МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОСТРОЗЬКА АКАДЕМІЯ»
Навчально-науковий інститут міжнародних відносин та національної безпеки
Кафедра інформаційно-документних комунікацій

ЗАТВЕРДЖУЮ
на засіданні кафедри
інформаційно-документних комунікацій
(протокол № __від _____2026 р.)
Завідувач кафедри _____Ганна ОХРІМЕНКО

Кваліфікаційна робота
на здобуття освітнього рівня бакалавра
на тему: **«ЗАСТОСУВАННЯ ІНСТРУМЕНТІВ ВІДКРИТОЇ РОЗВІДКИ У ПРОЦЕСІ ІДЕНТИФІКАЦІЇ ЦИФРОВОЇ ОСОБИСТОСТІ В УКРАЇНІ: ПАРАДИГМАЛЬНИЙ АСПЕКТ»**

Виконала здобувачка групи Інс-41
освітньо-професійної програми
«Інформаційна, бібліотечна та архівна справа»
Мосіюк Вікторія Олегівна

Керівник – доктор філософії (PhD),
ст. викладач кафедри інформаційно-документних комунікацій
ФЕДОРУК Олеся Михайлівна
Рецензент – доктор наук з мистецтвознавства,
доцент кафедри інформаційно-документних комунікацій
БОНДАРЧУК Ярослава Віталіївна

Острог, 2026

ГРАФІК

виконання кваліфікаційної роботи на першому (бакалаврському) рівні вищої освіти

студентки групи Інс-41

Мосіюк Вікторії Олегівни

№ п/п	Види та етапи роботи	Термін виконання	Підпис викладача
1	Вибір теми, затвердження її на кафедрі, призначення наукового керівника	до 15.10. 2025 р.	
2	Складання графіка роботи над темою і узгодження його з науковим керівником	жовтень-листопад 2025 р.	
3	Вивчення джерел, літератури, суспільних реалій, матеріалів архівів, періодичних видань; збір та узагальнення фактів і даних	листопад-грудень 2025 р.	
4	Складання плану роботи та узгодження його з науковим керівником	грудень 2025 р.	
5	Формування концепції, написання вступу та теоретичного розділу роботи	січень-лютий 2026 р.	
6	Написання дослідницької частини кваліфікаційної роботи	лютий-травень 2026 р.	
7	Завершення рукопису роботи та ознайомлення наукового керівника з її повним чорновим варіантом в друкованому вигляді	травень 2026 р.	
8	Повне завершення чистового варіанту роботи, оформлення її і подання роботи на зовнішнє рецензування	травень 2026 р.	
9	Проведення попереднього захисту	14 травня 2026 р.	
10	Подання чистового варіанту роботи на кафедру	до 15 червня 2026 р.	
11	Подання рецензії на кафедру	до 18 червня 2026 р.	
12	Захист кваліфікаційної роботи	23 червня 2026 р.	

Здобувачка першого (бакалаврського)
рівня вищої освіти _____ **Вікторія МОСІЮК**

Науковий керівник _____ **Олеся ФЕДОРУК**

ЗМІСТ

ВСТУП

Актуальність дослідження. З початком повномасштабного вторгнення РФ у 2022 році розвідка на основі відкритих джерел перестала бути лише допоміжним інструментом. Серед усього спектру напрямів її застосування саме ідентифікація особи набула особливої актуальності . Українські державні структури, волонтерські ініціативи та незалежні дослідницькі команди щоденно встановлюють особи військовослужбовців противника, виконавців ворожих інформаційно-психологічних операцій, а також осіб що сприяють обходу санкцій. У багатьох випадках ідентифікація особи стає ключовою ланкою, без якої неможливими є ані кримінальне переслідування, ані ефективна контрпропаганда. Цей стрімкий сплеск практичного застосування підкреслив значний розрив між практикою використання OSINT та науковим осмисленням цієї теми. Виникла потреба в систематизації накопиченого досвіду та аналізі реальних методик, за допомогою яких українські організації ідентифікують особу.

Таке зростання практичного застосування змінило саму парадигму ідентифікації. Якщо раніше встановлення особи було майже виключно прерогативою державних структур із доступом до закритих баз даних і спеціальних повноважень, то тепер ці завдання успішно вирішують перехід від централізованої монополії до децентралізованої аналітичної роботи докорінно змінив уявлення про те, хто і як може здійснювати ідентифікацію в інтересах національної безпеки. Однак саме він і загострив потребу в надійному методичному підґрунті: досліднику вже недостатньо володіти розрізненими інструментами, необхідно чітко розуміти, які з них є найбільш дієвими.

Стан наукової розробки теми. У вітчизняній науці одними з перших обґрунтували можливість використання OSINT для отримання криміналістично значущої інформації О.В. Одерій та О.А. Кожевніков [21], які навели приклади пошуку осіб за антропометричними даними на фото й відео. Правову оцінку таких даних досліджує І.В. Гловюк [8], яка аналізує критерії належності, допустимості та достовірності результатів OSINT у судовій практиці,

спираючись на рішення Касаційного кримінального суду. Д.О. Коновалова [15] розглядає проблемні аспекти використання OSINT у кримінальному провадженні, зокрема правові засади збору та оформлення результатів, а також ризики, пов’язані з використанням спеціалізованих сервісів. Потенціал поєднання OSINT із технологіями штучного інтелекту для розслідування воєнних злочинів висвітлює В.М. Шевчук [35].

Фундаментальний внесок у систематизацію методології OSINT зробив Д.В. Ланде, який опублікував навчальний посібник «OSINT у кіберпезпеці» [17], що охоплює теоретичні засади, розвідувальний цикл та практичний інструментарій. Крім того, О.О. Пучковим та І.Ю. Субачем розроблено методику виявлення об’єктів кібербезпеки на основі алгоритмів сканування та аналізу мереж. Різні аспекти технічного забезпечення OSINT досліджують І.Р. Опірський та колеги: у публікації з А.О. Главацькою та О.В. Ангельською [7] проаналізовано загрози деанонімізації особи при використанні відкритих даних, а в роботі з В.С. Івковою – можливості сучасних аналітичних засобів Maltego, Shodan тощо [12]. Серед закордонних дослідників методологічні аспекти систематизували М. Валков та Д. Пьон [62], які запропонували класифікацію джерел даних та інструментів для OSINT-розслідувань. Алгоритмічні підходи до автоматизованого збору й аналізу даних ґрунтовно виклали Р. Лейтон та П.Воттерс у праці «Automating Open Souurce Inteligence: Algorithms for Osint» [54].

Безпосередній стосунок до теми дослідження мають праці, присвячені зв’язуванню цифрових ідентичностей. Зокрема, С. Буцай та М. Бантан [44] провели систематичний огляд літератури щодо методів ідентифікації персональних даних за допомогою OSINT, констатувавши брак усталених моделей ідентифікації особи. Завдання крос-мережевого зв’язування акантів активно вивчається в міжнародній науковій спільноті; ключові підходи узагальнено К. Шу, С. Ванг та Х. Лю [60].

Мета дослідження полягає в теоретичному обґрунтуванні та аналізі застосування інструментів відкритої розвідки (OSINT) у процесі ідентифікації

цифрової особистості в Україні, а також у визначенні парадигмальних підходів до їх використання в умовах сучасного інформаційного середовища.

Для реалізації мети було поставлено такі **завдання дослідження:**

1. Сформувати понятєво-категорійний апарат дослідження.
2. Визначити теоретичні основи та класифікацію інструментів відкритої розвідки.
3. Проаналізувати сучасний стан та нормативно-правове регулювання цифрової ідентифікації в Україні
4. Дослідити зарубіжний досвід використання OSINT для цифрової ідентифікації.
5. Дослідити ефективність застосування OSINT-інструментів для ідентифікації особи на прикладі кейсів українських організацій.
6. Оцінити ефективність та ризики застосування OSINT-інструментів у сфері цифрової ідентифікації.

Об’єкт дослідження: процес ідентифікації цифрової особистості засобами відкритої розвідки в Україні.

Предмет дослідження: парадигмальні засади застосування інструментів відкритої розвідки у процесі ідентифікації цифрової особистості.

Методологія дослідження. Методологічну основу дослідження становить комплекс загальнонаукових і спеціальних методів, послідовне застосування яких забезпечило реалізацію поставлених завдань. . Вибір методів зумовлений міждисциплінарним характером теми. Для формування понятєво-категорійного апарату застосовано методи термінологічного аналізу та порівняння, що дало змогу зіставити різні підходи до трактування ключових понять і сформулювати робочі дефініції, покладені в основу дослідження. . Систематизацію інструментів OSINT здійснено за допомогою методу класифікації. Аналіз нормативно-правового регулювання цифрової ідентифікації проведено за допомогою аналізу нормативних документів. Для вивчення зарубіжного досвіду використано метод порівняння. Головним

методом став кейс-аналіз, за допомогою якого було досліджено конкретні випадки з діяльності українських організацій.

Наукова новизна роботи полягає в тому, що на основі аналізу реальної діяльності української OSINT-організацій вперше обґрунтовано, що ефективність інструментів відкритої розвідки для ідентифікації інформації не є універсальною, а залежить від дослідницької мети та пріоритетності окремих критеріїв. .

Практична значущість роботи. Матеріали роботи можуть бути використані під час викладання курсів з інформаційної безпеки та OSINT. Виявлені прогалини та порівняльний аналіз зарубіжних моделей можуть бути враховані для регуляції діяльності у сфері відкритої розвідки в Україні.

Апробація роботи. Основні положення та результати кваліфікаційного дослідження були апробовані на XXXI викладацько-студентській конференції «Дні науки» в Національному університеті «Острозька академія». Також участь у XI Міжнародній науково-практичній студентській конференції «Актуальні питання інформаційної діяльності: традиції та інновації», що відбулася у Національному університеті «Одеська політехніка» (26 березня 2026 р.). За матеріалами конференції опубліковано тези доповіді [20] та надано сертифікат учасника конференції (Додаток А).

Структура роботи. Кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та літератури (68 найменувань, із яких – 28 іноземною мовою). Загальний обсяг кваліфікаційної роботи становить 70 сторінок, із них – 57 сторінок основного тексту. Робота містить 6 рисунків, 3 таблиці та 2 додатки.

РОЗДІЛ 1

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ВИКОРИСТАННЯ ІНСТРУМЕНТІВ ВІДКРИТОЇ РОЗВІДКИ (OSINT) У ПРОЦЕСАХ ЦИФРОВОЇ ІДЕНТИФІКАЦІЇ

У першому розділі сформовано поняттєво-категорійний апарат дослідження. Зокрема надано визначення таких основних понять, як OSINT, цифрова особистість, цифрова ідентифікація, цифровий слід, цифрова тінь. Окреслено значення цифрового сліду та цифрової тіні як базових елементів для проведення OSINT-досліджень. Виокремлено теоретичні засади використання інструментів відкритої розвідки. Окрему увагу приділено їхній класифікації за різними критеріями.

