальним, і в розвідувальній діяльності немає “кришталевої кулі”. OSINT зазвичай слугує доброю відправною точкою для подальшого аналізу, оскільки дозволяє швидко отримати первинні дані, сформувати початкове уявлення про ситуацію і визначити, які питання потребують додаткової перевірки. Саме тому OSINT може не замінювати інші методи розвідки, а обмежувати зайве їх використання або точніше спрямовувати подальший збір інформації. Як зазначав Р. Стіл, OSINT забезпечує міцну основу для інших розвідувальних дисциплін [71, с. 129].

Однією з головних вимог до OSINT-аналітики є дотримання послідовних етапів здобуття, обробки, перевірки та поширення інформації. Водночас не менш важливим є структурований скептицизм, тобто постійна готовність перевіряти знайдені дані, порівнювати їх з іншими джерелами і не сприймати відкриту інформацію як автоматично достовірну. Наявність таких етапів характерна не лише для OSINT-аналітики, а й для розвідувальної діяльності загалом. За словами Д. Оманда, класичний процес розвідки складається з таких елементів: встановлення вимог до інформації та висновків, збір інформації, аналіз та оцінка, поширення результатів і зворотний зв’язок від замовників [72, с. 117-118].

Подібну логіку має і підхід Об’єднаного штабу США, де розвідувальний цикл поділяється на такі етапи: планування та керівництво, збір, обробка та використання, аналіз і виробництво, поширення та інтеграція [73, с. 170].

Українські дослідники Д. С. Зоренко та інші розглядають OSINT як процес пошукової роботи, що включає визначення вихідних даних і мети пошуку, вибір інструментів та заходів, збір і систематизацію інформації, а також формулювання висновків на основі отриманих даних [71, с. 6-7]. З огляду на ці підходи, у межах цього дослідження доцільно виділити такі основні етапи OSINT-аналітики: визначення інформаційної потреби, збір даних, обробку інформації, аналіз отриманих даних, поширення результатів, отримання зворотного зв’язку та внесення необхідних коригувань.

OSINT-аналітика також потребує дотримання послідовних етапів, оскільки її результатом має бути не просто масив знайдених повідомлень, а

інформація, придатна для подальшого використання. У сфері воєнної безпеки це особливо важливо, бо кінцевий аналітичний продукт може впливати на оцінку обстановки, визначення загроз і підготовку рішень на стратегічному, оперативному або тактичному рівні.

Водночас OSINT використовується не лише у військових питаннях. Його застосовують державні органи, приватний сектор, журналісти-розслідувачі, аналітичні центри та громадські ініціативи. Проте саме у сфері воєнної безпеки вимоги до якості такої аналітики є особливо високими, оскільки помилка в оцінці відкритих даних може мати практичні наслідки для безпеки держави.

Щодо OSINT-аналітики існує певна згода, що вона стала важливим фактором сучасного збройного конфлікту [47, с. 1-15]. Збройні сили різних держав дедалі більше усвідомлюють значення OSINT-аналітики для воєнної безпеки загалом і для власної діяльності зокрема. У літературі часто наводиться теза про те, що значна частина інформації, необхідної для ухвалення рішень, може надходити саме з відкритих джерел. Це не означає, що OSINT замінює інші види розвідки, але показує, що відкриті джерела можуть бути важливою основою для первинної оцінки обстановки, подальшої перевірки даних і підтримки рішень.

OSINT зазвичай здійснюється шляхом моніторингу, аналізу та дослідження інформації з мережі Інтернет, соціальних мереж, відкритих реєстрів, медіа, супутникових сервісів, комерційних баз даних та інших доступних джерел. Матеріали, підготовлені з використанням відкритих джерел, можуть підтримувати різні напрями розвідувальної діяльності завдяки накопиченню, аналізу й поширенню знань [66, с. 65-77]. Для воєнної безпеки України це має практичне значення, оскільки OSINT-аналітика може допомагати швидше перевіряти повідомлення, виявляти загрози, уточнювати ситуацію та зменшувати залежність від неперевірених інформаційних сигналів.

Чітка методологія потрібна тому, що лише частина великого обсягу доступної інформації є справді релевантною, своєчасною та практично корисною для OSINT-аналітика. Визначення того, яка інформація має більшу або меншу

цінність, потребує значних зусиль на всіх етапах: від початкового збору до поширення результатів і їх отримання особою, яка ухвалює рішення. Перетворення відкритої інформації на аналітичний продукт передбачає перевірку джерел, оцінку достовірності, встановлення контексту і розуміння того, як саме ці дані можуть бути використані. Саме тому OSINT-аналітика у сфері воєнної безпеки потребує не випадкового пошуку, а чіткої методичної послідовності [65, с. 25].

У межах цього дослідження доцільно зупинитися на чотирьох ключових етапах OSINT-аналітики: зборі, обробці, експлуатації та виробництві аналітичного продукту [65, с. 13]. При цьому обробка та експлуатація не завжди відбуваються строго послідовно; в окремих випадках вони можуть здійснюватися паралельно. Спрощено ці етапи можна описати як отримання інформації, перевірку цієї інформації, визначення її цінності та надання результату кінцевому споживачу.

Перший етап - збір інформації. Він включає визначення потенційно корисної інформації та її збереження для подальшої роботи. Цей етап потребує чітких вказівок для осіб, які працюють з відкритими джерелами: яку саме інформацію потрібно збирати, за якими критеріями, у який строк і для якої інформаційної потреби. У сфері воєнної безпеки це може стосуватися повідомлень про переміщення військ, появу техніки, наслідки ударів, активність окупаційних адміністрацій, інформаційні операції або цифрові сліди, які можуть мати безпекове значення.

Другий етап - обробка інформації. Він передбачає первинну перевірку, очищення, систематизацію та агрегацію зібраних даних. Агрегація не завжди є необхідною для традиційних новинних матеріалів або “сірої літератури”, але вона є важливою для аналізу соціальних мереж, особливо короткоформатного контенту. Окремі повідомлення в Telegram, TikTok, Twitter/X або Facebook можуть мати обмежену цінність самі по собі, але в поєднанні з іншими повідомленнями, геолокацією, часом публікації, фото-, відеоматеріалами або супутниковими знімками вони можуть створювати більш повну картину.

Третій етап - експлуатація, яку також можна розглядати як аналітичне опрацювання інформації. На цьому етапі необхідно визначити якість інформації, відокремити більш надійні дані від сумнівних, оцінити джерело, перевірити контекст і зрозуміти, яке значення має знайдена інформація. Аналітик повинен не лише збирати й сортувати дані, а й розуміти їхні обмеження, можливі ризики маніпуляції, потреби кінцевого користувача, інформаційний потік, організаційний контекст і правові межі використання відкритої інформації [65, с. 32]. У цьому сенсі експлуатація включає автентифікацію, оцінку достовірності та контекстуалізацію.

Автентифікація дозволяє встановити, чи є інформація справжньою, чи не була вона змінена, вирвана з контексту або повторно використана для іншої події. Оцінка достовірності допомагає визначити, наскільки можна довіряти конкретному джерелу і конкретному повідомленню. Контекстуалізація дає змогу зрозуміти, що саме означає отримана інформація для конкретної ситуації. Для воєнної безпеки це особливо важливо, бо одне й те саме повідомлення може мати різне значення залежно від часу, місця, джерела, попередніх подій і ширшого інформаційного середовища.

На завершальному етапі - етапі виробництва - результат OSINT-аналітики подається споживачу у формі, зручній для використання. Таким споживачем може бути аналітик розвідки з усіх джерел, командир, управлінська структура, державний орган, дослідницька інституція або інший суб’єкт, який потребує перевіреної інформації для ухвалення рішення. У частині випадків OSINT-матеріал використовується як один із елементів ширшого розвідувального продукту. В інших випадках результат OSINT-аналітики може бути достатньо обґрунтованим, щоб безпосередньо підтримати рішення у сфері воєнної безпеки.

Отже, організація OSINT-аналітики у сфері воєнної безпеки передбачає не лише доступ до відкритих джерел, а й дотримання чіткої послідовності роботи: від формулювання інформаційної потреби до підготовки кінцевого аналітичного продукту. Для України це має особливе значення в умовах російсько-української війни, де швидкість, достовірність і правильна інтерпретація відкритих даних

можуть впливати на ситуаційну обізнаність, оцінку загроз і якість рішень на різних рівнях воєнної безпеки.

2.2. Переваги OSINT-аналітики та можливості штучного інтелекту для підтримки рішень у сфері воєнної безпеки України

Переваги OSINT-аналітики для України варто розглядати через конкретні потреби війни. У цьому підрозділі йдеться не просто про те, що відкриті джерела дають багато інформації, а про те, як ця інформація може допомогти в реальній безпековій роботі: швидко перевірити повідомлення, уточнити обстановку, побачити цифрові сліди противника, зіставити фото, відео, супутникові знімки, повідомлення у соціальних мережах та інші відкриті дані. Для воєнної безпеки України це має значення саме тому, що в умовах війни рішення часто доводиться готувати тоді, коли повної картини ще немає, а інформаційний простір уже переповнений повідомленнями, чутками й дезінформацією.

Один із відомих прикладів використання OSINT у воєнній сфері пов’язаний із встановленням місцезнаходження командного пункту Ісламської держави Іраку та Сирії. У 2015 році бойовик ІДІЛ опублікував фотографію командного пункту в соціальних мережах, після чого ця інформація була використана для його виявлення. Цей приклад часто згадують саме тому, що він добре показує просту річ: у сучасній війні навіть одна необережна публікація у відкритому середовищі може мати практичне значення.

Для України це не абстрактний приклад. У російсько-українській війні подібну роль відіграють публікації російських військових, фото і відео з місць подій, повідомлення у Telegram, TikTok, YouTube, Twitter/X, а також цифрові сліди, які залишають самі учасники війни або пов’язані з ними особи. Наприклад, українська приватна розвідувально-аналітична компанія Molfar використовує відкриті інтернет-джерела для розслідувань, зокрема для ідентифікації російських військових і підрозділів на основі публікацій у соціальних мережах. Для теми воєнної безпеки України цей приклад важливий тим, що відкриті дані

можуть працювати не тільки як новина, а як матеріал для перевірки противника, документування його дій і кращого розуміння ситуації.

Ці приклади показують, чому OSINT-аналітика має окрему цінність порівняно з класичними способами отримання інформації. Йдеться не про те, що відкриті джерела кращі за закриті, а про те, що вони можуть швидше дати перший орієнтир, допомогти перевірити повідомлення або підтвердити те, що вже відомо з інших каналів. Американський дослідник розвідувальної діяльності А. Сендс визначив п’ять факторів, які OSINT пропонує порівняно із закритими джерелами розвідки: систему оцінки, захист закритих матеріалів, достовірність, легкий доступ та вдосконалену методологію оцінки [56, с. 63-78].

В українських умовах ця логіка має практичне значення. В стані війни відкриті джерела можуть не тільки доповнювати закриту інформацію, а й допомагати швидше зрозуміти, чи є повідомлення важливим, чи воно є повтором, помилкою або елементом інформаційного шуму. Тобто OSINT-аналітика працює як додатковий шар перевірки і контексту, а не як окрема “чарівна” система отримання істини.

Британський дослідник розвідувальних систем і безпекових організацій С. Гібсон також розглядає OSINT не як другорядну діяльність, а як частину ширшої розвідувальної функції. Він виокремлює сім факторів, через які відкриті джерела можуть бути корисними для розвідки, безпекових організацій, правоохоронних структур і навіть корпоративного сектору [39].

Контекст. Відкриті джерела дають загальний фон, без якого складно оцінювати окрему подію. У літературі це описують як “перший порт заходу”, “фон” або “контекстуальний матеріал” [55, с. 741-742]. У цьому сенсі для України це добре видно у війні: одне повідомлення саме по собі може нічого не означати, але в поєднанні з іншими джерелами воно допомагає зрозуміти, що саме відбувається.