1.1. Поняттєво-категорійний апарат дослідження

У межах наукового дослідження, присвяченого застосуванню інструментів відкритої розвідки в процесі ідентифікації цифрової особистості в Україні, особливої ваги набуває чітке визначення та систематизація базових термінів. Формування поняттєво-категорійного апарату дослідження є необхідною передумовою забезпечення теоретичної цілісності роботи, коректності наукового аналізу та однозначності інтерпретації ключових термінів. У цьому контексті актуалізується потреба в уточненні змісту таких понять, як «OSINT», «цифрова особистість», «ідентифікація», «цифровий слід» та «цифрова тінь», з урахуванням сучасних міждисциплінарних підходів. Системне осмислення зазначених дефініцій дозволяє вибудувати концептуальні межі дослідження та створює методологічне підґрунтя для подальшого аналізу обраної проблематики.

Поняття розвідки відкритих джерел (Open Source Intelligence, також OSINT) є ключовим для дослідження, оскільки саме воно визначає межі збору та аналізу інформації у цифровому середовищі. У сучасному науковому та прикладному середовищі OSINT розглядається як окремий напрям розвідувальної та аналітичної діяльності, що ґрунтується на використанні

загальнодоступних інформаційних ресурсів. У найголовнішому розумінні OSINT трактується як концепція, методологія і технологія добування інформації з відкритих джерел з подальшим її використанням для підтримки процесів прийняття рішень у сфері безпеки. У цьому визначенні акцент зроблено на тому, що OSINT містить багато компонентів. Відкрита розвідка розглядається як поєднання підходів, принципів і практик аналітичної роботи з відкритими даними [40].

Інший підхід до визначення OSINT зосереджується на результаті аналітичної діяльності. У цьому випадку відкриті джерела інформації розглядаються як база для отримання розвідувальних даних за допомогою цілеспрямованого збору, оцінки та аналізу загальнодоступної інформації з метою відповіді на конкретне розвідувальне питання. Таким чином, у центрі уваги опиняється не процес збору даних, а їх аналітичне опрацювання та практичне застосування [49].

Ще одне трактування терміну «OSINT» підкреслює комунікативний і часовий вимір розвідувальної інформації. У межах цього підходу OSINT визначається як розвідувальні дані, що створюються на основі загальнодоступної інформації, збираються, використовуються та поширюються серед відповідної аудиторії з метою задоволення конкретних розвідувальних потреб. Тут важливим є не лише факт отримання інформації, а й її своєчасність, адресність та корисність для визначеного кола користувачів [68, с. 9].

Порівняльний аналіз наведених визначень дозволяє підкреслити низку спільних характеристик поняття OSINT. По-перше, всі підходи наголошують на використанні виключно загальнодоступних джерел інформації. По-друге, OSINT розглядається як аналітичний процес, що включає не лише збір, а й оцінку, інтерпретацію та узагальнення даних. По-третє, OSINT орієнтований на вирішення конкретних завдань або потреб, що надає зібраній інформації прикладного значення. Також між наведеними визначеннями простежуються й відмінності. Частина з них фокусується на аспектах OSINT, пов’язуючи його передусім із військовою та політичною сферами, чи національною безпекою.

Інші трактування підкреслюють універсальність методів OSINT та можливість їх застосування у інших цілях.

Відсутність єдиного усталеного визначення OSINT свідчить про міждисциплінарний характер цього поняття та його динамічний розвиток. Залежно від завдань дослідження, розуміння OSINT може зміщуватися з визначення його як елементу розвідувальної діяльності до трактування його як універсального інструменту аналізу відкритої інформації. У межах даного наукового дослідження OSINT розглядається як концептуально-методологічна основа дослідження цифрових слідів особи. Зважаючи на це, під OSINT у роботі розуміється сукупність методів збору, аналізу та інтерпретації загальнодоступної цифрової інформації з метою ідентифікації цифрової особистості.

Не менш важливим для дослідження є термін «цифрова особистість». Оскільки у межах аналізу відкритих джерел саме вона відображає існування та діяльність людини у цифровому середовищі. У наукових джерелах існують різні підходи до визначення цього поняття. В одному з джерел цифрова (або електронна) особистість визначається як сукупність необхідних і достатніх даних у електронній формі, за якими здійснюється ідентифікація людини-володільця аватару та будь-яких електронних даних у кіберпросторі, включно з метавсесвітом. Цей підхід акцентує увагу на юридичному та формалізованому аспектах, підкресює важливість електронної ідентифікації в цифровому середовищі [16, с. 57].

Інший підхід розглядає цифрову особистість як соціальну ідентичність в Інтернеті, що виникає через створення онлайн-профілів і використовується для представлення себе у мережах у соціальному контексті. Тут акцент зміщується на соціальну функцію, спосіб комунікації та взаємодії з іншими у цифровому середовищі [43, с. 158]. Ще один із наукових підходів інтерпретує цифрову особистість як об’єктивовану форму існування особистості в цифровому середовищі, що може репрезентувати як фізичну, так і юридичну особу, а також мати індивідуальний або колективний характер. Цей підхід підкреслює

універсальність і багатовимірність поняття та його здатність відображати різні аспекти присутності в цифровому просторі [1, с. 53].

Завдяки порівнянню наведених підходів можна виділити спільні та відмінні риси. Спільним для всіх трактувань є те, що термін «цифрова особистість» відображає присутність людини у цифровому середовищі і пов'язана з її ідентифікацією та соціальними функціями. Водночас різні підходи акцентують увагу на юридичних, соціальних або об'єктивних аспектах, що зумовлює потребу формування робочого визначення у межах конкретного дослідження. У межах нашого наукового дослідження термін «цифрова особистість» розглядається як сукупність даних, онлайн-профілів та віртуальних проявів особи, що відображають її присутність у цифровому середовищі та дозволяють ідентифікувати її як об'єкт аналізу OSINT.

Ідентифікація є базовим поняттям для досліджень, пов'язаних з аналізом цифрової інформації та діяльністю у кіберпросторі, адже саме вона забезпечує можливість встановлення тотожності суб'єкта або об'єкта в інформаційних системах. У наукових і прикладних джерелах це поняття трактується по-різному залежно від його застосування. У найзагальнішому значенні ідентифікація розуміється як упізнання кого-небудь або чого-небудь. Таке тлумачення відображає універсальний і базовий характер поняття, який лежить в основі всіх подальших, більш спеціалізованих підходів [13].

У технічному та інформаційному контексті ідентифікація розглядається як процедура розпізнавання суб'єкта, що здійснюється за допомогою певного ідентифікатора: логіну, ідентифікатора процесу або інших унікальних облікових даних. У цьому підході ключового значення набуває вимога унікальності ідентифікатора, що дозволяє чітко відрізняти одного суб'єкта від іншого в межах інформаційної системи [4].

Інше визначення акцентує увагу на ідентифікації як засобі встановлення тотожності особи або її повноважень у системі. У цьому випадку ідентифікація пов'язується як із сукупністю загальних та індивідуальних даних особи, так і з

використанням механізмів доступу, зокрема паролів. Такий підхід поєднує особистісний та функціональний аспекти ідентифікації [31].

Порівняння наведених визначень дозволяє зробити висновок, що ідентифікація завжди передбачає процес встановлення відповідності між суб'єктом та набором ознак або даних, за допомогою яких цей суб'єкт може бути розпізнаний. Водночас відмінності між підходами полягають у рівні деталізації та сфері застосування. У межах цього наукового дослідження ідентифікація розглядається як процес встановлення тотожності цифрової особистості або підтвердження її повноважень на основі сукупності унікальних даних, отриманих з відкритих джерел.

Наступним поняттям, яке варто розглянути є термін «цифровий слід». У наукових дослідженнях термін «цифровий слід» розглядається як сукупність даних, що виникають у процесі взаємодії користувача з цифровим середовищем. У загальному розумінні цифровий слід визначається як інформація, яку користувач залишає у кіберпросторі добровільно чи мимоволі. Такий підхід акцентує увагу на неминучості формування цифрових даних у процесі онлайн-активності незалежно від намірів користувача [55, с. 1033].

Інший підхід зосереджується на керованості цифрового сліду, розглядаючи його як персональні дані, на які користувач може впливати повністю або частково. У цьому контексті цифровий слід постає як явище, що певною мірою піддається контролю з боку суб'єкта, хоча цей контроль часто є обмеженим технічними та організаційними умовами цифрового середовища [28, с. 197].

Водночас окремі визначення підкреслюють практичну та ідентифікаційну значущість цифрового сліду. Згідно з ними, термін «цифровий слід» – це інформація, залишена користувачем у мережі, за допомогою якої можливо не лише ідентифікувати особу, а й встановити зв'язок між нею та певними діями, подіями або навіть відновити окремі фрагменти її біографії. Такий підхід безпосередньо пов'язує цифровий слід з процесами аналізу поведінки та цифрової ідентифікації [6, с. 34].

Спільним у цих визначеннях є розуміння цифрового сліду як результату діяльності користувача у цифровому просторі та джерела інформації про нього. Відмінності полягають у ступені акцентування на контрольованості даних і їх ідентифікаційному потенціалі. У межах нашого дослідження термін «цифровий слід» доцільно розуміти як сукупність відкритих даних, сформованих у процесі взаємодії користувача з цифровим середовищем, які можуть бути використані для ідентифікації особи, аналізу її дій та встановлення зв'язків між окремими інформаційними фрагментами. Таке трактування дозволяє розглядати цифровий слід як базовий елемент для застосування інструментів відкритої розвідки у процесах цифрової ідентифікації.

Зокрема, цифрові сліди можуть бути активними чи пасивними. Активний цифровий слід – це інформація, яку користувач свідомо поширює в мережі Інтернет. Це можуть бути публікації в соціальних мережах, заповнення онлайн-форм, прийняття налаштувань файлів cookie тощо. Пасивний цифровий слід – це дані які користувач залишає ненавмисно,або в деяких випадках, навіть не знаючи про це. Наприклад, веб-сайти, записують IP-адресу користувача без його згоди. Також пасивним інформаційним слідом може бути інформація про місцезнаходження, отримана з фотографії, опублікованої в соціальних мережах тощо [64].

Деякі дослідники поряд із поняттям «цифровий слід» використовують термін «цифрова тінь», який є менш усталеним, але важливим для аналізу процесів цифрової ідентифікації. Цифрову тінь розглядають як категорію персональних даних, поширення яких користувач не контролює або не усвідомлює. На відміну від інших форм присутності у цифровому середовищі, цифрова тінь формується поза прямою волею суб'єкта [28, с. 198].

Окремі підходи трактують термін «цифрова тінь» як інформацію про користувача, що створюється без його безпосередньої участі. Вона виникає внаслідок дій третіх осіб або автоматизованих процесів, зокрема під час пошуку користувача в мережі, обробки контактних списків, розсилок. У такому розумінні термін «цифрова тінь» є наслідком соціальної та технічної взаємодії,

а не свідомої активності самого користувача [6, с. 34]. Інший підхід акцентує увагу на неусвідомленості формування цифрової тіні та її відмінність від даних, які користувач може свідомо регулювати або контролювати [5, с. 19].

Порівняння наведених визначень дозволяє виокремити спільні ознаки поняття «цифрова тінь». Всі підходи наголошують на відсутності контролю з боку користувача. Цифрова тінь розглядається як результат опосередкованих або автоматизованих процесів у цифровому середовищі. Відмінності між визначеннями полягають у ступені акцентування на джерелах формування такої інформації. Загалом, за своєю суттю цифрова тінь подібна до пасивного цифрового сліду. Різниця між ними полягає у тому , що пасивний цифровий слід – це дані, які користувач залишає ненавмисно, а цифрова тінь – це сукупність інформації, сформована на основі тих даних. У межах цього дослідження цифрову тінь доцільно розуміти як сукупність інформації про користувача, що формується у цифровому середовищі без його прямої участі та не підлягає прямому контролю з його боку. Таке трактування є важливим для аналізу цифрової ідентифікації, оскільки цифрова тінь може містити важливі дані і доповнювати інформацію, отриману раніше.

У результаті розгляду ключових понять було сформовано понятійний апарат який є теоретичною основою для систематизації інструментів відкритої розвідки та застосовується у подальших етапах дослідження (Табл. 1.1).

Таблиця 1.1

Визначення основних понять дослідження

Поняття	Визначення
OSINT	Сукупність методів збору й аналізу загальнодоступної цифрової інформації з метою ідентифікації цифрової особистості [40], [49], [68].
Цифрова особистість	Сукупність даних, профілів та віртуальних проявів особи, що відображають її присутність у цифровому середовищі та дозволяють ідентифікувати її [1], [16], [43].

Продовження таблиці 1.1

Ідентифікація	Процес встановлення тотожності цифрової особистості або підтвердження її повноважень на основі сукупності унікальних даних, отриманих з відкритих джерел [4], [13], [31].
Цифровий слід	Сукупність відкритих даних, сформованих у процесі взаємодії користувача з цифровим середовищем, які можуть бути використані для ідентифікації особи [6], [28], [55].
Цифрова тінь	Сукупність інформації про користувача, що формується у цифровому середовищі без його безпосередньої участі або усвідомлення та не підлягає прямому контролю з його боку [5], [6], [64].

Джерело: складено автором

Таким чином, у межах даного дослідження було систематизовано та уточнено поняттєво-категорійний апарат, що забезпечує концептуальну цілісність і методологічну коректність аналізу процесів ідентифікації цифрової особистості із застосуванням інструментів відкритої розвідки.

У дослідженні визначено зміст і співвідношення таких базових категорій, як «OSINT», «цифрова особистість», «ідентифікація», «цифровий слід» та «цифрова тінь», що дозволило розкрити їх функціональне значення в контексті сучасного інформаційного середовища України. Уточнення цих понять сприяло формуванню цілісного наукового бачення процесів збору, аналізу та інтерпретації відкритих даних у межах ідентифікації цифрової особистості.

Застосування парадигмального підходу до формування поняттєво-категорійного апарату дозволило розглянути досліджувану проблематику крізь призму трансформацій інформаційного суспільства, цифровізації соціальних процесів та зростання ролі відкритих інформаційних ресурсів. Це забезпечило узгодженість теоретичних положень дослідження з сучасними науковими підходами у сфері інформаційної аналітики, кібербезпеки та соціальних комунікацій.

1.2. Теоретичні основи та класифікація інструментів відкритої розвідки (OSINT)

Інструменти OSINT забезпечують практичну реалізацію методів збору та аналізу інформації. У сучасному цифровому середовищі обсяг відкритих даних є надзвичайно великим, що унеможливлює їх ефективне опрацювання без використання спеціалізованих інструментів.

У структурі відкритої розвідки інструменти з'єднують джерела інформації та результат аналізу. Вони дозволяють здійснювати пошук, фільтрацію, систематизацію та первинну обробку даних, отриманих з відкритих ресурсів, зокрема вебсайтів, соціальних мереж, онлайн-платформ та відкритих реєстрів. Таким чином, інструменти OSINT слугують засобом досягнення поставлених розвідувальних завдань. Вибір інструментів безпосередньо залежить від цілей дослідження та типу інформації, яку необхідно отримати. Наприклад, для збору базових відомостей про цифрову особистість використовуються інструменти пошуку та агрегації даних, а для поглибленого аналізу можуть застосовуватися засоби візуалізації зв'язків або перевірки достовірності інформації. Отже, ефективність розслідування значною мірою визначається якісним добором інструментів.

Важливою характеристикою інструментів OSINT є їх універсальність та доступність оскільки більшість з них ґрунтується на роботі з відкритими джерелами і не потребує доступу до закритих даних. Це робить їх придатними для використання у різних сферах. Наприклад, застосування в наукових дослідженнях, журналістиці, аналітичній діяльності та сфері інформаційної безпеки. Водночас застосування інструментів відкритої розвідки потребує критичного підходу до отриманих результатів. Дані з відкритих джерел можуть бути неповними, застарілими чи викривленими, що створює необхідність їх перевірки та співставлення з іншими джерелами. У цьому контексті інструменти потрібно розглядати як елемент аналітичного процесу,

ефективність якого залежить не лише від технічних можливостей, а й від компетентності дослідника.

Одним із підходів до систематизації інструментів відкритої розвідки є їх класифікація за типом джерел інформації (Рис. 1.1). Такий поділ базується на походженні даних і специфіці інформаційного середовища, яке визначає методи збору, аналізу та інтерпретації інформації. Інструменти аналізу соціальних мереж (Blackbird, WhatsMyName, Socsal Searcher) спрямовані на роботу з даними, що розміщуються користувачами у соціальних медіа. Вони дозволяють збирати дані про профілі, публікації та активність користувачів. Такі інструменти є важливими для дослідження цифрової особистості, адже соціальні мережі є основним простором її формування та прояву.

Рис. 1.1 Класифікація інструментів OSINT за типом джерел інформації

Джерело: складено автором на основі джерел [60, 65, 66].

Інструменти роботи з вебресурсами (Wayback Machine, Wappalyzer, Shodan) охоплюють аналіз відкритих даних, розміщених на вебсайтах, форумах, блогах тощо. Вони застосовуються для дослідження структури сайтів, змісту публікацій, а також зв’язків між різними інтерент-ресурсами. Ці інструменти дозволяють відстежувати інформаційний контекст та динаміку поширення відкритих даних у мережі.

Інструменти аналізу відкритих баз даних (OpenCorporates, OpenSanctions, Wikidata) забезпечують доступ до інформації, що міститься у державних реєстрах, судових базах, корпоративних реєстрах тощо. Такі інструменти використовуються для отримання перевірених фактів, а також підтвердження або спростування інформації, отриманої з інших джерел.

Інструменти мультимедійного аналізу (TinEye, FotoForensics, ExifTool) дозволяють здійснювати аналіз зображень, відео й аудіо файлів, зокрема шляхом дослідження метаданих, зворотнього пошуку зображень та перевірки автентичності контенту. У відкритій розвідці такі інструменти відіграють важливу роль у верифікації інформації та виявленні маніпулятивних або фальсифікованих матеріалів.

Геопросторові інструменти (Google Earth, OpenStreetMap, NASA Worldview) орієнтовані на аналіз просторових даних і використовують картографічну інформацію, супутникові знімки та дані геолокації. Вони дають можливість визначати місце подій, аналізувати просторові зв’язки та уточнювати географічний контекст отриманих даних. Застосування таких інструментів розширює можливості OSINT-досліджень.

Іншим важливим підходом до систематизації інструментів відкритої розвідки є їх класифікація за функціональним призначенням (Рис. 1.2.). Такий поділ відображає послідовні етапи роботи з інформацією від її пошуку до представлення результатів. Пошукові інструменти (Google, Startpage, Sherlock) призначені для первинного збору інформації з відкритих джерел. Вони використовуються на початковому етапі дослідження та забезпечують доступ до масиву відкритих даних. За допомогою таких інструментів здійснюється пошук відомостей у мережі Інтернет, соціальних медіа, відкритих базах даних та інших ресурсах. Їх основна функція полягає у швидкому виявленні інформації за заданими параметрами.

Рис. 1.2 Класифікація інструментів OSINT за функціональним призначенням

Джерело: складено автором на основі джерел [60, 65, 66].

Аналітичні інструменти (SpiderFoot, Maltego, Censys) застосовуються для обробки зібраних даних та виявлення логічних і структурних зв'язків. Вони допомагають систематизувати інформацію, аналізувати взаємозв'язки між об'єктами, а також формувати узагальнені висновки. У межах OSINT такі інструменти відіграють ключову роль у перетворенні розрізнених відомостей та важливої для аналізу інформації.

Інструменти верифікації (Mapillary, InVID, ExifTool) забезпечують перевірку достовірності отриманих даних. Вони використовуються для підтвердження або спростування інформації завдяки порівнянню з іншими джерелами, аналізу метаданих, перевірки часу, місця та умов появи інформаційного матеріалу. Застосування інструментів верифікації є необхідним елементом досліджень, оскільки відкриті джерела не завжди містять точні та оперативні дані.

Візуалізаційні інструменти (Gephi, Palladio, Kumu) призначені для наочного представлення результатів OSINT-дослідження. Вони дають можливість відображати результати аналізу у вигляді графіків, схем або інших форм візуалізацій. Графічне зображення, здійснене за допомогою цих інструментів, сприяє полегшенню інтерпретації результатів та кращому

розумінню складних зв'язків між об'єктами особливо підготовки звітів про виконане дослідження.

Процес відкритої розвідки передбачає послідовне виконання кількох пов'язаних між собою етапів, кожен з яких має власні завдання та методи роботи з інформацією. У цьому контексті інструменти OSINT доцільно класифікувати за етапами дослідження, на яких вони застосовуються (Рис. 1.3).