Фактор - корисність. OSINT часто дає інформацію швидше і дешевше, ніж закриті способи її отримання. Його перевага не в тому, що він завжди точніший, а в тому, що він може швидко дати первинний орієнтир. В умовах війни це

важливо, бо інколи потрібно не чекати повної картини, а швидко зрозуміти, чи є подія реальною і чи потребує вона подальшої перевірки.

Розглядаючи орієнтир. Відкриті джерела можуть підказати, куди саме варто спрямувати подальший аналіз. Якщо певна інформація вже є у відкритому доступі й підтверджується кількома джерелами, немає сенсу витрачати ресурси на її повторне здобуття закритими методами. Для воєнної безпеки України це означає, що OSINT може допомагати відділяти справді важливі питання від другорядних.

“Сплеск”. Закриту розвідку неможливо швидко “увімкнути” там, де раптово виникла нова проблема. Відкриті джерела вже існують у цифровому середовищі, тому їх можна швидко залучити під час різкої зміни обстановки. У ситуації російсько-української війни це особливо помітно під час масованих обстрілів, змін на фронті або подій на окупованих територіях, коли перша картина часто складається саме з відкритих повідомлень.

Підходячи до Фокусу. OSINT допомагає не тільки збирати інформацію, а й звужувати поле пошуку. Він показує, які повідомлення варто перевіряти, які джерела можуть бути корисними, а які лише створюють шум. У російсько-українській війні це має значення, бо інформаційний простір постійно перевантажений повідомленнями, частина з яких є помилковими або навмисно маніпулятивними.

Комунікабельність. Інформацією з відкритих джерел зазвичай легше ділитися, ніж матеріалами, отриманими закритими способами. Це спрощує передачу частини аналітичних матеріалів між державними структурами, волонтерськими ініціативами, аналітичними центрами та міжнародними партнерами. Але у українському практичному вимірі тут є важливе обмеження: навіть відкрита інформація може стати небезпечною, якщо її поширювати без урахування безпеки.

Аналіз. Головна цінність OSINT не в самому зборі даних, а в тому, що з них можна зробити зрозумілий аналітичний продукт. Це можуть бути огляди, бази знань, карти, попередження, індикатори загроз або матеріали для подальшої

перевірки. Для воєнної безпеки України така аналітика важлива тоді, коли вона допомагає не просто знати більше, а краще розуміти ситуацію і готувати рішення.

Отже, переваги OSINT-аналітики не зводяться лише до того, що джерела є відкритими. Її сила в іншому: швидко знайти сигнал, перевірити його, зіставити з іншими даними і перетворити на матеріал, який може бути корисним для рішення. Для України це особливо важливо, бо під час війни інформаційний простір одночасно дає і цінні свідчення, і велику кількість шуму, повторів, чуток та дезінформації.

Окремо треба згадати про “туман війни”. OSINT-аналітика справді може частково його зменшувати, але не прибирає повністю. У війні завжди є невизначеність: частина інформації закрита, частина запізнюється, частина спеціально викривлюється противником. Відкриті джерела в цій ситуації можуть дати перші сигнали: фото, відео, повідомлення у Telegram, TikTok, Twitter/X, супутникові знімки, цифрові карти, публікації місцевих мешканців або навіть самих російських військових.

Дослідники Г. ван Бік і С. Ріт’єнс, які досліджують роль відкритих джерел у російсько-українській війні, пишуть про цю війну як про один із показових прикладів використання OSINT у сучасному конфлікті [63, с. 57-76]. Важливо, що тут працюють не тільки державні структури. Значну роль відіграють OSINT-спільноти, журналісти-розслідувачі, волонтери, аналітичні центри, приватні компанії. Для України це плюс, бо такі суб’єкти часто швидше фіксують події, перевіряють відео, знаходять геолокацію, документують дії противника і дають матеріал для ширшого аналізу.

Але OSINT не варто переоцінювати. О. Крпец, М. Чованчик та А. Ілавська, які аналізують OSINT на стратегічному рівні війни, більш обережно оцінюють його можливості [47]. Відкриті джерела можуть допомогти перевірити окремі факти, але вони не завжди показують наміри противника, приховані процеси або реальний стан складних військово-промислових систем. Тому для воєнної

безпеки України OSINT-аналітика має бути не заміною іншим джерелам, а способом їх доповнення і перевірки.

Разом із тим переваги OSINT не варто плутати з автоматичною точністю. Великий масив відкритої інформації може допомогти швидше побачити сигнал, але він так само може затягнути аналітика в повтори, чутки, пропаганду або емоційні повідомлення. Для воєнної безпеки України цінність має не сам факт наявності відкритих даних, а здатність відібрати з них те, що справді допомагає зрозуміти ситуацію і підготувати рішення. Саме тут з'являється питання використання штучного інтелекту та автоматизованих інструментів.

У цьому контексті важливими стають геоінформаційні системи, супутникові знімки, комп'ютерний зір, машинне навчання та інші інструменти, які допомагають працювати з великими масивами відкритих даних. Наприклад, програмне забезпечення ГІС може використовуватися для визначення районів України, забруднених боєприпасами, що не розірвалися, і для встановлення пріоритетів розмінування. Інші приклади стосуються витягування інформації з неструктурованих текстових даних, аналізу комерційних супутникових знімків, оцінки пошкоджень інфраструктури або прогнозування розвитку подій за різними сценаріями. Усі ці напрями показують, що штучний інтелект і машинне навчання можуть посилювати OSINT-аналітику, але лише тоді, коли вони працюють разом із людською перевіркою та розумінням воєнного контексту України.

Після повномасштабного вторгнення 2022 року Telegram став одним із головних майданчиків, де швидко поширюється інформація про російсько-українську війну. Йдеться не тільки про офіційні канали, а й про російські пропагандистські ресурси, воєнкорів, локальні спільноти, канали окупаційних адміністрацій, OSINT-стрічки та канали лідерів думок. Для воєнної безпеки України такі дані можуть бути корисними, бо вони дозволяють відстежувати зміни в російському інформаційному середовищі, бачити появу нових наративів, фіксувати реакції на події війни або виявляти інформаційні кампанії. Проблема в тому, що вручну опрацювати такий масив повідомлень майже неможливо.

Одним із прикладів інструментів для такої роботи є ExTrac [104]. Ця система відстежує контент і онлайн-комунікації учасників конфлікту в режимі реального часу та в ретроспективі. Щоб зменшити інформаційний шум, вона використовує підхід “людина в циклі”, тобто працює не з усім масивом випадкових повідомлень, а з джерелами, які попередньо відібрали аналітики. Це важливо, бо в умовах війни автоматизація без людського контролю може швидко почати обробляти не лише корисні дані, а й пропаганду, повтори або навмисні вкиди.

Можливості ExTrac спочатку тестувалися на масиві з 427 груп і Telegram-каналів, серед яких були сепаратистські форуми, OSINT-орієнтовані стрічки, російські воєнні канали та медійні ресурси, пов’язані з воєнізованими структурами. Для українського контексту цей приклад показує, що ШІ та автоматизовані інструменти можуть бути корисними не лише для пошуку окремих фактів, а й для спостереження за інформаційним середовищем противника. Проте кінцевий висновок усе одно має робити аналітик, який розуміє мову, контекст, пропагандистські прийоми та логіку російського інформаційного простору.

Такі технології поступово стають доступнішими не лише для технічних фахівців, а й для аналітиків, які працюють із відкритими джерелами. Їхня головна перевага - швидкість. Вони можуть знаходити повтори, тенденції, аномалії або зв’язки в таких масивах даних, які людина вручну просто не встигла б переглянути. Для OSINT-аналітики у сфері воєнної безпеки України найбільш помітними є три напрями використання машинного навчання: робота з текстом, аналіз зображень і прогнозування.

Перший напрям - робота з текстовими даними. Великі мовні моделі можуть допомагати OSINT-аналітикам опрацьовувати повідомлення в Telegram, пости у Twitter/X, новинні матеріали, офіційні заяви, коментарі, чати або неструктуровані бази даних. Їх можна використовувати для швидкого узагальнення матеріалів, попереднього групування повідомлень, пошуку

повторюваних тем, перекладу, виділення імен, назв організацій, географічних об’єктів або ключових наративів.

В українських умовах це особливо корисно під час аналізу російського інформаційного простору. Такі інструменти можуть допомагати швидше побачити, які теми просуваються російськими пропагандистськими каналами, як змінюється риторика після конкретних подій на фронті, які повідомлення повторюються різними каналами і які наративи спрямовані на українську або західну аудиторію. Але тут є серйозне обмеження: Telegram і соціальні мережі не пишуть мовою академічних статей. Там є сленг, меми, помилки, іронія, приховані натяки, пропагандистські кліше та свідомі маніпуляції. Тому мовна модель може допомогти з первинною обробкою, але результат усе одно має перевіряти людина, яка розуміє контекст війни і специфіку російської інформаційної кампанії.

Другий напрям - аналіз зображень. Для OSINT це дуже важливо, бо значна частина інформації про війну існує не у вигляді тексту, а у вигляді фото, відео та супутникових знімків. Моделі комп’ютерного зору можуть допомагати знаходити на зображеннях певні об’єкти, порівнювати кадри, попередньо визначати тип техніки, аналізувати пошкодження інфраструктури або швидко відбирати матеріали, які потребують ручної перевірки.

У російсько-українській війні таких матеріалів дуже багато: фото й відео наслідків ударів, пересування техніки, руйнування цивільної інфраструктури, активність окупаційних адміністрацій, події на тимчасово окупованих територіях. Людина-аналітик фізично не завжди може швидко переглянути великий масив таких даних. Тому комп’ютерний зір варто розглядати як перший фільтр. Він не робить остаточний висновок, але допомагає звузити обсяг ручної роботи.

Окреме значення має автоматизована геолокація та попереднє визначення часу зйомки. Нові моделі вже можуть припускати, де і коли було зроблено зображення, хоча до рівня досвідченого OSINT-аналітика вони ще не доходять. Для України це все одно важливо, бо кадровий ресурс обмежений, а кількість

цифрових матеріалів величезна. Тому такі інструменти доцільно використовувати як допоміжний етап: спочатку вони сортують матеріал і підказують можливі варіанти, а потім людина перевіряє місце, час, джерело і контекст.

Третій напрям – прогнозування. Тут йдеться не про точне передбачення майбутнього, а про спробу на основі відкритих даних побачити можливі тенденції: де може зрости напруга, які інформаційні теми можуть посилюватися, як змінюється активність певних груп або які події можуть повторюватися за подібних умов. Для цього можуть використовуватися відкриті набори даних про конфлікти, повідомлення в соціальних мережах, новинні публікації, геопросторові дані та інші цифрові сліди[35, с. 391-406; 52, с. 801-823] .

У сфері воєнної безпеки України прогнозування на основі OSINT може бути корисним, але до нього треба ставитися обережно. Такі інструменти можуть допомагати бачити тенденції в російському інформаційному середовищі, фіксувати зміну риторики, відстежувати повторювані інформаційні кампанії або оцінювати ризики на окремих напрямах. Але прогноз не є фактом. Він залежить від якості даних, методики, контексту і того, чи правильно аналітик розуміє обмеження моделі [35, с. 391-406; 104].

Саме тому штучний інтелект у OSINT-аналітиці не варто розглядати як заміну людині. Його сильна сторона - швидкість обробки великих масивів інформації. Він може знайти повтори, згрупувати повідомлення, виділити об’єкти на зображеннях, допомогти з перекладом або підказати можливі закономірності. Але остаточне значення цих даних має визначати аналітик. У воєнній сфері особливо небезпечно покладатися лише на автоматичний висновок, бо помилка може призвести до неправильного розуміння ситуації.

Отже, штучний інтелект у OSINT-аналітиці важливий не тому, що він може сам ухвалювати рішення, а тому, що допомагає швидше працювати з великими масивами відкритих даних. Для України це має значення через масштаб російсько-української війни, кількість цифрових матеріалів, активність російської пропаганди та постійну потребу швидко перевіряти інформацію.