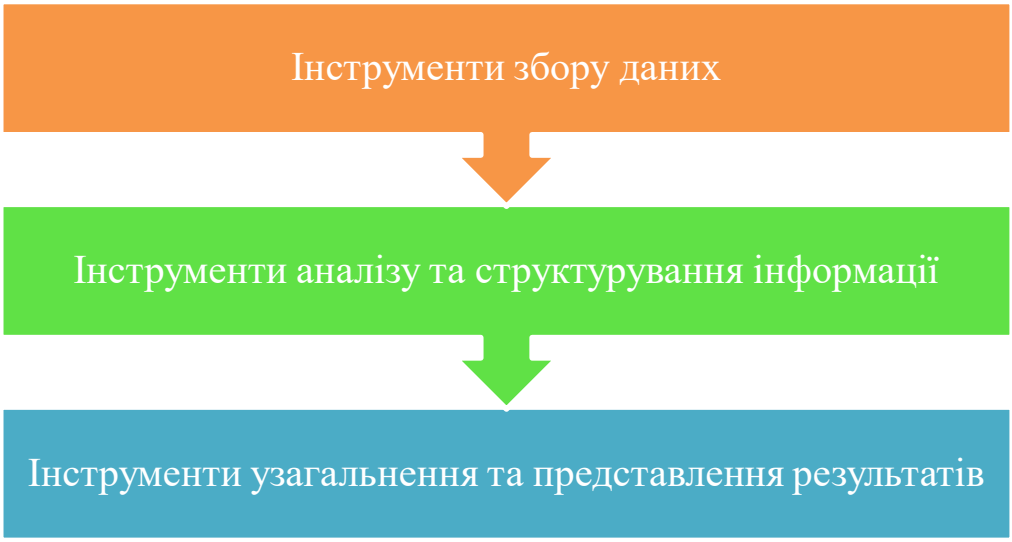

Рис. 1.3 Класифікація інструментів OSINT за етапами дослідження

Джерело: складено автором на основі джерел [60, 65, 66].

Інструменти збору даних (TGSat, Bing, DNSlytics) використовуються на початковому етапі OSINT-дослідження та призначені для отримання інформації з відкритих джерел. Вони забезпечують доступ до різних типів даних, що розміщені у відкритому інформаційному просторі. Основною функцією цих інструментів є накопичення первинного масиву даних, який у подальшому підлягає аналізу та обробці.

Інструменти аналізу та структурування інформації (Hunchly, Tableau, OpenRefine) застосовуються на етапі опрацювання зібраних даних. Вони слугують для впорядкування інформації, виявлення зв'язків між окремими елементами, класифікації та групування даних за визначеними ознаками. Використання таких інструментів сприяє логічному перетворенню неструктурованих відомостей та робить їх придатними для подальшого узагальнення.

Інструменти узагальнення та представлення результатів (Flourish, QGIS, Zotero) застосовуються на завершальному етапі дослідження. Вони орієнтовані на формування висновків і подання результатів у зрозумілій формі. За допомогою цих інструментів результати дослідження можуть бути представлені у вигляді схем, таблиць, графіків тощо, що полегшує використання в аналітичній або науковій діяльності.

Класифікація інструментів відкритої розвідки має важливе значення для дослідження цифрової особистості, оскільки дозволяє впорядкувати різні джерела та методи роботи. Систематизація інструментів OSINT створює методологічну основу для послідовного аналізу інформації, що характеризує присутність особи у цифровому середовищі. Практична цінність класифікації полягає у можливості раціонального вибору інструментів залежно від поставлених завдань дослідження. Поділ інструментів за типом джерел інформації, функціональним призначенням та етапами дослідження дозволяє ефективно організувати процес збору та аналізу даних, уникнути дублювання інформації та зосередитися на релевантних джерелах. Це особливо важливо під час роботи з великими масивами відкритих даних.

Таким чином, зв’язок класифікації OSINT інструментів з ідентифікацією цифрової особистості проявляється у можливості поетапного встановлення та підтвердження інформації про суб’єкта у цифровому просторі. Використання пошукових інструментів забезпечує первинне виявлення цифрових слідів особи, аналітичні та верифікаційні інструменти дозволяють зіставляти дані з різних джерел і перевіряти їх достовірність, а візуалізаційні інструменти сприяють формуванню цілісного уявлення про цифрову особистість. Обґрунтування вибору інструментів для аналізу базується саме на запропонованій класифікації. Вона дозволяє аргументовано визначити, які інструменти є доцільними для дослідження цифрової особистості.

Висновки до першого розділу

У межах даного розділу здійснено теоретико-методологічне обґрунтування дослідження застосування інструментів відкритої розвідки в процесі ідентифікації цифрової особистості, що дозволило сформувати цілісне наукове підґрунтя для подальшого аналізу обраної проблематики. Особливу увагу приділено систематизації та уточненню понятєво-категорійного апарату.

Обґрунтовано розгляд OSINT як концептуально-методологічної основи аналізу цифрових слідів і цифрової тіні особи. Визначено, що саме сукупність відкритих цифрових даних, сформованих внаслідок активної та пасивної присутності людини в мережі, становить інформаційну базу для ідентифікації цифрової особистості. Розмежування понять «цифровий слід» і «цифрова тінь» дозволило глибше осмислити джерела формування інформації про особу та рівень контролю над нею, що є принципово важливим у контексті відкритої розвідки.

Також проаналізовано теоретичні засади та здійснено класифікацію інструментів відкритої розвідки. Доведено, що інструменти OSINT відіграють ключову роль у реалізації аналітичного потенціалу відкритих джерел, забезпечуючи пошук, обробку, верифікацію та візуалізацію даних. Запропонована класифікація інструментів за типом джерел інформації, функціональним призначенням та етапами дослідження створює методологічну основу для впорядкованого та послідовного аналізу цифрової особистості.

РОЗДІЛ 2

АНАЛІЗ ПРАКТИКИ ЗАСТОСУВАННЯ OSINT-ІНСТРУМЕНТІВ ДЛЯ ІДЕНТИФІКАЦІЇ ЦИФРОВОЇ ОСОБИСТОСТІ В УКРАЇНІ ТА ЗА КОРДОНОМ

У другому розділі проаналізовано сучасний стан та нормативно-правове регулювання цифрової ідентифікації в Україні. Узагальнено зарубіжний досвід використання інструментів відкритої розвідки в ідентифікації цифрової особистості. Здійснено порівняльний аналіз українського та іноземного підходів.

2.1. Сучасний стан та нормативно-правове регулювання цифрової ідентифікації в Україні

Цифрова ідентифікація в Україні формується у двох правових площинах: забезпечення права людини на особисте життя та юридичне закріплення механізмів електронної ідентифікації. Тобто, держава одночасно створює інструменти для дистанційного підтвердження особи і паралельно встановлює запобіжники проти неправомірного збору та використання даних, які супроводжують ці процеси.

Базовим нормативним актом для цифрової ідентифікації є стаття 32 Конституції України, яка закріплює заборону втручання в особисте і сімейне життя та прямо встановлює, що не допускається збирання, зберігання, використання і поширення конфіденційної інформації про особу без її згоди, окрім випадків, визначених законом і лише в інтересах національної безпеки, економічного добробуту та прав людини [30]. Будь-яка система, що підтверджує особу онлайн, фактично здійснює обробку інформації про особу, тобто входить у сферу конституційної охорони приватності. Тобто цифрова ідентифікація в Україні не повинна розглядатися як лише технічна процедура. Вона є юридично значущим процесом, у якому необхідно дотримуватися принципів пропорційності втручання в приватне життя.

Додатково це підтверджується правовою позицією Конституційного Суду України щодо змісту права на недоторканність приватного та сімейного життя. Суд виходить із того, що обмеження цього права є допустимим лише за умови дотримання принципу пропорційності та непорушення його сутнісного змісту [22]. У контексті цифрової ідентифікації це означає що навіть за умови запровадження державною спеціальних режимів доступу до даних або посилення контрольних механізмів, вона має довести необхідність цих заходів.

Наступний рівень регулювання забезпечує Закон України «Про інформацію». Він формує загальні правила щодо інформації, у тому числі щодо інформації про фізичну особу, яка має ознаки конфіденційності та потребує спеціального доступу. Цей закон важливий для дослідження цифрової ідентифікації, тому що, визначає правовий статус даних та послідовність їх обігу, а саме що може бути відкритим, що є обмеженням у доступі, які підстави та межі поширення [26]. У практиці цифрової ідентифікації дія цього закону проявляється в узгодженні відкритості даних та права особи на приватність. Також цей законодавчий акт є частиною нормативної бази для застосування OSINT. Частина персональних даних може бути розміщена у відкритих інформаційних системах, проте це не дає права на їх вільне використання. Правила, за якими обробляються такі дані, залежать не тільки від їхньої відкритості, а й від характеру самої інформації та від підстав обробки. Важливо чітко розмежовувати випадки, коли збирання даних здійснюються в межах правового поля, і ситуації, в яких такі дії стають порушенням законодавства.

Попередні нормативно-правові акти визначають межі та правила обробки даних, тоді як Закон України «Про електронну ідентифікацію та електронні довірчі послуги» закріплює механізми, через які цифрова ідентифікація набуває юридичної значущості. Зазначений Закон регулює сферу електронної ідентифікації та довірчих послуг, зокрема пов’язаних з кваліфікованим електронним підписом, електронними печатками, часовими мітками тощо, визначає вимоги до надавачів таких послуг та до рівнів довіри [24].

Цифрову ідентифікацію в Україні побудовано на реєстровій моделі. Підтвердження особи в інтернеті здійснюється через верифікацію атрибутів (ПІБ, дата народження, документ, РНОКПП тощо) з даними державних реєстрів. Саме тому Закон України «Про публічні електронні реєстри» є важливою нормативним актом. Він регламентує створення, ведення, взаємодію реєстрів, принципи їх функціонування та вимоги до даних як до критичного державного ресурсу [27].

Коли стандартизація реєстрів зростає, процеси ідентифікації стають надійнішими, зменшується дублювання інформації і з'являються чіткі правила взаємодії. Проте інтеграція реєстрів означає зростання цінності їхніх даних. Наслідком цього стає підвищення ризиків пов'язаних з доступом до інформації. Закон України «Про електронні документи та електронний документообіг» визначає правові засади електронного документообігу та використання електронних документів. Це важливо, бо цифрова ідентифікація часто завершується створенням або підписанням електронного документа, а отже потребує правового визнання електронної форми [23].

Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» визначає правові засади функціонування системи документів, що посвідчують особу, а також регулює обіг демографічних даних як ключових ідентифікаційних атрибутів . У межах цифрової ідентифікації цей закон важливий тим, що встановлює первинні атрибути особи, які далі відображаються у цифрових системах та використовуються для верифікації [25].

Нормативно-правова база цифрової ідентифікації в Україні має багаторівневу структуру (Рис 2.1.). Конституційний рівень закріплює недоторканність приватного життя та межі обробки конфіденційної інформації про особу. Загальні інформаційні акти встановлюють правила доступу до персональних даних та інформації загалом. Спеціальне законодавство про персональні дані деталізує підстави для обробки, самі правила та

відповідальність за їх порушення. Спеціальне законодавство про електронну ідентифікацію надає цифровій ідентифікації юридичну силу. Закон про реєстри забезпечує інфраструктурну основу цифрової ідентичності. При цьому підвищує значення безпеки і контролю обігу даних. Усе це створює умови для розвитку цифрово ідентифікації в Україні як інструменту електронних послуг.

Рис. 2.1. Структура нормативно-правової бази цифрової ідентифікації в Україні

Джерело: складено автором.

Ефективність нормативно-правового регулювання цифрової ідентифікації значною мірою залежить від його реалізації. В Україні система цифрової ідентифікації поєднує органи формування державної політики, органи технічного і криптографічного забезпечення, а також суб'єкти контролю за дотриманням прав людини у сфері обробки персональних даних. Така структура є необхідною з огляду на комплексний характер цифрової ідентичності як явища.

Ключову роль у формуванні політики цифрової ідентифікації відіграє Міністерство цифрової трансформації України. Відповідно до положення про міністерство, воно забезпечує формування та реалізацію державної політики у сферах цифровізації, електронного урядування, розвитку електронних довірчих послуг та електронної ідентифікації. У межах ідентифікації цифрової особистості Міністерство цифрової трансформації України :

- координує розвиток державних електронних сервісів;
- забезпечує інтеграцію державних реєстрів;
- формує стандарти взаємодії інформаційних систем;
- бере участь в адаптації українського законодавства до європейських вимог у сфері електронної ідентифікації [19]. Міністерство впровадило національне цифрове середовище, основою якого є інтеграція реєстрів та використання електронних атрибутів особи для доступу до послуг. У цьому контексті інституційна роль Мінцифри полягає не лише у створенні сервісів, а й у визначенні моделі цифрової особистості як об'єкта правового регулювання.

Не менш важливою є діяльність Державної служби спеціального зв'язку та захисту інформації України, яка здійснює державну політику у сфері захисту інформації, кіберзахисту та криптографічного забезпечення. Цей орган встановлює вимоги до систем захисту інформації та здійснює контроль у сфері технічного та криптографічного захисту інформації. Також забезпечує функціонування кваліфікованих надавачів електронних довірчих послуг і координує заходи безпеки щодо державних інформаційних ресурсів [9]. Тобто, цей державний орган формує технічну основу довіри до цифрової ідентифікації. Якщо Міністерство цифрової трансформації відповідає за політичну та сервісну архітектектуру, то Держспецзв'язку забезпечує її захищеність та відповідність стандартам безпеки .

У системі забезпечення захисту персональних даних також варто розглянути діяльність Уповноваженого Верховної Ради України з прав людини, який відповідно до Закону України «Про захист персональних даних» здійснює контроль за дотриманням законодавства у цій сфері. У межах цифрової ідентифікації функції Омбудсмана полягають у розгляді скарг суб'єктів персональних даних, застосуванні заходів реагування у разі порушень, тлумаченні норм щодо правомірності обробки даних [33]. Таким чином, інститут Омбудсмана виступає гарантом того, що розширення цифрових інструментів ідентифікації не призведе до порушення права на особисте життя.

Окремим елементом державної системи ідентифікації цифрової особистості є залучення правоохоронних органів до використання та аналізу цифрових даних у межах кримінальних проваджень та оперативно-розшукової діяльності. У цій площині функціонують: Служба безпеки України, Національна поліція України та Бюро економічної безпеки України. Їхня діяльність пов'язана з використанням цифрових слідів, аналізом відкритих джерел інформації, встановленням осіб у межах кримінального процесу. У цьому контексті цифрова ідентифікація виступає інструментом формування доказів, реагування на загрози безпеці. Проте саме тут виникає зона перетину між державними повноваженнями та правом на приватність. Використання цифрових ідентифікаційних даних у правоохоронній діяльності потребує чіткого нормативного регулювання.

Важливим учасником системи цифрової ідентифікації є банківський сектор. Координацію у цій сфері здійснює Національний банк України, який встановлює вимоги до ідентифікації клієнтів фінансових установ. Банківські механізми ідентифікації є одними з ключових, оскільки фінансові дані часто виступають додатковим підтвердженням особи в електронному середовищі. Цифрова ідентифікація в Україні характеризується інтеграцією державного та приватного секторів. Також спостерігається розподіл функцій та посилена роль безпекових органів в умовах воєнного стану. Цифрова особистість формується цілою мережею організацій, що генерують, обробляють і зберігають різні дані. Саме це створює передумови для підвищення ефективності ідентифікації, але збільшує ризики для цілісності даних.

Цифрова ідентифікація в Україні відбувається через конкретні технологічні інструменти. Вони забезпечують автентифікацію особи, підтвердження її статусу та взаємодію з електронними сервісами. Сукупність цих інструментів формує модель цифрової особистості, в якій ідентифікаційні атрибути зберігаються, передаються та перевіряються в електронному середовищі. Центральним елементом державної моделі цифрової ідентифікації є Дія. До її основних функцій входить: відображення цифрових документів,

електронна автентифікація користувача, отримання адміністративних послуг онлайн. Усі ці послуги відбуваються завдяки інтеграції з державними реєстрами для верифікації даних [10].

Юридична значущість цифрових документів у застосунку ґрунтується на положеннях законодавства про електронні довірчі послуги та про Єдиний державний демографічний реєстр. Цифровий паспорт у «Дії» не є окремим документом, а відображає інформацію з відповідного державного реєстру. Відповідно, це підтверджує принцип реєстрової моделі ідентифікації. З точки зору аналізу цифрової особистості, «Дія» виконує роль агрегатора атрибутів. Вона репрезентує наявну інформацію в зручному інтерфейсі. Водночас інтеграція великої кількості реєстрів посилює роль кіберзахисту та механізмів контролю доступу. Адже витік даних з одного облікового запису може надати доступ до широкого спектра персональних даних. .

Кваліфікований електронний підпис (КЕП) є одним з базових механізмів юридично значущої ідентифікації особи в електронному середовищі. Його правовий статус визначається Законом України «Про електронну ідентифікацію та електронні довірчі послуги». Зокрема, КЕП забезпечує підтвердження особи підписувала, цілісність електронного документа та неможливість забезпечення факту підписання. На відміну від звичайної автентифікації, КЕП базується на криптографічних механізмах і має вищий рівень довіри [11]. У практиці цифрової ідентифікації він використовується для підписання договорів, подання звітності, участі в електронних закупівлях, реєстраційних процедур тощо. З позиції OSINT-досліджень електронний підпис сам по собі не є відкритим джерелом інформації. Проте його використання у публічних реєстрах може залишати цифрові сліди, які підлягають аналізу.

Суттєвим інструментом дистанційної ідентифікації є система BankID, що координується Національним банком України. Механізм BankID дозволяє підтвердити особу шляхом передачі банком ідентифікаційних даних клієнта суб’єкту надання послуги [38]. У цьому процесі банк виступає довіреним посередником. Значною перевагою BankID є те, що ідентифікація може

здійснюватися без фізичної присутності особи. Водночас ця модель зберігає великі масиви персональних даних, що створює додаткові ризики витоків.

MobileID базується на використанні SIM-карт із криптографічним захистом, що дозволяють здійснювати електронну ідентифікацію та підписання документів через мобільний пристрій [37]. Крім того, застосовуються інші способи електронної ідентифікації, наприклад одноразові коди підтвердження, двофакторна автентифікація, біометричні методи тощо. Використання біометричних атрибутів підвищує рівень захисту доступу, але ставить питання щодо зберігання та обробки біометричних даних як чутливої категорії персональних даних.

Усі зазначені інструменти функціонують разом з публічними електронними реєстрами. Саме реєстри забезпечують первинність ідентифікаційних даних (паспортних відомостей, інформації про місце проживання, статус підприємця, судові рішення тощо). Інтеграція реєстрів дозволяє перевіряти достовірність інформації та забезпечити достатню швидкість надання послуг. Саме завдяки реєстровій моделі виникає значний потенціал для того, щоб співвідносити між собою дані з різних джерел. Якщо окремі реєстри мають відкритий доступ, їх комбінування дозволяє сформувати розширений профіль особи.

В Україні сформувалася багатокомпонентна система державних цифрових інструментів ідентифікації. Вона забезпечує високу доступність до послуг і сприяє цифровізації державного управління. Однак концентрація й тісна взаємодія великих масивів персональних даних підвищують ризики для інформаційної безпеки. У контексті OSINT важливо враховувати, що електронні ідентифікаційні інструменти генерують цифрові сліди. Вони можуть використовуватися і для досліджень, і для порушення прав особи.

Україна поступово формує модель цифрової ідентифікації, що орієнтується на європейські стандарти. Повна гармонізація потребує подальшого вдосконалення національного законодавства, посилення інституційного контролю та забезпечення міжнародної сумісності електронних

засобів ідентифікації. Розвиток цифрової ідентифікації в Україні відбувається паралельно з розширенням електронних сервісів, інтеграцією реєстрів і зростанням обсягів даних, що циркулюють у цифровому середовищі. Це підвищує ефективність взаємодії громадян із державою.

Основні проблеми правового регулювання цифрової ідентифікації в Україні пов'язані із необхідністю забезпечення балансу між відкритістю даних і правом на приватність. Додатковим фактором ризику виступає поглиблена інтеграція державних реєстрів та концентрація значної кількості персональних даних в інформаційних системах. Це підвищує наслідки можливих технічних збоїв або неправомірного доступу. Також складності зумовлені зміною режимів доступу до інформації в умовах воєнного стану, що актуалізує потребу у чіткості підстав і прозорості таких обмежень. Окрему проблему становить загроза суспільній довірі до цифрових сервісів через повідомлення про можливі витоки даних. Такі ситуації вимагають від держави ефективного реагування та комунікації. Водночас залишається потреба в оновленні законодавства про захист персональних даних та його подальшому наближенні до стандартів Європейського Союзу. Станом на сьогодні в національному законодавстві відсутній спеціальний нормативний акт, який би прямо визначав поняття OSINT або встановлював порядок його застосування в процесах цифрової ідентифікації.

Застосування інструментів аналізу відкритих джерел інформації фактично здійснюється в межах діяльності правоохоронних органів, журналістських розслідувань, фінансового моніторингу тощо. Таким чином, OSINT в Україні існує як частково дозволена практика, що базується на загальних нормах інформаційного законодавства про персональні дані та спеціальних актах у сфері безпеки і правопорядку.