Водночас ШІ не можна сприймати як джерело остаточної істини. Він має працювати як допоміжний інструмент, а остаточний висновок повинен залишатися за аналітиком, який розуміє воєнний контекст, джерела, ризики дезінформації та обмеження самої моделі. Саме поєднання автоматизованої обробки, людської перевірки й методичної OSINT-аналітики може реально посилювати підтримку рішень у сфері воєнної безпеки України.[2, с. 21; 35, с. 391-406]

2.3. Тактичний і локальний рівні застосування OSINT-аналітики в умовах російсько-української війни

На тактичному й локальному рівнях OSINT має більш прикладний характер, ніж стратегічний аналіз. Тут важливі не великі узагальнення, а конкретні фрагменти: фото, коротке відео, повідомлення в Telegram, частина карти, цифровий слід або публікація з місця події. Але сам факт появи такого матеріалу ще нічого не доводить. У розвідувальній діяльності цінність має не просто обсяг зібраної інформації, а конкретні дані, підтверджені різними джерелами [74, с. 77].

У російсько-українській війні це видно дуже чітко. Відео з TikTok або Telegram може бути старим, вирваним з контексту або поданим як доказ зовсім іншої події. Тому локальний OSINT починається не з довіри до першого повідомлення, а з перевірки. Чи справді це те місце? Чи відповідає воно заявленому часу? Чи не було це відео опубліковане раніше? Лише після таких питань окремий цифровий фрагмент може мати аналітичну цінність.

Тактичний рівень у цьому підрозділі варто розуміти як роботу з конкретною ділянкою, районом або подією. Це не прогнозування війни загалом, а швидке уточнення обстановки: де сталася подія, які є відкриті підтвердження, що видно на фото чи відео, чи є зв’язок з іншими повідомленнями. У такому форматі OSINT не замінює військове управління або закриту розвідку, але може

доповнювати ситуаційну обізнаність і допомагати швидше відділяти важливе від інформаційного шуму.

Найпростіший приклад - геолокація фото і відео. Для цього аналітики дивляться не тільки на сам об’єкт у кадрі, а й на дрібні деталі: дорожні знаки, лінії електропередач, форму будівель, рельєф, тіні, погоду, карти, супутникові знімки або панорами місцевості. Саме такі ознаки часто дозволяють зрозуміти, чи відповідає матеріал реальному місцю і часу.

Для українських умов це має практичний сенс під час перевірки повідомлень про наслідки ударів, переміщення техніки, руйнування інфраструктури, події на окупованих територіях або активність окупаційних адміністрацій. Подібну логіку демонструють Bellingcat та інші OSINT-спільноти: вони не спираються на одне фото чи відео, а зіставляють його з іншими відкритими джерелами. У цьому й полягає базове правило локального OSINT: цифровий фрагмент стає цінним не сам по собі, а після перевірки й включення в ширший контекст.

Окремо можна згадати картографування ситуації. У російсько-українській війні це видно на прикладі публічних карт, зокрема DeepState, де відкриті повідомлення, фото, відео та інші сигнали після перевірки можуть перетворюватися на зрозумілу візуалізацію ситуації. Такі карти не є офіційним військовим джерелом, але вони показують, як OSINT може допомагати бачити просторовий контекст подій і динаміку бойових дій.

Подібна логіка працює і щодо тимчасово окупованих територій. Там відкриті джерела часто залишаються одним із небагатьох способів отримати хоча б часткове уявлення про ситуацію: заяви окупаційних адміністрацій, місцеві Telegram-канали, відео з місць подій, супутникові знімки, російські пропагандистські матеріали. Українські та міжнародні OSINT-ініціативи, зокрема InformNapalm, Molfar, Cyber Resistance і Bellingcat, використовують такі дані для перевірки окремих епізодів війни, ідентифікації російських військових або документування дій противника. Але відкриті джерела тут не можна брати

на віру: поряд із корисними свідченнями є фейки, повтори, пропаганда й інформаційні пастки.

Окремо варто розглянути фітнес-додатки - Strava, Polar, Suunto та подібні сервіси. Формально вони створені для спорту: фіксації тренувань, маршруту, часу активності, фізичних показників, коментарів або фото. Але фактично такі додатки давно стали ще й соціальними платформами. Користувачі самі відкривають частину даних, часто не думаючи, що маршрут пробіжки або регулярне місце тренування може мати безпекове значення.

Для військовослужбовців, працівників сектору безпеки або людей, які перебувають у районах службового розгортання, це створює очевидні OPSEC-ризики. У 2017 році Strava оприлюднила глобальні “теплові карти” тренувань користувачів. Після цього дослідники звернули увагу, що повторювані маршрути у віддалених районах можуть вказувати на військові об’єкти або місця розміщення персоналу [75; 76]. Пізніше схожі ризики обговорювалися щодо Polar і Suunto, де відкриті профілі могли розкривати маршрути, регулярність пересування або інші чутливі деталі [77; 78].

Ці приклади важливі не лише як історії про окремі додатки. Насправді вони показують ширшу проблему операційної безпеки: люди часто самі залишають у відкритому цифровому середовищі більше даних, ніж усвідомлюють. Для України в умовах війни це має пряме значення, оскільки військовослужбовці, працівники сектору безпеки, волонтери, журналісти або цивільні можуть несвідомо відкривати місце перебування, маршрути, звички або зв’язки.

Польський дослідник Інституту стратегічних студій Університету воєнних студій у Варшаві Ц. А. Козера окремо аналізував ризики використання фітнес-додатків військовослужбовцями та співробітниками сектору безпеки [79]. У його прикладах йдеться не про складні технічні злами, а про відкриті тренувальні дані, профілі, фотографії, маршрути та зв’язки з іншими соціальними мережами. У сукупності такі дрібні фрагменти можуть розкривати місця службового перебування, регулярні маршрути, належність до певного середовища або інші чутливі цифрові сліди.

Для локального OSINT це показовий приклад: один маршрут або одна фотографія можуть здаватися незначними, але після зіставлення з іншими джерелами вони дають набагато більше інформації. Саме тому фітнес-додатки в цьому підрозділі варто розглядати не як окрему технологічну цікавинку, а як приклад того, як побутові цифрові сервіси можуть створювати ризики для операційної безпеки.

Наведені приклади показують, що фітнес-додатки є лише частиною ширшої проблеми цифрових слідів. Вони не замінюють інші види розвідки, але можуть доповнювати їх, якщо дані з додатків зіставляються з соціальними мережами, картами, фотографіями та іншими відкритими джерелами. Для OSINT-аналітика цінність тут не в одному маршруті чи одному профілі, а в тому, що кілька дрібних фрагментів разом можуть створити більш повне уявлення про людину, об’єкт або місце.

Для України цей приклад має попереджувальне значення. У сучасній війні відкритість цифрового середовища створює ризики не лише для противника, а й для власних військовослужбовців, підрозділів, волонтерів, журналістів і цивільних. Публічні маршрути, фото з географічними ознаками, регулярна поява в одному місці або необережні дописи можуть розкривати чутливу інформацію. Тому локальний OSINT варто розглядати не тільки як інструмент пошуку й перевірки даних, а й як підставу для посилення культури операційної безпеки.

Отже, на тактичному й локальному рівнях OSINT-аналітика має практичне значення саме через роботу з конкретними фрагментами інформації. Геолокація фото й відео, картографування ситуації, моніторинг окупованих територій, документування дій противника та аналіз цифрових слідів можуть посилювати ситуаційну обізнаність у сфері воєнної безпеки України. Водночас ці самі відкриті дані можуть створювати ризики, якщо їх залишають безконтрольно. Тому ефективне використання OSINT на цьому рівні потребує не лише технічних навичок, а й дисципліни, перевірки джерел і розуміння меж відкритої інформації.

Висновки до розділу ІІ

У другому розділі було розглянуто OSINT-аналітику як практичний інструмент посилення воєнної безпеки України. У підрозділі 2.1 було визначено організаційну та методичну послідовність проведення OSINT-аналітики у сфері воєнної безпеки. На прикладі досвіду США було показано, що ефективне використання відкритих джерел потребує не лише окремих фахівців, а й організаційного закріплення, навчання, визначених посад, процедур і швидкої передачі результатів тим, хто ухвалює рішення. Для України цей досвід важливий не як модель для механічного копіювання, а як приклад того, що OSINT має розглядатися як частина системної аналітичної роботи у сфері воєнної безпеки.

У підрозділі 2.2 було проаналізовано переваги OSINT-аналітики та можливості штучного інтелекту. Було встановлено, що переваги OSINT полягають у швидкості доступу до інформації, можливості перевірки даних через кілька джерел, формуванні ситуаційної обізнаності та доповненні інших видів розвідки. Водночас відкриті джерела не можна сприймати як автоматично достовірні. В умовах російсько-української війни вони містять не лише корисні свідчення, а й фейки, повтори, пропаганду та навмисні інформаційні вкиди. Тому практичне значення має не сам обсяг відкритої інформації, а здатність аналітика відокремити корисний сигнал від інформаційного шуму.

Окремо було показано, що штучний інтелект може посилювати OSINT-аналітику, але не замінює людину. Інструменти машинного навчання, обробки природної мови, комп’ютерного зору й прогнозування можуть допомагати швидше працювати з великими масивами відкритих даних, виявляти повтори, групувати повідомлення, аналізувати зображення або помічати певні тенденції. Проте остаточний висновок має залишатися за аналітиком, який розуміє воєнний контекст, джерела, ризики дезінформації та обмеження самої моделі.

У підрозділі 2.3 було розглянуто тактичний і локальний рівні застосування OSINT-аналітики в умовах російсько-української війни. Було показано, що на цих рівнях значення мають не стільки великі узагальнення, скільки конкретні

фрагменти інформації: фото, відео, повідомлення в Telegram або TikTok, фрагменти карт, цифрові сліди, супутникові знімки, відкриті профілі чи публікації з місця події. Такі дані можуть бути корисними лише після перевірки, геолокації, зіставлення з іншими джерелами та включення в ширший контекст.

Таким чином, у розділі було доведено, що OSINT-аналітика може реально посилювати воєнну безпеку України, якщо вона використовується методично, обережно й у поєднанні з іншими джерелами інформації. Її практична цінність проявляється у підтримці рішень, уточненні обстановки, документуванні дій противника, моніторингу окупованих територій, підвищенні ситуаційної обізнаності та виявленні ризиків операційної безпеки. Водночас OSINT не є самодостатньою або безпомилковою системою. Він потребує критичного мислення, перевірки джерел, цифрової дисципліни й розуміння того, що відкритість інформації одночасно створює і можливості, і загрози.

РОЗДІЛ ІІІ
МЕТОДИ ТА ІНСТРУМЕНТИ OSINT-АНАЛІТИКИ У СФЕРІ ВОЄННОЇ БЕЗПЕКИ УКРАЇНИ

У третьому розділі пройдемо від загального пояснення OSINT до того, як ця робота виглядає на практиці. Для України це не теоретичне питання. Під час війни постійно виникає потреба перевіряти повідомлення, фото, відео, карти, супутникові знімки, Telegram-канали, відкриті реєстри й цифрові сліди.

Наприклад, у відкритому доступі з'являється відео після обстрілу або повідомлення з окупованої території. Самого повідомлення недостатньо. Потрібно зрозуміти, хто його опублікував, коли воно з'явилося, чи не було це старе відео, чи збігається місцевість із картою, чи є підтвердження з інших джерел.

Тому в цьому розділі інструменти OSINT розглядаються як допоміжні засоби для перевірки інформації. Один інструмент допомагає знайти першоджерело, інший - перевірити місце, ще інший - зберегти матеріал або показати зв'язки між даними. Саме їх поєднання має практичне значення для воєнної безпеки України.