Державний сектор володіє найбільшим доступом до персональних даних і певними повноваженнями, тому у більшості випадків не потребує використання відкритої розвідки або не афішує її застосування. Натомість громадський та приватний сектор демонструє значно більшу активність. Вони застосовують

OSINT для документування воєнних злочинів, виявлення інформаційних операцій, встановлення причетних осіб, реконструкції подій тощо. Така діяльність стала особливо помітною після 2014 року і посилилася з 2022 року, коли зріс суспільний запит на перевірену інформацію. Цим займаються команди і проекти різного масштабу, як великі медійні редакції так і менші волонтерські ініціативи.

Приватний сегмент може бути проілюстрований діяльністю Molfar, яка позиціонує себе як приватну розвідувальну агенцію з акцентом на застосуванні методів OSINT, а також здійснює бізнес-аналітику [56]. Громадський сегмент репрезентує InformNapalm, що публікує OSINT-розслідування на різну тематику [53]. Журналістський сектор демонструє практичне застосування OSINT через навчальні курси наприклад, Слідство.Інфо заявило метою своїх тренінгів навчання журналістів ідентифікувати осіб за допомогою технологій OSINT та роботи з відкритими інформаціями майданчиками [36].

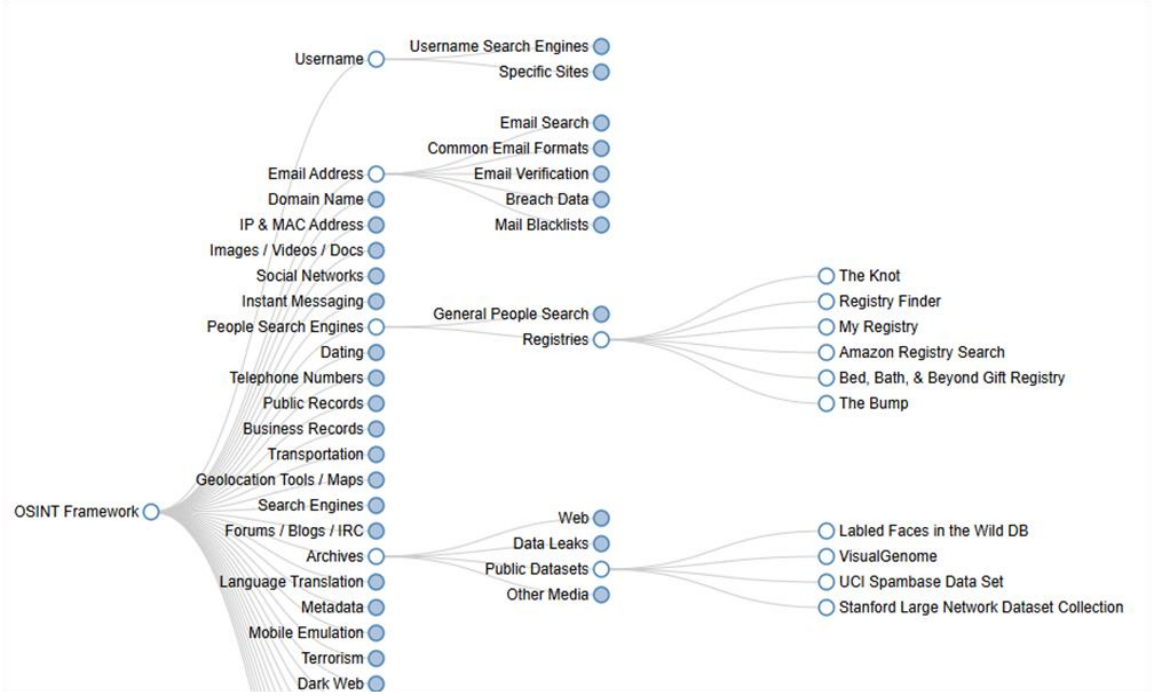

Рис. 2.2 Приклади групування інструментів у каталозі OSINT Framework

Джерело: [59]

Для систематизації пошуку у відкритих джерелах часто використовують каталоги інструментів і ресурсів, наприклад OSINT Framework (Рис 2.2.). Це відкритий веб-каталог, який структурує інструменти та ресурси для збору

інформації. На цьому сайті запропоновані, переважно, безкоштовні ресурси. Він слугує довідником для дослідників, подаючи різні джерела та інструменти, погруповані за сферою застосування [59].

На первинному етапі OSINT дослідження компанії зазвичай спираються на інструменти пошуку й виявлення цифрових маркерів у відкритій мережі та соціальних платформах: розширений пошук, роботу з вебархівами, пошук профілів за нікнеймами, відстеження публічних згадок тощо. Для українського контексту характерно, що соціальні мережі й месенджери стають ключовим полем первинного пошуку, оскільки значна частина ідентифікаційних маркерів існує у формі фото- та відеоматеріалів або публічних каналів комунікації. Навіть навчальні програми для розслідувачів акцентують саме на роботі із соціальними мережами та відкритими платформами. Аналітичний етап передбачає співставлення та структурування знайденої інформації. Тут застосовуються методики мультимедійної верифікації (перевірка зображень і відео, пошук першоджерела, аналіз ознак редагування). Також активно застосовується геопросторова перевірка для підтвердження місця події та аналітичне зіставлення часових меж подій. Цифрова особистість встановлюється через сукупність незалежних підтверджень, що зменшує ризик помилок та підвищує переконливість висновків. Завершальний етап дослідження включає верифікацію та зіставлення результатів. Зазвичай реалізується у форматі аналітичних довідок, звітів та візуалізацій зв’язків. Той факт, що відкрита розвідка розглядається як інструмент аналізу процесів у воєнний період у публічних дискусіях, додатково підтверджує його практичну актуальність.

Як вже було зазначено вище, ідентифікацію за допомогою OSINT-інструментів доцільно умовно поділити на три послідовні етапи. Перший етап охоплює ініціювання дослідження та збір даних. Ключовим завданням на цьому рівні є встановлення первинного ідентифікатора, яким може виступати обліковий запис, нікнейм, зображення, згадка, доменне ім’я або інший

цифровий слід. Надалі здійснюється виявлення та акумулювання пов'язаних із цим ідентифікатором даних, що містяться у відкритих джерелах.

Другий етап передбачає аналітичну обробку зібраної інформації. На цьому рівні відбувається верифікація даних, встановлення та підтвердження їх належності одній особі або об'єкту.

Третій етап полягає у верифікації та документуванні результатів. Він реалізується через додаткову перевірку встановлених зв'язків і сформованого профілю досліджуваної особи. ажливим є належне фіксування доказової бази таким чином, щоб забезпечити можливість її відтворення іншими дослідниками та отримання аналогічних висновків. Загалом такий підхід узгоджується з трактуванням OSINT у профільній науковій та навчальній літературі України, де відкриту розвідку розглядають як комплексний процес або цілісний методологічний підхід, що застосовується в дослідницькій та аналітичній діяльності [17].

Якщо аналізувати практику ідентифікації в Україні, то можна зробити висновок, що у нас добре розвинений перший етап дослідження. Це видно по тому як працюють приватні агенції та громадські організації. Вони швидко знаходять публічні профілі, відновлюють видалені сторінки через вебархіви, збирають публічні фото і відео. Це сильна сторона вітчизняного OSINTу, бо запит на ідентифікацію високий. Під час війни значну увагу приділяють саме ідентифікації воєнних злочинців та інших причетних осіб.

Другий етап характеризується дещо нижчою ефективністю порівняно з першим. Частина аналітичних команд здійснює дослідження системно, не покладаючись на поодинокі докази, здійснює верифікацію джерел, проводить їх порівняльний аналіз та формує виважені висновки. Водночас інші команди можуть надавати пріоритет швидкості проведення аналізу, що, у свою чергу, підвищує ризик виникнення помилкових інтерпретацій. Це важливо, бо в українському інформаційному середовищі багато фейків, які є результатом інформаційної війни. Тому важливо зосереджуватися на якості дослідження та ретельно перевіряти зібрані дані. Найбільша проблема виникає на третьому

етапі. Висновки досліджень можуть бути переконливими у приватному чи громадському секторі, але вони не зажди є такими на державному рівні. Відповідно це ускладнює їх використання у якості доказів у певних ситуаціях. Тут виникає відчутний розрив між державним та приватним використанням OSINT. Оскільки в Україні немає відповідного законодавства, яке б регулювало використання відкритих джерел у цифровій ідентифікації.

З наведеного випливає низка ключових висновків. По-перше, цифрова ідентифікація має два основні виміри – державний і приватний. OSINT виступає механізмом реконструкції цифрової особистості в ситуаціях, коли формальна ідентифікація ускладнена або недоступна. По-друге, рівень доказовості та методи дослідження можуть істотно відрізнятися, залежно від суб'єкта і мети розслідування. По-третє, розвиток OSINT-практики у приватному секторі підсилює актуальність питання правових меж. Адже відкрите джерело не завжди означає відсутність обмежень на роботу з даними.

Отже, аналіз сучасного стану цифрової ідентифікації в Україні свідчить, що нормативна база сформована достатньо комплексно щодо регулювання персональних даних та електронної ідентифікації, проте питання використання OSINT-інструментів у процесі встановлення цифрової особистості залишається неврегульованим, що зумовлює необхідність звернення до зарубіжного досвіду, де практика застосування OSINT у сфері цифрової ідентифікації має більш структурований характер.

2.2. Аналіз зарубіжного досвіду використання OSINT-інструментів у цифровій ідентифікації.

Для визначення можливих орієнтирів розвитку української практики варто звернутися до досвіду країн, де відкрита розвідка функціонує в умовах усталеного правового поля. Їх порівняльний аналіз дає змогу простежити, як схожі завдання вирішуються в різних правових системах і оцінити наскільки ці рішення можуть бути адаптовані до українського контексту.

Сполучені Штати Америки є однією з перших держав, у яких використання OSINT набуло системного характеру. На відміну від багатьох інших країн, у США відкрита розвідка розглядається як повноцінний елемент безпекової діяльності. У структурі американської розвідки функціонує Центр розвідки з відкритих джерел, який є частиною Офісу директора національної розвідки [57]. Його діяльність спрямована на системний збір, обробку та аналіз інформації з відкритих джерел. Закріплення у секторі розвідки означає визнання відкритих даних як джерела інформації. Тобто, у США розвідка з відкритих джерел має визначений статус і методологічну основу.

У сфері кримінального правосуддя OSINT активно використовується такими структурами, як Федеральне бюро розслідувань [67] та Міністерство національної безпеки [51]. У процесі цифрової ідентифікації використовуються: профілі в соціальних мережах, цифрові сліди, зв’язки між особами тощо. Особливістю американської моделі є те, що використання відкритих джерел не потребує судового дозволу, якщо інформація перебуває у публічному доступі. Водночас подальше використання отриманих даних у кримінальному процесі повинно відповідати вимогам допустимості доказів.

Американська правова система виробила підхід, згідно з яким інформація, добровільно оприлюднена особою у відкритому доступі, не має такого самого рівня захисту приватності, як закрита комунікація. У контексті цифрової ідентифікації OSINT використовується для встановлення реальної особи за псевдонімом, верифікації даних про особу та підтвердження або спростування алібі через відкриті цифрові сліди. Особливо активно ці методи застосовувалися під час розслідування штурму Капітолію, коли значна кількість осіб була ідентифікована через аналіз відкритих фото- та відеоматеріалів і соціальних мереж [47]. На відміну від України, де не має окремого нормативного визначення, у США ця практика інтегрована в систему національної безпеки та правоохоронної діяльності. Проте, що американська модель функціонує в умовах іншої правової культури та судової системи, що

передбачає активний судовий контроль. Тому пряме копіювання підходів без урахування національного контексту неможливим.

У межах Європейського Союзу використання OSINT-інструментів розвивається в умовах жорсткішого регуляторного середовища порівняно зі США. Визначальним нормативним актом у сфері обробки персональних даних є Загальний регламент про захист даних [48]. Регламент встановлює універсальні правила для будь-якої обробки персональних даних. Згідно з цим документом, факт відкритості персональних даних не скасовує необхідності правової підстави для їх обробки, адже персональні дані залишаються такими навіть при публічній доступності. Таким чином, у ЄС OSINT не розглядається як вільна зона, а підпадає під ті самі вимоги що й інші форми обробки даних.

Європейська правова традиція базується на принципі пропорційності, закріпленому у практиці Європейського суду з прав людини [46]. У контексті цифрової ідентифікації не допускається надмірна агрегація інформації. Збір і аналіз відкритих даних мають бути необхідними для конкретної законної мети. Наприклад, навіть якщо інформація розміщена в соціальній мережі у відкритому доступі, її систематичний моніторинг може потребувати окремого правового обґрунтування. Крім того, OSINT активно використовується європейськими правоохоронними та безпековими структурами, наприклад, Європейське поліцейське управління (Європол). У Європолі передбачені внутрішні механізми оцінки впливу на захист даних, що застосовується перед запуском нових аналітичних систем. Це свідчить про інституціоналізацію контролю за OSINT-аналізом.

Європейський підхід до відкриття даних базується на тому, що їх повторне використання допускається лише за умови дотримання вимог. Відповідні положення містяться у Директиві про відкриті дані, яка не скасовує вимоги «Загального регламенту про захист даних». Навіть якщо державний реєстр частково відкритий його систематичне копіювання, масове завантаження та побудова профілів можуть вважатися новою формою обробки. Тому така діяльність потребує правової підстави. У контексті цифрової ідентифікації це

суттєво обмежує можливість створення розширеного цифрового портрета особи виключно на основі відкритих джерел. Європейська модель характеризується жорстким регулюванням та високим рівнем нагляду за обробкою даних. Натомість в Україні відсутній детальний механізм контролю за агрегацією відкритих персональних даних. Питання допустимості OSINT як інструменту цифрової ідентифікації не має чітко визначених процедурних меж. Відсутність чіткої регуляції значно підвищує ризики зловживань.

Окрім державних структур, значний внесок у розвиток методології OSINT зробили незалежні аналітичні та журналістські ініціативи. Найвідомішим прикладом є Bellingcat – платформа, що спеціалізується на використанні відкритих джерел для розслідування міжнародних інцидентів, воєнних злочинів, випадків дезінформації та державних операцій [42]. Громадянська модель ідентифікації грунтується на принципі максимальної прозорості джерел та публічної верифікації отриманих результатів. Процес встановлення особи в межах такої моделі передбачає комплексний аналіз цифрових слідів, зокрема дослідження профілів у соціальних мережах, застосування зворотного пошуку зображень, геолокаційний аналіз фото- і відеоматеріалів, виявлення повторюваних цифрових маркерів, а також зіставлення часових і просторових характеристик публікацій. Висновок формується лише за наявності підтвердження з декількох незалежних джерел.

У практиці Bellingcat застосовуються різноманітні методичні підходи, спрямовані на перевірку достовірності та зіставлення даних. Організація має свій власний каталог інструментів (Рис. 2.3.). Одним із ключових елементів є геопросторова верифікація, що полягає у зіставленні особливостей ландшафту, архітектурних об’єктів, дорожньої інфраструктури чи погодних умов із супутниковими знімками та картографічними сервісами. Важливим процесом у ідентифікації цифрової особистості є аналіз цифрових зображень, який передбачає перевірку метаданих, пошук першоджерела публікації та виявлення можливого редагування. Соціальна кореляція дозволяє встановлювати зв’язки між профілями через мережу контактів, спільні фото або взаємодії, тоді як

часовий аналіз забезпечує зіставлення моменту публікації з конкретними подіями, метеоумовами чи особливостями освітлення. У результаті цифрова особистість реконструюється як цілісна сукупність поведінкових, просторових і комунікативних ознак.

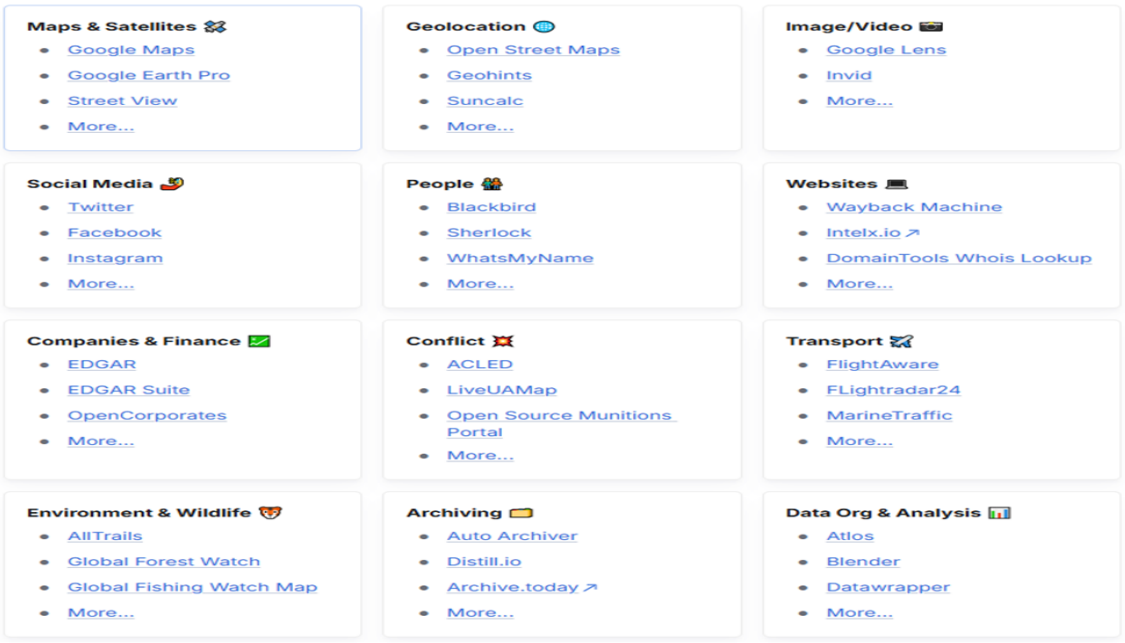

Рис. 2.3. Каталог OSINT-інструментів Bellingcat

Джерело: [41].

Практика Bellingcat показує, що цифрова особистість може бути встановлена без застосування державних засобів електронної ідентифікації. Це свідчить про те, що цифрова ідентичність формується не лише на основі офіційних документів, а існує як сукупність відкритих цифрових слідів, які за умови належної аналітичної кореляції дозволяють реконструювати особу. Таким чином, громадянська модель OSINT постає як альтернативна форма встановлення цифрової особистості, що функціонує поза межами державних структур, проте суттєво впливає на сучасні практики цифрової ідентифікації.

Порівняння різних моделей застосування OSINT дозволяє виявити три різні підходи до встановлення цифрової особистості, що відрізняються ступенем інституціоналізації, рівнем правового контролю та процесуальним статусом отриманих результатів. У США OSINT є офіційним елементом державної безпекової та правоохоронної діяльності. Його застосування

інтегроване у діяльність розвідувальних структур, зокрема у контексті кібербезпеки та кримінальних розслідувань. Встановлення цифрової особистості в американській моделі відбувається як аналітичний етап, що передує процесуальним діям. Хоча інформація отримується з відкритих джерел, її використання підпорядковується вимогам і судовому контролю. Таким чином, OSINT у США функціонує як складова державної доказової системи.

Європейський союз демонструє більші обмеження. Тут OSINT-інструменти застосовуються правоохоронними органами, однак перебувають під жорстким впливом норм захисту персональних даних, насамперед положень Загального регламенту про захист даних (GDPR). Навіть якщо дані є публічними, їх систематична агрегація та профілювання розглядається як обробка персональної інформації, що потребує правової підстави та дотримання принципів пропорційності й мінімізації. У європейській моделі ключовим є баланс між ефективністю ідентифікації та захистом приватності. Отже, OSINT у ЄС розглядається не стільки як інструмент розширення аналітичних можливостей, скільки як діяльність, що потребує чітких правових меж.

На відміну від обох державних моделей, діяльність Bellingcat представляє громадянський підхід до OSINT-ідентифікації. У цьому випадку встановлення цифрової особистості здійснюється виключно через відкриті джерела, без доступу до закритих реєстрів і без примусових повноважень. Методологія ґрунтується на багаторівневій кореляції даних, геопросторовій верифікації, аналізі цифрових зображень та соціальних зв’язків. Однак результати такої ідентифікації мають аналітичний характер і не набувають автоматично юридичного статусу доказу. Легітимність громадянської моделі визначається не процесуальними нормами, а публічною прозорістю та переконливістю методики.

Таким чином, американська модель характеризується високим рівнем інституціоналізації та інтеграцією OSINT у систему доказування. Європейська модель вирізняється посиленим нормативним контролем та пріоритетом

захисту персональних даних. Громадянська модель – методологічною гнучкістю та опорою на відкритість джерел. Відмінності між ними полягають не в інструментах, а у правовому режимі їх застосування та статусі отриманих результатів.

Для України це порівняння є показовим, оскільки національна практика поки що не повністю сформованої інституціональної моделі OSINT-ідентифікації. В умовах цифровізації та воєнного стану зростає потреба у чіткій регламентації меж використання відкритих даних, одночасно зберігаючи ефективність аналітичних механізмів встановлення особи.