3.1. Відкриті та комерційні інструменти OSINT-аналітики для збору, перевірки й візуалізації інформації

У практичній OSINT-аналітиці інструменти мають значення лише тоді, коли зрозуміло, яку саме задачу вони мають вирішити. Один сервіс може бути корисним для пошуку першоджерела відео, інший - для перевірки геолокації, третій - для аналізу супутникового знімка, четвертий - для візуалізації даних на карті. Тому у сфері воєнної безпеки України інструменти OSINT варто розглядати не як окремий "набір програм", а як частину аналітичного процесу: що шукаємо, звідки беремо дані, як перевіряємо, як зіставляємо і в якому вигляді передаємо результат.

У російсько-українській війні така логіка особливо помітна. Повідомлення про удар, переміщення техніки, активність окупаційної адміністрації або новий інформаційний вкид РФ саме по собі ще не є готовим аналітичним висновком. Його потрібно перевірити: знайти першоджерело, встановити час появи, порівняти з іншими повідомленнями, звірити з картою або супутниковим знімком, оцінити, чи не використовується старе фото під виглядом нової події.

Умовно такі інструменти можна поділити на кілька груп: пошукові системи й відкриті реєстри; сервіси для аналізу соціальних мереж і Telegram; інструменти геолокації фото та відео; карти й геоінформаційні системи; супутникові сервіси; платформи для візуалізації та побудови зв'язків; засоби архівації й перевірки цифрового сліду. Для воєнної безпеки України важливе не саме володіння цими інструментами, а здатність правильно поєднувати їх між собою.

Першу групу становлять пошукові системи, відкриті реєстри та архіви вебсторінок. На перший погляд, це найпростіші інструменти OSINT, але саме з них часто починається перевірка інформації. У сфері воєнної безпеки України вони можуть використовуватися для пошуку першоджерела повідомлення, перевірки дати публікації, встановлення походження фото або відео, порівняння заяв різних сторін, а також для пошуку додаткових підтверджень у відкритому інформаційному полі.

Пошукові системи дають змогу швидко побачити, чи з'являлася певна інформація раніше, хто її поширював і в якому контексті. Наприклад, якщо у Telegram або російських медіа з'являється повідомлення про нібито нову подію, першим кроком може бути перевірка, чи не використовувалися ті самі фото, відео або формулювання раніше. Для російсько-української війни це важливо, бо противник часто використовує старі матеріали, вирвані з контексту кадри або повторно поширює вже відомі сюжети як "нові докази".

Окреме значення мають відкриті реєстри й офіційні бази даних. Вони можуть бути корисними для перевірки організацій, компаній, публічних осіб, санкційних зв'язків, судових рішень, державних закупівель або офіційних

повідомлень. У контексті воєнної безпеки України такі джерела можуть допомагати перевіряти інформацію про структури, пов’язані з державою-агресором, окупаційними адміністраціями, постачанням товарів подвійного призначення або інформаційними кампаніями. Водночас дані з реєстрів також потребують обережного тлумачення: сама наявність запису ще не завжди означає наявність прямого зв’язку чи причетності.

Корисними є й архіви вебсторінок, оскільки відкритий інтернет постійно змінюється. Сайти видаляють матеріали, змінюють формулювання, приховують старі публікації або переносять сторінки. Архівні копії дозволяють побачити, як виглядала сторінка раніше, чи змінювалася позиція певного ресурсу, коли саме була опублікована інформація і чи не було її відредаговано після події. Для OSINT-аналітики це важливо, бо іноді саме зміна або видалення публікації може бути додатковим сигналом для перевірки.

Після пошукових систем і реєстрів окремо треба виділити соціальні мережі, месенджери та відкриті цифрові платформи. У російсько-українській війні саме там часто з’являється перша інформація про подію: коротке відео після удару, повідомлення місцевих мешканців, допис російського воєнкора, заява окупаційної адміністрації або реакція пропагандистських каналів. Але для OSINT-аналітика важливий не сам факт появи такого повідомлення. Потрібно зрозуміти, хто його поширив, коли саме, чи було першоджерело, чи не повторює канал старий матеріал і чи підтверджується ця інформація іншими джерелами.

У цьому блоці окремо варто згадати Telegram, бо для російсько-української війни він став не просто месенджером. Через нього дуже швидко розходяться повідомлення з місць подій, заяви офіційних осіб, публікації російських воєнкорів, матеріали окупаційних адміністрацій і повідомлення OSINT-спільнот. Але саме швидкість робить Telegram проблемним джерелом. Там поруч можуть бути корисні свідчення, чутки, старі відео, емоційні дописи й навмисні інформаційні вкиди. Тому повідомлення з Telegram краще сприймати як привід для перевірки, а не як готовий доказ [63].

Інші платформи теж мають значення, але кожна працює по-своєму. У TikTok можуть з’являтися короткі відео з місць подій або пересування техніки. На YouTube частіше трапляються довші відео, інтерв’ю чи пропагандистські сюжети. У Twitter/X швидко реагують журналісти, аналітики та OSINT-спільноти. Facebook більше пов’язаний із локальними дописами, групами, коментарями очевидців. Для цієї роботи важливо інше: такі платформи дають не готовий висновок, а цифровий слід, який потім треба перевіряти через інші джерела.

Після соціальних мереж зазвичай постає питання місця. Наприклад, є відео після удару або фото з певним об’єктом. Треба зрозуміти, де це зроблено і чи відповідає воно заявленому району. Тут у роботу входять Google Maps, Google Earth, OpenStreetMap та інші картографічні сервіси. Вони допомагають звірити дорогу, міст, форму будівлі, залізницю, промисловий об’єкт, лінію електропередач або інші орієнтири. Карта в такому випадку не дає остаточної відповіді, але дозволяє перевірити версію.

Супутникові знімки потрібні тоді, коли треба подивитися на ситуацію ширше. Sentinel, Planet, Maxar та інші відкриті або комерційні сервіси можуть показати пожежі, руйнування, наслідки ударів, стан інфраструктури, будівництво нових об’єктів або зміни в районах, куди немає нормального доступу. Для України це особливо актуально щодо окупованих територій, наслідків російських обстрілів, критичної інфраструктури та зони бойових дій [[63, с. 57–76; 83; 89; 90]].

Якщо даних стає багато, звичайної карти вже мало. У таких випадках можуть використовуватися геоінформаційні системи, наприклад QGIS. Вони дають змогу накладати різні шари: дороги, межі, об’єкти інфраструктури, супутникові знімки, повідомлення з відкритих джерел або часові позначки. Це корисно не для того, щоб просто знайти точку на карті, а щоб побачити зв’язок між подією, місцем і кількома різними джерелами.

Після перевірки дані ще треба нормально подати. У роботі з OSINT це не завжди має бути великий текст. Іноді достатньо таблиці, карти, короткої

хронології або схеми зв’язків. Наприклад, якщо кілька Telegram-каналів одночасно розганяють однакове повідомлення, зручніше показати це не абзацами, а в таблиці: хто опублікував першим, хто повторив, які фото чи формулювання збігаються. Для українського контексту це корисно під час аналізу російських інформаційних кампаній, бо так швидше видно не тільки саме повідомлення, а й спосіб його поширення.

Ще один потрібний напрям - архівація відкритих матеріалів. У війні публікації часто швидко зникають: сторінку можуть видалити, відео закрити, допис відредагувати, канал перейменувати або прибрати старі матеріали. Тому для OSINT-аналітика важливо не тільки побачити повідомлення, а й зафіксувати його стан на певний момент часу. Для цього можуть використовуватися вебархіви, збережені копії сторінок, скриншоти, посилання на першоджерело, дата й час фіксації.

Для України це має практичне значення під час перевірки російських заяв, матеріалів окупаційних адміністрацій, повідомлень пропагандистських ресурсів або відео з місць подій. Якщо матеріал потім зникне або буде змінений, архівна копія дозволяє показати, що саме було опубліковано раніше. Але й тут потрібна обережність: скриншот сам по собі не завжди є достатнім доказом, тому його бажано підкріплювати посиланням, архівною копією або іншими відкритими джерелами.

Отже, інструменти OSINT у сфері воєнної безпеки України варто оцінювати не за кількістю сервісів, а за тим, чи допомагають вони перевірити конкретну інформацію. Пошук, реєстри, соціальні мережі, карти, супутникові знімки, архіви й візуалізація працюють найкраще тоді, коли використовуються разом. Один інструмент може дати лише фрагмент, але поєднання кількох джерел дозволяє краще зрозуміти подію, її місце, час, контекст і можливе значення для ухвалення рішень.

3.2. Проблеми використання OSINT-інструментів у воєнній безпеці: достовірність даних, обмеження доступу та ризики помилкової інтерпретації

Попри практичну користь OSINT-аналітики, її використання у сфері воєнної безпеки України має низку проблем. Відкриті джерела не є “чистим” і повністю надійним середовищем. У них одночасно містяться корисні дані, помилки, чутки, пропаганда, повтори старих матеріалів і навмисні інформаційні вкиди. Тому головна складність полягає не тільки в тому, щоб знайти інформацію, а в тому, щоб зрозуміти, чи можна їй довіряти.

Перша проблема - інформаційний шум. Під час російсько-української війни повідомлення про події з’являються дуже швидко: у соцмережах, на сайтах новин, у російських пропагандистських ресурсах або місцевих каналах. Частина таких повідомлень справді може містити важливі свідчення. Але поряд із ними поширюються старі відео, фото з іншого місця, неточні підписи, емоційні коментарі або матеріали, спеціально подані так, щоб створити неправильне враження.

Для OSINT-аналітика це означає, що швидкість не може бути важливішою за перевірку. Якщо повідомлення з’явилося першим, це ще не означає, що воно правильне. Його потрібно звіряти з іншими джерелами: картою, супутниковим знімком, датою публікації, архівною копією, попередніми повідомленнями або офіційною інформацією. У воєнних умовах помилка в такій перевірці може створити хибне уявлення про ситуацію.

Друга проблема пов’язана з фото- і відеоматеріалами. На перший погляд, вони виглядають переконливо, бо ніби показують подію “як вона є”. Але в OSINT це не працює автоматично. Відео може бути старим, знятим в іншому місці, обрізаним, змонтованим або підписаним неправильно. Іноді достатньо змінити опис до ролика, щоб у глядача склалося зовсім інше враження про подію.

Для України це особливо важливо під час війни, коли в мережі швидко з’являються кадри після обстрілів, переміщення техніки, наслідків ударів або

подій на окупованих територіях. Якщо аналітик помилково визначить місце зйомки або час події, то весь подальший висновок буде слабким. Тому фото і відео потрібно перевіряти через деталі: місцевість, будівлі, дороги, дорожні знаки, лінії електропередач, погоду, тіні, метадані, карту або супутниковий знімок.

Окремий ризик - бажання швидко підтвердити вже готову версію. У такому випадку аналітик може помічати тільки ті деталі, які підходять під очікуваний висновок, і не звертати уваги на суперечності. Для OSINT це небезпечно, бо відкриті джерела часто дають неповну картину. Тому перевірка має йти не від бажаного висновку, а від питання: що саме цей матеріал реально доводить, а що лише припускається.

Окремо треба враховувати російську пропаганду. Вона не завжди працює через повністю вигадані повідомлення. Часто використовується реальне фото, реальне відео або справжня подія, але подається з потрібним для противника поясненням. Наприклад, матеріал може бути справжнім, а підпис до нього - неправдивим. Або подія могла відбутися, але її масштаб, причина чи наслідки спеціально перебільшуються.

Для OSINT-аналітика це означає, що не можна автоматично брати готову версію з російського каналу. Таке повідомлення може бути корисним тільки як сигнал для перевірки. Потрібно дивитися, хто опублікував матеріал першим, чи повторюють його інші канали, чи збігається місце, час, фото, відео і загальний контекст. У війні це важливо, бо російські джерела можуть одночасно давати частину реальної інформації і нав’язувати неправильний висновок.

Є ще одна межа, про яку не можна забувати. Те, що інформація відкрита, не означає, що її завжди можна безпечно поширювати далі. Фото з місця події, маршрут, відкритий профіль, коментар або відео можуть показати більше, ніж здається на перший погляд. У кадрі може бути місце, час, техніка, об’єкт інфраструктури або люди, яких не варто додатково підсвічувати.

Для України це особливо чутливо. Ризики стосуються не тільки військових, а й волонтерів, журналістів, працівників сектору безпеки, цивільних

біля фронту або людей в окупації. Тому OSINT-аналітика має відповідати не тільки на питання “чи це правда?”, а й на питання “чи не нашкодить публікація цих даних?”. Частину інформації можна використати для внутрішньої перевірки, але не виносити у відкритий текст.

Є ще одна річ, яка в OSINT часто недооцінюється: джерело може просто зникнути. Російський Telegram-канал опублікував заяву, а через кілька годин видалив її. Сайт змінив текст. Автор прибрав відео. Канал перейменувався. Якщо матеріал не зафіксувати одразу, потім складно показати, що саме було опубліковано і в якому вигляді.

Тому під час війни важливо зберігати цифровий слід: посилання, дату, час, скриншот, архівну копію або інше підтвердження. Це особливо стосується російських ресурсів, окупаційних каналів і пропагандистських майданчиків. Вони можуть змінювати формулювання після появи нових фактів або після того, як попередня версія стала невигідною.

Окремо треба враховувати людський фактор. Аналітик теж може помилитися: поспішити, повірити першому повідомленню, не перевірити першоджерело або прийняти повтор за незалежне підтвердження. Наприклад, кілька Telegram-каналів одночасно пишуть про одну подію. На перший погляд це виглядає як підтвердження. Але на практиці вони могли просто перепостити один і той самий початковий допис.

Є і проблема контексту. Російські воєнкори, окупаційні канали або місцеві групи часто використовують сленг, натяки, скорочення, іронію чи пропагандистські формули. Без розуміння цього середовища можна неправильно оцінити зміст повідомлення.

Отже, проблеми OSINT-аналітики у сфері воєнної безпеки України пов’язані не лише з пошуком інформації. Основні ризики виникають під час перевірки, тлумачення і подальшого використання відкритих даних. Інформаційний шум, старі фото й відео, російська пропаганда, зникнення джерел, людський фактор, а також різний доступ до інструментів можуть впливати на якість висновків. Тому OSINT має бути не швидким збором

повідомлень, а обережною перевіркою, де важливі джерело, контекст, час, місце і можливі наслідки публікації.

3.3. Перспективи використання штучного інтелекту й автоматизованих інструментів в OSINT-аналітиці для потреб воєнної безпеки України

Після розгляду інструментів і проблем OSINT-аналітики логічно перейти до питання, як цю роботу можна посилити в майбутньому. Для України це важливо через масштаб війни і кількість відкритої інформації. Щодня з'являються повідомлення в Telegram, відео в соціальних мережах, супутникові знімки, фото з місць подій, заяви російських джерел, матеріали окупаційних адміністрацій і повідомлення очевидців. Людина-аналітик не завжди може швидко переглянути такий обсяг даних вручну.

Саме тому перспективним напрямом є використання штучного інтелекту й автоматизованих інструментів. Йдеться не про те, що ШІ має самостійно ухвалювати рішення або замінювати аналітика. Його роль інша: швидше знаходити повтори, групувати повідомлення, перекладати тексти, виділяти імена, географічні назви, канали, організації або події. У такому форматі штучний інтелект може зменшити ручне навантаження і допомогти аналітику швидше перейти від хаотичного масиву повідомлень до перевірки конкретних фактів.

Для воєнної безпеки України це має практичний сенс. Наприклад, автоматизований аналіз може допомагати відстежувати російські інформаційні кампанії, повторювані наративи, активність окремих Telegram-каналів або появу однакових повідомлень у різних джерелах. Але результат такої обробки все одно має перевіряти людина, бо ШІ може помилятися, не розуміти контексту, плутати іронію, сленг або пропагандистські формули.

Перший напрям, де ШІ може бути корисним для OSINT, - робота з текстами. У війні це не тільки офіційні заяви чи новини. Це Telegram-дописи,

коментарі, короткі повідомлення, російські пропагандистські тексти, публікації окупаційних адміністрацій, дописи воєнкорів і повідомлення місцевих каналів. У такому масиві складно швидко побачити, які теми повторюються, які канали поширюють однакові формулювання і як змінюється риторика після конкретних подій.

Штучний інтелект може допомогти на першому етапі: згрупувати повідомлення за темами, знайти повтори, виділити назви населених пунктів, організацій, підрозділів, каналів або конкретних осіб. Наприклад, якщо після удару чи події на фронті російські канали починають одночасно просувати однакове пояснення, автоматизований аналіз може швидше показати цю синхронність. Для України це корисно під час виявлення інформаційних кампаній РФ і перевірки того, як певний наратив розходиться в різних джерелах.

Але тут є обмеження. Текст у Telegram або TikTok не завжди прямий і зрозумілий. Там можуть бути натяки, жаргон, меми, сарказм, помилки, скорочення або навмисно розмиті формулювання. Тому ШІ може допомогти знайти сигнал, але не має сам робити остаточний висновок. Аналітик усе одно повинен перевірити джерело, контекст і те, що саме повідомлення реально доводить.

Другий напрям - робота із зображеннями. У російсько-українській війні велика частина відкритої інформації з’являється не у вигляді тексту, а як фото, відео або супутниковий знімок. Це можуть бути кадри після обстрілу, зруйнований об’єкт, дорога, міст, техніка, пожежа, промислова зона або ділянка на окупованій території. Людині складно швидко переглянути великий масив таких матеріалів, особливо якщо вони надходять одночасно з різних джерел.

Тут можуть допомагати інструменти комп’ютерного зору. Вони здатні попередньо відбирати зображення, знаходити схожі об’єкти, порівнювати кадри, помічати зміни на місцевості або допомагати з аналізом супутникових знімків. Наприклад, якщо потрібно переглянути багато знімків після ударів по інфраструктурі, автоматизований інструмент може швидше показати ділянки, де

є помітні зміни. Це не означає, що він одразу дає правильний висновок, але він скорочує обсяг ручної роботи.

Для України такий напрям має практичне значення під час моніторингу окупованих територій, перевірки наслідків російських обстрілів, аналізу пошкоджень критичної інфраструктури або фіксації змін у зоні бойових дій. Але остаточна перевірка все одно залишається за людиною. Модель може неправильно розпізнати об’єкт, переплутати схожі елементи або не врахувати місцевий контекст. Тому ШІ тут варто розглядати як фільтр і помічника, а не як джерело остаточного доказу.

Ще один напрям, який може розвиватися, - автоматичне відстеження відкритого інформаційного простору. У війні проблема не лише в тому, щоб знайти одне повідомлення. Важливо ще побачити, коли певна тема починає різко повторюватися. Наприклад, кілька російських Telegram-каналів майже одночасно просувають однакове пояснення події, використовують схожі слова або поширюють один і той самий відеофрагмент. Якщо таких повідомлень багато, вручну це можна помітити не одразу.

У такій ситуації автоматизовані інструменти можуть бути корисними як система раннього сигналу. Вони не пояснюють подію замість аналітика, але можуть швидше показати повтор, зміну риторики або незвичну активність певних каналів. Для України це може допомагати під час спостереження за російськими інформаційними кампаніями, реакцією пропагандистських ресурсів на події фронту, темами мобілізації, допомоги партнерів, втрат, обстрілів або ситуації на окупованих територіях.

Але автоматизацію не можна сприймати як безпомилкову. Система може прийняти звичайне поширення новини за скоординовану кампанію або, навпаки, пропустити важливий сигнал. Тому остаточна оцінка має залишатися за людиною. ШІ може показати, де варто подивитися уважніше, але висновок має робити аналітик, який розуміє джерела, контекст і логіку російського інформаційного середовища.

Окремо треба сказати і про ризики самого штучного інтелекту. Такі інструменти можуть помилятися, вигадувати неточні пояснення, неправильно групувати повідомлення або не бачити різниці між жартом, пропагандою і реальним фактом. У звичайній ситуації це може бути просто помилкою аналізу. У воєнній сфері така помилка вже небезпечніша, бо може вплинути на розуміння події.

Наприклад, модель може неправильно визначити зміст повідомлення через сленг, переклад, іронію або специфічну лексику російських воєнкорів. Вона також може об’єднати різні події в одну тему лише тому, що там повторюються схожі слова. Тому результат роботи ШІ потрібно сприймати як чернетку для перевірки, а не як готовий аналітичний висновок.

Для України це означає, що перспективи ШІ в OSINT мають поєднуватися з обережністю. Автоматизація може допомогти швидше обробити великі масиви даних, але вона не замінює знання війни, мови, контексту, джерел і логіки противника. Без людської перевірки навіть сильний інструмент може дати слабкий або небезпечний результат. Тут важливо не перебільшувати роль ШІ. У OSINT він може зробити чорнову роботу: швидко знайти повтори, згрупувати повідомлення, перекласти текст або підсвітити підозрілу активність. Але сам по собі він не розуміє війну так, як її розуміє аналітик. Наприклад, російський воєнкор може писати натяками, сленгом або пропагандистськими формулами. Модель може це прочитати буквально і дати неправильне узагальнення. Тому результат ШІ треба перевіряти так само, як будь-яке інше джерело: хто написав, коли, у якому контексті і що це реально доводить.

Отже, перспективи ШІ в OSINT-аналітиці для України є реальними, але їх не треба перебільшувати. Найбільша користь ШІ - у швидкій чорновій роботі: знайти повтори, відсортувати повідомлення, допомогти з перекладом, підсвітити підозрілу активність або попередньо переглянути великий масив фото й текстів. Це може економити час аналітика, особливо коли інформації надходить дуже багато.

Але остаточний висновок усе одно має робити людина. У воєнній сфері помилка може коштувати дорого, тому ШІ має бути не “автоматичним експертом”, а інструментом допомоги. Для воєнної безпеки України найбільш перспективним є не заміна аналітика, а поєднання автоматизованої обробки, людської перевірки, знання джерел і розуміння російсько-української війни.

Висновки до розділу ІІІ

У третьому розділі було розглянуто практичні методи та інструменти OSINT-аналітики, які можуть застосовуватися у сфері воєнної безпеки України. Було показано, що значення мають не самі сервіси або програми, а те, яку саме перевірку вони дозволяють зробити. Пошукові системи, відкриті реєстри, архіви вебсторінок, соціальні мережі, Telegram, карти, супутникові знімки, геоінформаційні системи, таблиці й засоби візуалізації виконують різні функції, але найкраще працюють у поєднанні. Один інструмент може допомогти знайти першоджерело, інший - перевірити місце події, третій - побачити зміни на місцевості, четвертий - зафіксувати цифровий слід або показати зв’язки між даними. Для України це має практичне значення, оскільки під час війни відкриті джерела використовуються для перевірки повідомлень про обстріли, аналізу наслідків ударів, моніторингу окупованих територій, виявлення російських інформаційних кампаній і документування дій противника. Отже, головний результат цього підрозділу полягає в тому, що OSINT-інструменти варто розглядати не як окремий набір технічних засобів, а як частину послідовної аналітичної роботи.

Разом із цим у розділі було визначено основні проблеми використання OSINT-аналітики у сфері воєнної безпеки України. Відкриті джерела не є повністю надійним середовищем, бо в них одночасно присутні корисні дані, чутки, старі матеріали, помилки, російська пропаганда й навмисні інформаційні вкиди. Особливу складність становлять фото- і відеоматеріали, які можуть бути справжніми, але неправильно підписаними або поданими в маніпулятивному контексті. Тому OSINT потребує постійної перевірки джерела, часу, місця,

контексту і можливих наслідків публікації. Окремо було показано, що перспективним напрямом є використання штучного інтелекту та автоматизації. ШІ може допомагати з пошуком повторів, групуванням повідомлень, перекладом, первинною обробкою текстів, фото й відео. Але він не може замінити аналітика, який розуміє війну, джерела, мову, російський інформаційний простір і ризики помилкової інтерпретації. Таким чином, основний висновок розділу полягає в тому, що ефективна OSINT-аналітика для воєнної безпеки України можлива лише за поєднання інструментів, людської перевірки, критичного мислення та розуміння реального воєнного контексту.

ВИСНОВКИ

Проведене дослідження дало змогу розглянути OSINT-аналітику як один із сучасних інструментів посилення воєнної безпеки України. У роботі йшлося не лише про пошук інформації у відкритих джерелах, а про ширший процес: постановку аналітичного питання, добір джерел, перевірку даних, зіставлення різних повідомлень, оцінку контексту, виявлення ризиків і підготовку висновків, які можуть бути корисними для розуміння безпекової ситуації. Саме такий підхід дозволяє відмежувати OSINT-аналітику від звичайного моніторингу соціальних мереж, перегляду новин чи механічного накопичення відкритих даних.

У процесі дослідження було визначено генезу становлення OSINT-аналітики в системі розвідувальної та безпекової діяльності. Використання відкритих джерел не є явищем, яке виникло лише разом з Інтернетом. Його передумови пов’язані з використанням преси, радіомоніторингу, відкритих урядових повідомлень, публічних заяв, журналістських матеріалів, картографічних даних та інших форм доступної інформації. Тобто сама ідея використання відкритих джерел для безпекових потреб існувала раніше, але цифрова епоха суттєво змінила її масштаб.

Розвиток Інтернету, соціальних мереж, відеоплатформ, супутникових сервісів, відкритих реєстрів, комерційних баз даних і автоматизованих інструментів перетворив OSINT із допоміжного напряму роботи з інформацією на важливу складову сучасної аналітики. Особливо це проявилося під час російсько-української війни, коли значна частина відомостей про події на фронті, наслідки ударів, переміщення техніки, ситуацію на тимчасово окупованих територіях, діяльність окупаційних адміністрацій та інформаційні операції противника почала відображатися у відкритому цифровому просторі.

Тому історію OSINT-аналітики варто розуміти не просто як історію появи нових сервісів. Змінилася сама роль відкритої інформації. Раніше вона частіше була додатковим матеріалом до інших джерел, а тепер нерідко саме з неї починається перевірка події. Для українських умов це добре видно на прикладах

війни: повідомлення місцевого каналу, відео очевидця, супутниковий знімок або навіть публікація російського ресурсу можуть бути неповними, але все одно давати перший сигнал для подальшого аналізу.

Із самим поняттям OSINT ситуація також не є однозначною. У різних джерелах його пояснюють по-різному: десь наголошують на відкритості інформації, десь — на законному доступі до неї, а десь — на тому, що з відкритих даних має бути створений аналітичний продукт. Така різниця є логічною, бо OSINT використовується не в одній сфері. Його застосовують у розвідці, безпековій аналітиці, кібербезпеці, журналістських розслідуваннях, правоохоронній роботі, документуванні воєнних злочинів і громадському контролі.

У цій роботі OSINT-аналітика розуміється передусім як робота з інформацією, а не як сам факт доступу до неї. Відкрите повідомлення ще не є висновком. Воно має пройти перевірку: звідки взялося, коли з'явилося, чи відповідає місцю події, чи підтверджується іншими джерелами і чи не подане в маніпулятивному контексті. Тому для воєнної безпеки України важливо не просто знаходити відкриті дані, а доводити їх до такого рівня, коли вони можуть бути використані для обережного й обґрунтованого розуміння ситуації.

Окремо у висновках потрібно зафіксувати ще одну річ: у воєнний час проблема OSINT часто полягає не в браку інформації, а в її надмірі. Після обстрілів, заяв сторін, появи відео, повідомлень у Telegram або дописів місцевих каналів інформаційний простір швидко заповнюється різними версіями однієї події. Частина таких повідомлень може містити важливі дані, але поряд із ними з'являються припущення, повтори, емоційні оцінки, старі матеріали або свідомо вигідні для противника пояснення. Для воєнної безпеки це важливо, бо хибна версія події може впливати на загальне розуміння ситуації. Тому аналітик має оцінювати не кількість повідомлень, а їх походження, час появи, прив'язку до місця і те, що саме вони реально підтверджують.

Фото і відеоматеріали в цьому сенсі є окремим ризиком. Вони створюють враження прямого доказу, хоча на практиці потребують не меншої перевірки, ніж

текстові повідомлення. Відео може бути справжнім, але старим; кадр може бути знятий в іншому місці; підпис може змінювати зміст події; фрагмент може бути вирваний із ширшого контексту. Для OSINT-аналітики у сфері воєнної безпеки важливим є не тільки те, що видно на фото чи відео, а й другорядні на перший погляд ознаки: форма будівель, дороги, дорожні знаки, лінії електропередач, тіні, погода, рельєф, карта, супутникові знімки та попередні публікації. Саме такі деталі часто дозволяють зрозуміти, чи можна використовувати матеріал як підтвердження.

Людський фактор також не можна виносити за дужки. Навіть за наявності реальних матеріалів аналітик може помилитися: поспішити, прийняти першу версію за основну, не дійти до першоджерела або сплутати масовий перепост із незалежним підтвердженням. В умовах війни це особливо небезпечно, бо інформація поширюється швидко, часто емоційно і не завжди з повним контекстом. Тому OSINT-аналітика для потреб воєнної безпеки вимагає не лише інструментів, а й дисципліни перевірки. Потрібно щоразу відділяти те, що матеріал справді доводить, від того, що лише припускається або нав’язується його подачею.

Також варто окремо залишити питання меж використання відкритої інформації. Для OSINT важливо не тільки знайти матеріал і перевірити його, а й зрозуміти, що з ним можна робити далі. У воєнний час навіть звичайне фото, відео, коментар, маршрут або фрагмент карти можуть випадково показати місце перебування людей, стан об’єкта, наслідки удару, напрям руху чи деталі роботи інфраструктури. Тому не вся відкрита інформація має автоматично переходити у відкритий текст. Частину даних доцільно використовувати лише для внутрішньої перевірки, якщо їх публікація може створити додаткові ризики.

У цьому і проявляється зв’язок OSINT-аналітики з воєнною безпекою України. Вона не підміняє військову розвідку, закриті джерела чи рішення командування, але може посилювати інформаційно-аналітичну частину безпекової роботи. Через відкриті джерела можна швидше помітити інформаційний сигнал, перевірити повідомлення, уточнити місце і час події,

побачити цифровий слід, простежити російський наратив або порівняти кілька версій однієї події. Тобто користь OSINT полягає не в самій відкритості даних, а в тому, що вони допомагають точніше оцінювати безпекову ситуацію.

Звідси логічно випливає, що OSINT-аналітика має починатися з питання, а не з інструмента. Спочатку потрібно зрозуміти, що саме треба встановити: де відбулася подія, коли з'явився матеріал, хто його поширив, чи є ознаки інформаційної операції, чи змінювалася місцевість, чи підтверджується повідомлення іншими джерелами. Лише після цього варто обирати карти, супутникові знімки, Telegram-канали, архіви сторінок, реєстри або комерційні сервіси. Такий порядок робить OSINT не випадковим пошуком у відкритому просторі, а послідовною перевіркою інформації для потреб воєнної безпеки.

Якщо переходити від методики до практики, то російсько-українська війна добре показує: OSINT працює не тільки в кабінетній аналітиці. Часто перший матеріал про подію з'являється у відкритому просторі — у місцевому Telegram-каналі, на відео очевидця, на супутниковому знімку, у повідомленні російського ресурсу або на карті, яку оновлюють волонтери. Для воєнної безпеки України це важливо, бо такі фрагменти не завжди дають повну відповідь, але можуть стати початком перевірки.

У цьому контексті показовими є приклади Bellingcat, InformNapalm, Molfar, DeepState, Cyber Resistance та інших ініціатив. Їх не варто розглядати однаково, бо вони працюють з різними завданнями. Одні більше зосереджені на розслідуваннях і верифікації матеріалів, інші — на картографуванні, аналізі відкритих даних, фіксації дій противника, роботі з інформаційними мережами або документуванні цифрових слідів війни. Спільним для них є те, що відкриті дані використовуються не самі по собі, а після перевірки й прив'язки до конкретної події.

На локальному рівні цінність OSINT часто проявляється через дрібні деталі. Це може бути дорожній знак, силует будівлі, тінь, лінія електропередач, звук на відео, повідомлення місцевого каналу або зміна на супутниковому знімку. Окремо така деталь може майже нічого не доводити. Але якщо вона

збігається з картою, іншими фото, відео, часом публікації або попередніми повідомленнями, тоді з неї можна зробити обережний висновок. Саме в цьому практична користь OSINT для воєнної безпеки: він допомагає не просто збирати матеріали, а поступово перевіряти картину події.

Щодо інструментів, то з роботи видно: ручний пошук залишається важливим, але його вже недостатньо. У війні відкритих даних занадто багато, і вони з'являються дуже швидко. Це Telegram-канали, відео, фото, супутникові знімки, карти, повідомлення медіа, архіви сторінок, реєстри, коментарі очевидців і матеріали російських ресурсів. Аналітик може працювати з цим вручну, але тоді частина даних буде втрачатися або перевірятися надто повільно. Тому інструменти потрібні не для заміни людини, а для того, щоб швидше зібрати матеріал, зберегти його і порівняти з іншими джерелами.

Комерційні сервіси в цьому сенсі можуть бути корисними, але їх не варто ідеалізувати. Платні супутникові знімки, сервіси моніторингу соціальних мереж, інструменти для архівації, побудови зв'язків або роботи з картами справді розширюють можливості OSINT. Вони допомагають побачити зміни на місцевості, знайти зв'язок між каналами, перевірити динаміку повідомлень або зафіксувати матеріал до того, як його видалять. Для воєнної безпеки України це має практичне значення, бо у війні важлива не тільки сама інформація, а й те, чи вдалося її вчасно зберегти, перевірити і правильно прочитати.

Разом з тим доступ до сильного сервісу ще не означає якісного висновку. Інструмент може пришвидшити пошук або показати зв'язки, але він не пояснить самостійно, що саме відбувається у воєнному контексті. Це все одно має робити аналітик, який розуміє джерела, логіку противника, ризики маніпуляції та межі використання відкритих даних. До того ж у різних суб'єктів різні можливості: державна структура, волонтерська ініціатива, журналіст або окремий дослідник не завжди мають однаковий доступ до платних платформ. Тому питання інструментів для України — це не лише питання техніки, а й питання підготовки людей, правил роботи з даними і спільної культури перевірки.

OSINT не обмежується пошуком окремого фото, відео чи повідомлення. Часто важливо подивитися, як саме побудована мова джерел. У російському інформаційному просторі одні й ті самі формули можуть повторюватися в різних каналах, змінювати акценти або просувати певну версію подій. Для воєнної безпеки України це має значення, бо такі мовні повтори іноді показують не випадкові емоційні реакції, а підготовлену інформаційну лінію. Тому аналіз текстів у OSINT потрібен не заради самого підрахунку слів, а для того, щоб побачити, які теми противник намагається зробити помітними.

Не менш важливо дивитися на те, як повідомлення поширюються між джерелами. Один допис у Telegram може виглядати як окрема думка, але якщо його швидко підхоплюють інші канали, сайти або акаунти, тоді з’являється інше питання: це природне поширення чи частина узгодженої інформаційної дії. Для OSINT-аналітики така перевірка корисна тим, що дозволяє не плутати повторення з підтвердженням. Якщо кілька ресурсів поширили одну версію події, це ще не означає, що вона стала достовірнішою. Потрібно зрозуміти, чи є між цими джерелами зв’язок і звідки реально пішло повідомлення.

Окреме місце займає робота з простором. У воєнній тематиці часто потрібно не просто прочитати повідомлення, а зрозуміти, де саме могла відбутися подія. Тут допомагають карти, супутникові знімки, фото місцевості, відео, відкриті геосервіси й навіть дрібні ознаки на кадрі. Це може бути форма дороги, розташування будівель, лінія електропередач, рельєф або тінь. Для аналізу наслідків ударів, ситуації біля об’єктів інфраструктури, подій на окупованих територіях чи в прифронтових районах така перевірка є дуже важливою. Але і тут головним залишається не сам інструмент, а правильне зіставлення просторових ознак з іншими даними.

Питання штучного інтелекту в OSINT не варто подавати як окрему “магічну” перевагу. У цій роботі він радше розглядається як інструмент, який може зняти з аналітика частину технічної роботи. Наприклад, коли є багато повідомлень, відео, текстів або коментарів, такі засоби можуть допомогти швидше розкласти матеріал по темах, знайти повтори, перекласти фрагменти,

витягнути назви місць або помітити схожі формулювання. Але це тільки початковий рівень роботи, а не готовий висновок.

Для воєнної безпеки України тут є і користь, і ризик. Користь у тому, що під час війни обсяг відкритої інформації часто більший, ніж людина може швидко переглянути вручну. Ризик у тому, що автоматизований інструмент не завжди розуміє, що стоїть за повідомленням: чи це реальна подія, чи повтор старого матеріалу, чи російська подача, чи просто емоційний допис. Тому результат такої обробки треба сприймати як підказку, яку ще потрібно перевірити.

У підсумку для OSINT-аналітики важливе не саме використання ШІ, а те, як він вбудований у роботу людини. Якщо аналітик розуміє джерела, контекст війни, логіку російських інформаційних дій і межі відкритих даних, тоді автоматизовані інструменти можуть прискорити перевірку. Якщо ж покладатися на них без контролю, вони можуть тільки швидше поширити помилку. Тому в цій сфері остаточне рішення все одно має залишатися за людиною.

У підсумку не можна сказати, що OSINT сам по собі вирішує проблему воєнної невизначеності. Відкриті джерела дають багато матеріалу, але цей матеріал ще треба розібрати. Одне відео, фото, повідомлення в Telegram або супутниковий знімок можуть бути корисними, але без перевірки вони залишаються лише фрагментом. У війні фрагмент легко прийняти за повну картину, і саме в цьому полягає один із головних ризиків.

Для України цінність OSINT полягає в іншому. Він допомагає не пропустити сигнал, який з’явився у відкритому просторі, і перевірити його до того, як робити висновок. Це може стосуватися наслідків удару, ситуації на окупованій території, російської інформаційної кампанії, зміни на місцевості або появи нової версії події. Але кожного разу треба дивитися не тільки на сам матеріал, а й на те, хто його поширив, коли він з’явився, чи є інші підтвердження і чи не створить його публікація додаткової шкоди.

Тому OSINT-аналітика має розвиватися як частина ширшої безпекової роботи, а не як окрема віра в цифрові інструменти. Потрібні підготовлені аналітики,

фіксація джерел, нормальна перевірка фото й відео, доступ до карт, супутникових знімків, архівів і комерційних сервісів. Потрібна також обережність із чутливою інформацією. У такому вигляді OSINT не замінює розвідку чи рішення командування, але може допомагати швидше перевіряти відкриту інформацію, зберігати цифрові сліди й точніше розуміти події у воєнному середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

Джерела

1. Best R.A. Jr., Cumming A. Open Source Intelligence (OSINT): Issues for Congress. URL: https://apps.dtic.mil/sti/citations/ADA488690 (дата звернення: 15.05.2026)
2. OSINT STRATEGY 2024-2028. URL: https://www.dia.mil/Portals/110/Documents/OSINT-Strategy.pdf (дата звернення: 15.05.2026)
3. United States Office of the Director of National Intelligence. U.S. National Intelligence-An Overview 2011. URL: https://www.dni.gov/files/documents/IC_Consumers_Guide_2011.pdf (дата звернення: 15.05.2026)

Наукова література

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://ppdnz.com.ua/index.php/home/article/view/199 (дата звернення: 15.05.2026)
5. Биба Р.Ю. Поняття OSINT у сфері публічного порядку та безпеки. *Науковий вісник Ужгородського Національного Університету*. Серія ПРАВО. 2025. Випуск 92: Том 3. С. 38-43.
6. Білобров А.В., Клімушин П.С. Використання технологій OSINT для отримання інформації. *Протидія кіберзлочинності та торгівлі людьми: Збірник матеріалів Міжнародної науково-практичної конференції (м. Харків. 27 травня 2020 року)*. С. 135-137. URL: https://www.univd.edu.ua/general/publishing/konf/27_05_2020/pdf/39.pdf. (дата звернення: 15.05.2026)
7. Дрижакова Д., Волинець Р. Використання відкритих джерел інформації (OSINT) у сфері безпеки держави: технології та перспективи. *Матеріали*

конференцій МЦНД. (28.02.2025; Дніпро. Україна). С. 138-141. URL: https://doi.org/10.62731/mcnd-28.02.2025.005 (дата звернення: 15.05.2026)

8. Думчиков М.О. Використання OSINT технологій для виявлення корупційних правопорушень: сучасні підходи та виклики. *Академічні візії. Секція: Право*. 2024. №36. С. 1-6.

9. Жарков Я.М., Васильєв А.О. Наукові підходи щодо визначення суті розвідки з відкритих джерел. *Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки*. 2013. Вип. 30. С. 38-41. URL: http://nbuv.gov.ua/UJRN/VKNU_vsn_2013_30_12 (дата звернення: 15.05.2026).

10. Жмур Н.В., Землянікіна М.П. Історія становлення та сучасний стан технології пошуку інформації OSINT. *Наукові праці Київського авіаційного інституту. Серія: Юридичний журнал "Повітряне і космічне право".* 2022. №3 (64). С. 95-101.

11. Ковалів М., Іваха В. Військова безпека як чинник стабільності суспільства. *Науковий вісник Львівського державного університету внутрішніх справ*. 2015. № 3. URL: http://dspace.lvduvs.edu.ua/bitstream/1234567890/1903/1/3-2015kmvchss.pdf (дата звернення: 15.05.2026)

12. Кожушко О.О. Розвідка відкритих джерел інформації (OSINT) у розвідувальній практиці США. URL: http://jrnl.nau.edu.ua/index.php/IMV/article/viewFile/3264/3217. (дата звернення: 15.05.2026)

13. Лаврьонов Р.П. Військова безпека: аналіз стану трансформації системи управління. *Київський часопис права*. 2023. №4. С. 149-156.

14. Ковалів М.В., Іваха В.О. Воєнна безпека як чинник стабільності суспільства. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична.* 2015. Вип. 3. С. 124-132. URL: http://dspace.lvduvs.edu.ua/handle/1234567890/1903 (дата звернення: 15.05.2026).

15. Ліцук Б.В., Стрелков В.В. Галузі застосування розвідки відкритих джерел даних (OSINT). URL: https://jppasa.donnu.edu.ua/article/view/15733 (дата звернення: 15.05.2026)

16. Мартинюк С.О. Характеристика принципів функціонування OSINT у сфері національної безпеки. *Юридичний науковий електронний журнал*. 2021. № 9. С. 332-334. URL: http://www.lsej.org.ua/9_2021/85.pdf. (дата звернення: 15.05.2026)

17. Минько О.В. Використання технологій OSINT для отримання розвідувальної інформації. *Системи управління, навігації та зв'язку*. 2016. Вип. 4. С. 81-84.

18. Минько О.В.. Іохов О.Ю., Оленченко В.Т., Власов К.В. Використання технологій OSINT для отримання розвідувальної інформації. *Експерт: парадигми юридичних наук і державного управління*. 2019. № 4(6). С. 201-208. URL: http://nbuv.gov.ua/UJRN/suntz_2016_4_22. (дата звернення: 15.05.2026)

19. Пархоменко-Куцевіл О. Теоретичні засади формування та розвитку воєнної безпеки України. *Літопис Волині. Всеукраїнський науковий часопис*. 2023. Вип. 28. С. 367-372.

20. Радейко Р. І. Інструментарій OSINT у юридичній методології: теоретичні основи та практичне застосування. *Наукові записки Львівського університету бізнесу та права. Серія юридична*. 2024. Вип. 43. С. 400-410.

21. Скриньковський Р.М. Воєнна безпека держави як складова національної безпеки. *International scientific journal «Internauka». Series: «Juridical sciences».* 2025. № 1 (83).

22. Франчук В., Мельник С., Гобела В., Шупрудько Н., & Тюріна Н. Розвиток безпекового середовища: концептуальна модель OSINT та управління. *Financial and Credit Activity Problems of Theory and Practice*. 2026. №2(67). С.239-251.

23. Abdalla N.S., Davies P.H.J., Gustafson K., Lomas D. & Wagner S. Intelligence and the War in Ukraine: Part 2. War on the Rocks. URL: https://warontherocks.com/2022/05/intelligenceand-the-war-in-ukraine-part-2/. (дата звернення: 15.05.2026)

24. Abdalla N.S., Davies P.H.J., Gustafson K., Lomas D. & Wagner, S. Intelligence and the War in Ukraine: Part 1. War on the Rocks. URL: https://warontherocks.com/2022/05/intelligenceand-the-war-in-ukraine-part-1/. (дата звернення: 15.05.2026)

25. Alexander E. Military Memoirs of a Confederate. A Critical Narrative. New York: Charles Scribners Sons. 1907.

26. Arango S.J. Data brokers: A benefit or peril to U.S. national security? *Ohio State Technology Law Journal*. 2023. №20:1. P. 107-38;

27. Bean H. No more secrets. Open source information and the reshaping of U.S. intelligence. Praeger security international, 2011. 240 c.

28. Benes L. OSINT, New Technologies, Education: Expanding Opportunities and Threats. A New Paradigm. *Journal of Strategic Security*. 2013. Vol. 6, № 5.

29. Block L. The long history of OSINT. *Journal of Intelligence* History. 2024. №23:2. P. 95-109.

30. Böhm I., Lolagar S. Open source intelligence Introduction, legal, and ethical considerations

31. Colley T., Dylan H. The War on Open-Source Intelligence. *The Washington Quarterly*. 2025. Vol. 48. Is. 3. P. 147-162

32. Coulthart S., Nussbaum B. A definition of open source intelligence.

33. Dover R. Adding value to the intelligence community: What role for expert external advice? *Intelligence and National Security*. 2020. №35:6. P. 852-869..

34. Dover R. SOCMINT: A Shifting Balance of Opportunity. *Intelligence and National Security*. 2020. №35:2. P. 216-232.

35. Eldridge C., Hobbs C., Moran M. Fusing algorithms and analysts: Open-source intelligence in the age of big data. *Intelligence and National Security*. 2017. № 33:3. P. 391-406.

36. Feinberg M. Everyday Adventures with Unruly Data. The MIT Press, 2022. 336 p.

37. Fuhlhage M. Yankee Reporters and Southern Secrets. Journalism. Open Source Intelligence and the coming of the Civil War. Peter Lang: New York, 2019

38. Gentry J.A. Favorite INTs: How they develop. why they matter. *Intelligence and National Security.* 2018. №33:6. P. 822-838.

39. Gibson S.D. Future Roles of the UK Intelligence System. *Review of International Studies.* 2009. Vol. 35. №4. P. 917-928.

40. Glassman M., Kang M. Intelligence in the Internet Age: The Emergence and Evolution of Open Source Intelligence (OSINT). *Computers in Human Behavior*. 2012. №28:2. P. 673-682;

41. Hassan N.A., Hijazi R. Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence. New York - Mississauga: Apress, 2018

42. Hatfield J.M. There is no such thing as open source intelligence. *International Journal of Intelligence and CounterIntelligence*. 2023. №37:2. P. 397-418.

43. Holden-Rhodes J. Unlocking the Secrets: Open Source Intelligence in the War on Drugs. *American Intelligence Journal*. 1993. Spring/Summer. P. 67-71.

44. Hulnick A.S. The Dilemma of Open Sources Intelligence: Is OSINT Really Intelligence? *The Oxford Handbook of National Security Intelligence*. 2010.

45. Kotaridis I. Benekos G. Integrating Earth observation IMINT with OSINT data to create added-value multisource intelligence information: A case study of the Ukraine-Russia war. *Security and Defence Quarterly.* 2023. №43 (3) P. 1-21.

46. Kozera C.A. Fitness OSINT: Identifying and tracking military and security personnel with fitness applications for intelligence gathering purposes

47. Krpec O., Chovančík M., Ilavská A. Open Source Intelligence (OSINT) and the fog of war at the strategic level: Defence industrial production in Russia. URL: https://www.cambridge.org/core/journals/european-journal-of-international-security/article/open-source-intelligence-osint-and-the-fog-of-war-at-the-strategic-level-defence-industrial-production-in-russia/C732FF8D8AE9956A4920BA6DC2451F20 (дата звернення: 15.05.2026)

48. Lahneman W.J. The need for a new intelligence paradigm. *International Journal of Intelligence and CounterIntelligence*. 2010. № 23:2 P. 201-225.

49. Lowenthal M.M. OSINT: The State of the Art. The Artless State. *Studies in Intelligence*. 2001. Vol. 45. № 3.

50. Mercado S. Sailing the Sea of OSINT in the Information Age. *Studies in Intelligence.* 2004. №48(3). P. 45-55.

51. Minkina M. Sztuka wywiadu w państwie współczesnym. Warszawa: Oficyna Wydawnicza RYTM, 2014.

52. Omand D., Bartlett J., Miller C. Introducing Social Media Intelligence (SOCMINT). *Intelligence and National Security*. 2012. №27(6) P. 801-823.

53. Palk L., Muralidhar K. A Free Ride: Data Brokers Rent-Seeking Behavior and the Future of Data Inequality.

54. Researching a Rigged Game: Digital Approaches to Tracing the Illicit Trade in Cultural Objects. URL: https://link.springer.com/book/10.1007/978-3-032-02014-7 (дата звернення: 15.05.2026)

55. Rolington A. Objective Intelligence or Plausible Denial: An Open Source Review of Intelligence Method and Process since 9/11. *Intelligence and National Security*. 2006. Vol. 21. № 5. P. 741-742.

56. Sands A. Integrating Open Sources into Transnational Threat Assessments. *Transforming US Intelligence*. Washington. DC: Georgetown University Press, 2005. P. 63-78.

57. Schrijver Pr. The wise man will be master of the stars. The use of Twitter by a military intelligence service in wartime: The case of the GUR. *Reflections on the Russia-Ukraine war*. Leiden: Leiden University Press, 2024. P. 77-95.

58. Smith-Boyle. How OSINT Has Shaped the War;

59. Steele R. Intelligence in the 1990s: Recasting National Security in a changing world. American Intelligence Journal. 1990. Summer/Fall.

60. Studeman W. Open Sources and the Intelligence Community: Myths and Realities. P. 19-24;

61. Studeman W. Teaching the Giant to Dance: Contradictions and Opportunities in Open Source Information within the Intelligence Community. *American Intelligence Journal*. 1993. Spring/Summer. P. 11-18.

62. Towards a data-driven military. A multidisciplinary perspective. Leiden; Leiden University Press, 2023. 364 p.

63. Van Beek H., Rietjens S OpenSource Intelligence in the Russia-Ukraine War. *Reflections on the Russia-Ukraine War*. Leiden: Leiden University Press. 2024. P. 57-76.

64. Van Puyvelde D., Rienzi F.T. The rise of open-source intelligence. *European Journal of International Security*. 2025. №10:4. P. 1-15.

65. Williams H.J., Blum I. Defining second generation open source intelligence (OSINT) for the defense enterprise. Santa Monica: Rand Corporation, 2018. URL: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1964/RAND_RR1964.pdf (дата звернення: 15.05.2026)

66. Ziółkowska A. Open source intelligence (OSINT) as an element of military recon

67. Zwanenburg M. The Use of OSINT for Military Operations Abroad under International Humanitarian Law and International Human Rights Law

Словники та енциклопедичні видання

68. NATO. NATO Glossary of Terms and Definitions. AAP-6 (2021).

69. Open Source Intelligence Tools and Resources Handbook/ i-Intelligence, 2018. 327 с.

Інтернет-ресурси.

70. Базовий OSINT курс від Molfar. OSINT-спільнота Molfar. URL: https://www.udemy.com/course/osint-molfar/ (дата звернення: 16.01.2026)

71. Використання інструментів та методів OSINT для отримання пошукової інформації : практичний порадник / Зоренко Д. С.. Лех Р. В.. Кулик Д. О.. Червяков О. І. Х.: ІПЮК для СБУ. 2023. 36 с.

72. Дикий О.В.. Сидорчук В.В. Поняття OSINT та суміжні категорії. URL: http://lsej.org.ua/9_2024/80.pdf. (дата звернення: 15.05.2026)

73. Інструмент FOCA. URL: https://github.com/foca-js/foca (дата звернення: 15.05.2026)

74. Інструмент GIFTHUB. URL: https://github.com/smicallef/spiderfoot (дата звернення: 15.05.2026)

75. Інструмент Maltego. URL: https://www.maltego.com/ (дата звернення: 15.05.2026)

76. Інструмент RECON-NG. URL: https://github.com/lanmaster53/recon-ng (дата звернення: 15.05.2026)

77. Інструмент theHarvester. URL: https://github.com/laramies/theHarvester (дата звернення: 15.05.2026)

78. Інструмент URLSCAN. URL: https://urlscan.io/ (дата звернення: 15.05.2026)

79. Albon C. How Commercial Space Systems Are Changing the Conflict in Ukraine. URL: https://www.c4isrnet.com/intel-geoint/2022/04/25/how-commercial-space-systems-are-changing-the-conflict-in-ukraine/. (дата звернення: 15.05.2026)

80. Aldhous P., Miller C. How Open-Source Intelligence is Helping Clear the Fog of War in Ukraine. *BuzzFeed News*. URL: https://www.buzzfeednews.com/article/peteraldhous/osint-ukraine-war-satellite-images-plane-tracking-social. (дата звернення: 15.05.2026)

81. Block L. A (working) definition of OSINT. *BLOCKINT* (5 December 2022). URL: https://www.blockint.nl/methods/a-working-definition-of-osint/ (дата звернення: 15.05.2026)

82. Campbell A. Legitimate actors or security concern? How OSINT hobbyists are changing the nature of conflict. Masters diss. Charles University (2022). P. 44-50. URL: https://dspace.cuni.cz/bitstream/handle/20.500.11956/178382/120428403.pdf?sequence=1&isAllowed=y (дата звернення: 15.05.2026).

83. Colquhoun C. A Brief History of Open Source Intelligence. *Bellingcat*. URL:https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/ (дата звернення: 15.05.2026)

84. Endsor M., Peace B. A Call to Arms: Open Source Intelligence and Evidence Based Policymaking. *Bellingcat*. URL: (дата звернення: 15.05.2026)

85. Freear M. OSINT in an Age of Disinformation Warfare. *RUSI*. URL: https://rusi.org/exploreour-research/publications/commentary/osint-age-disinformation-warfare/. (дата звернення: 15.05.2026)

86. Gibson S.D. Open Source Intelligence (OSINT): A Contemporary Intelligence Lifeline (Cranfield University: PhD thesis. 2007). Appendices: Interview EUROPOL 4. URL: https://dspace.lib.cranfield.ac.uk/handle/1826/6524. (дата звернення: 15.05.2026)

87. GlobalData. The Role of OSINT in the War in Ukraine. *Army Technology*. URL: https://www.army-technology.com/analyst-comment/osint-war-in-ukraine/. (дата звернення: 15.05.2026)

88. Harris S. Open source intelligence on the Russian internet. SANS Open-Source Intelligence Summit (1 March 2024). URL: https://www.sans.org/presentations/a-practical-guide-to-osint-on-the-russian-internet/. (дата звернення: 15.05.2026)

89. Higgins E. Geolocation Techniques-Mapping Landmarks,. Bellingcat (July 15, 2014).

90. Hockenhull J. How Open-Source Intelligence Has Shaped the Russia-Ukraine War. URL: https://www.gov.uk/government/speeches/how-open-source-intelligence-has-shaped-the-russia-ukraine-war. (дата звернення: 15.05.2026)

91. Karalis M. Open-Source Intelligence in Ukraine: Asset or Liability? Chatham House (16 December 2022). URL: https://www.chathamhouse.org/2022/12/open-source-intelligence-ukraine-asset-or-liability. (дата звернення: 15.05.2026)

92. Littell J., Smith M., Starck N. The Devil is in the Data: Publicly Available Information and the Risks to Force Protection and Readiness. URL: https://mwi.westpoint.edu/the-devil-is-in-the-data-publicly-available-information-and-the-risks-to-force-protection-and-readiness/ (дата звернення: 15.05.2026)

93. Lomas D. The death of secret intelligence? Think again. *RUSI* (5 July 2023). URL: https://rusi.org/explore-ourresearch/ publications/commentary/death-secret-intelligence-think-again. (дата звернення: 15.05.2026)

94. Miller B. Evolution of intel: How valuable is OSINT? URL: https://amuedge.com/evolution-of-intel-how-valuable-is-osint/ (дата звернення: 15.05.2026)

95. Open Source Information: A True Collection Discipline. M.A. thesis. Royal Military College of Canada;

96. Open Source Intelligence in the Twenty-First Century New Approaches and Opportunities

97. OSINT Unveiled: The technology behind the intelligence. How is the Army leveraging OSINT to strengthen its intelligence capabilities? URL: https://federalnewsnetwork.com/cme-event/federal-insights/osint-unveiled-the-technology-behind-the-intelligence/ (дата звернення: 15.05.2026)

98. Postma F. After Strava, Polar is Revealing the Homes of Soldiers and Spies. *The Bellingcat*. URL: https://www.bellingcat.com/resources/articles/2018/07/08/strava-polar-revealing-homes-soldiers-spies/ (дата звернення: 15.05.2026).

99. Rodewig C. Geotagging poses security risks. *The Official Homepage of the U.S. Army*. URL: https://web.archive.org/web/20120309232923/https://www.army.mil/article/75165/geotagging_poses_security_risks (дата звернення: 15.05.2026).

100. Romansky S., Boswinkel L., Rademaker M. The Parallel Front: An Analysis of the Military Use of Information in the First Seven Months of the War in Ukraine. URL: https://hcss.nl/report/the-parallel-front-military-use-information-ukraine/. (дата звернення: 15.05.2026)

101. Sage-Passant L. The Security Intelligence Services of the Private Sector. URL: https://doi.org/10.26174/thesis.lboro.24050421.v1. (дата звернення: 15.05.2026)

102. Schaurer F., Storger J. The evolution of open source intelligence (OSINT). International Relations and Security Network (ETH Zurich. 2010).

103. Van Puyvelde D., Rienzi T.F. OSINT and the war in Ukraine: workshop summary

104. Winter Ch., Gallacher J., Harris A. Artificial Intelligence. OSINT and Russias information landscape. *CETaS Expert Analysis* (2 February 2023). URL: https://cetas.turing.ac.uk/publications/artificial-intelligence-osint-andrussias-information-landscape. (дата звернення: 15.05.2026)

105. Zegart A. Open secrets: Ukraine and the next intelligence revolution. Foreign Affairs (20 December 2022). URL: https://www.foreignaffairs.com/world/open-secrets-ukraine-intelligence-revolution-amy-zegart (дата звернення: 15.05.2026)

106. Zwijnenburg W. Yemen’s Disappearing Date Palms: Applied Environmental OSINT. The Bellingcat. URL: https://www.bellingcat.com/news/mena/2020/07/24/yemens-disappearing-date-palmsapplied-environmental-osint/ (дата звернення: 15.05.2026).
107. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 15.05.2026)