Правове регулювання використання OSINT-інструментів безпосередньо пов’язане з нормами про доступ до інформації, захист персональних даних, кримінальний процес та національну безпеку. Водночас у більшості країн світу OSINT як термін не закріплений окремим законом, а його застосовування регулюється опосередковано через загальні правовові механізми.

В Україні спеціального нормативного акту, який би визначав правовий статус OSINT або встановлював процедури використання відкритих джерел для цифрової ідентифікації, не існує. Використання відкритої інформації регулюється насамперед Законом України «Про інформацію», Законом України «Про доступ до публічної інформації», Законом України «Про захист персональних даних», а також нормами Кримінального процесуального кодексу щодо допустимості доказів. Таким чином, OSINT в українській правовій системі функціонує як практичний інструмент, що не має самостійного нормативного визначення, але не суперечить законодавству за умови дотримання вимог щодо обробки персональних даних і процесуального порядку збирання доказів. Водночас відсутність чітких методичних стандартів створює неоднорідність практики та ризики правової невизначеності.

У Сполучених Штатах OSINT інтегрований у діяльність розвідувальних і правоохоронних органів у межах ширшої системи регулювання національної безпеки. Його застосування ґрунтується на нормах про розвідувальну діяльність, кримінальне судочинство та конституційні гарантії, зокрема

«Четверту поправку» щодо захисту від необгрунтованих обшуків. Відкриті джерела не вимагають судового дозволу для аналізу, однак їх використання як доказів у суді підпорядковується стандартам допустимості. Американська модель характеризується високим рівнем інституціоналізації OSINT та чітким розмежуванням між відкритим збором інформації і втручанням у приватне життя.

У країнах Європейського Союзу правове регулювання OSINT перебуває під суттєвим впливом режиму захисту персональних даних, насамперед положень Загального регламенту про захист даних (GDPR). Європейський підхід виходить із того, що навіть публічно доступні персональні дані залишаються об'єктом правового захисту. Систематичний моніторинг, агрегація або профілювання відкритої інформації розглядаються як обробка персональних даних і потребують законної підстави, дотримання принципів мінімізації та пропорційності. Це означає, що в ЄС OSINT як аналітична діяльність підлягає суворому нормативному контролю. Такий підхід забезпечує вищий рівень захисту приватності, однак одночасно обмежує масштаб і автоматизацію аналітичних процесів.

Отже, можна констатувати, що зарубіжні моделі демонструють два основні підходи: застосування OSINT у межах системи національної безпеки та його жорстке регулювання з акцентом на захист персональних даних. Водночас українська модель перебуває на етапі формування та потребує чіткого нормативного визначення меж використання відкритих даних для цифрової ідентифікації. Це питання є особливо актуальним в умовах цифровізації державних процесів і запровадження правового режиму воєнного стану.

Висновки до другого розділу

У другому розділі було проаналізовано нормативно-правові засади цифрової ідентифікації в Україні, практичне застосування OSINT-інструментів. Також, розглянуто зарубіжний досвід використання відкритих джерел в ідентифікації цифрової особистості. Порівняльний аналіз показав, що в Україні

цифрова ідентифікація нормативно розвинена, але відкрита розвідка не має чіткого регулювання. На практиці використання відкритих джерел існує, проте реалізується переважно громадським та приватним сектором. Такі дослідження стосуються здебільшого воєнної тематики. Сюди входять розслідування воєнних злочинів, ідентифікація причетних осіб, визначення місця подій тощо.

Зарубіжний досвід демонструє більш структурований підхід. У США та ЄС OSINT закріплений на законодавчому рівні та активно використовується державними організаціями, особливо правоохоронними органами та розвідувальними підрозділами. Громадську діяльність в сфері відкритої розвідки представляє Bellingcat. Організація активно використовує інструменти OSINT та демонструє розроблення власних алгоритмів дослідження.

Отже, ключова відмінність між Україною та іншими країнами полягає у відсутності стандартизації та правового регулювання використання інструментів OSINT. Для України актуальним завданням залишається створення відповідних нормативних актів, які будуть регулювати процеси відкритої розвідки та діяльність профільних організацій.

РОЗДІЛ 3

ПРАКТИЧНІ АСПЕКТИ ЕФЕКТИВНОСТІ ІНСТРУМЕНТІВ ВІДКРИТОЇ РОЗВІДКИ ДЛЯ ІДЕНТИФІКАЦІЇ ЦИФРОВОЇ ОСОБИСТОСТІ В УКРАЇНІ

У третьому розділі проаналізовано діяльність українських OSINT-організацій шляхом ознайомлення з деякими кейсами з їхньої діяльності. На основі розглянутого матеріалу сформовано модель оцінювання ефективності OSINT-інструментів за п'ятьма основними критеріями. Також описано ризики, які виникають у процесі використання таких інструментів та надано практичні рекомендації щодо подальшого використання OSINT в Україні.

3.1. Дослідження ефективності OSINT-інструментів у процесі цифрової ідентифікації (на прикладі кейсів)

З метою визначення результативності та доцільності застосування інструментів відкритої розвідки у процесі цифрової ідентифікації необхідно розглянути діяльність українських організацій, які спеціалізуються на OSINT-розслідуваннях. Аналіз конкретних кейсів дає змогу простежити механізми використання таких інструментів у процесі встановлення особи. Для цього застосовано метод кейс-аналізу, порівняльний метод, а також елементи контент-аналізу відкритих джерел.

У контексті дослідження ефективності OSINT-інструментів для ідентифікації цифрової варто звернути увагу на український проект «Миротворець». Цей сайт був запущений у грудні 2014 року і позиціонує себе як база даних про осіб, «дії яких мають ознаки злочинів проти національної безпеки України, миру, безпеки людства та міжнародного правопорядку. Хоча проект не має офіційного державного статусу, він тісно пов'язаний із силовими структурами, зокрема Службою безпеки України [57].

З точки зору OSINT, методологія «Миротворця» є яскравим прикладом поєднання пасивного збору даних та активної роботи з конфіденційними

джерелами. Персонал проекту діє анонімно, а аналітична група обробляє інформацію, отриману двома основними каналами. Перший канал – це моніторинг відкритих джерел (соціальних мереж, форумів, публічних реєстрів медіа тощо). Другий – конфіденційна інформація, надана фізичними особами на анонімній основі, а також, ймовірно, матеріали зі зламаних баз даних. Одним з найвідоміших випадків використання такої інформації є публікація персональних даних журналістів, акредитованих при так званій «ДНР» у 2016 році [57; 63]. Така гібридна модель суттєво підвищує ефективність ідентифікації, оскільки верифікувати цифровий слід особи через альтернативні канали.

Хоча точний перелік програмного забезпечення, яке використовує команда «Миротворця», не розголошується, загальна логіка діяльності проекту дозволяє реконструювати ймовірний арсенал засобів. Передусім це інструменти моніторингу соціальних мереж, за допомогою яких аналізуються відкриті профілі у ВКонтакті, Однокласниках, Facebook, Telegram для збору біографічних даних, геолокацій, фотографій, соціальних зв'язків. Також, використовуються бази даних з витоками для отримання верифікованих персональних даних, які потім зіставляються з інформацією, знайденою у відкритих джерелах.

Зібрана інформація дає змогу зробити кілька важливих висновків про те, наскільки ефективним OSINT виявився у роботі «Миротворця». Передусім проект показує, що самих відкритих даних часто замало, щоб ідентифікувати людину повністю. Тому у деяких випадках можна комбінувати їх з інформацією, отриманою через прямі контакти з людьми. Проте висока ідентифікаційна спроможність проекту може мати негативні наслідки. Публікація персональних даних осіб несе потенційну загрозу їхньому життю чи безпеці. У таких випадках гостро постає етичне питання, а саме визначення межі дозволеного. «Миротворець» неодноразово був об'єктом гучних скандалів та навіть кримінальних проваджень. Його діяльність була неодноразово розкритикована міжнародними організаціями та медіа. Загалом проект

демонструє величезний потенціал OSINT-методів у встановленні цифрової особистості в умовах війни. Але водночас показує, що відбувається коли проект досягає критичної маси впливу.

Іншим важливим прикладом використання OSINT для ідентифікації цифрової особистості в українському контексті є волонтерський проект InformNapalm. Вони позиціонують себе як міжнародну OSINT-спільноту, що проводить розслідування та публікує не лише результати, а й повну методологію їх отримання [53]. Такий підхід дозволяє будь-кому перевірити висновки самостійно, що відповідає фундаментальному принципу відкритості. Автори проекту публікують матеріали 30 мовами, що свідчить про орієнтацію на міжнародну аудиторію.

Методологія InformNapalm є класичним прикладом комплексного OSINT-аналізу, що поєднує кілька напрямів роботи з відкритими даними. Основним видом діяльності проекту є збирання та аналіз інформації з відкритих джерел, включно з соціальними мережами. Ключову роль відіграє геопросторовий аналіз, тобто визначення точних координат місця події за допомогою супутникових знімків, відеоматеріалів, фотографій тощо. Розслідування InformNapalm щодо командира 53-ї артилерійської бригади полковника Сергія Мучкаєва, підозрюваного у причетності до збиття малайзійського Boeing-777, було використане в звіті дослідницької команди Bellingcat [38; 45]. Це свідчить про високий рівень довіри до аналітичних матеріалів проекту з боку міжнародних OSINT-спільнот.

Після початку російського вторгнення в Сирію InformNapalm розпочав публікацію персональних даних російських пілотів, які бомбардували сирійські міста, включно з іменами, прізвищами, фотографіями, бортовими номерами літаків [32]. Ці публікації викликали різко негативну реакцію в Росії. У відповідь автори сайту заявили, що кожне порушення режиму припинення вогню на Донбасі спричинить публікацію чергового OSINT-розслідування з іменами, фотографіями, тактичними і реєстраційними номерами та іншими

деталями, пов’язаними зі злочинами російських льотчиків під час військової операції в Сирії.

Ефективність InformNapalm як OSINT-інструменту підтверджується не лише міжнародним резонансом, а й кількісними показниками. До кінця 2016 року спільнота мала 407 розслідувальних публікацій, 1197 перекладів та понад 3920 репостів у медіа. У квітні 2018 року InformNapalm опублікував інтерактивну базу даних російської агресії, яка складається з понад 1700 розслідувань [14]. База даних розділена на дві групи: російське озброєння знайдене на Донбасі та російські підрозділи, які брали участь в агресії проти України, Грузії, Сирії. Вона є пошуковою за номером військової частини. Зображення шевронів або військової техніки клікабельні і ведуть до списку відповідних розслідувань. Усе це утворює джерело інформації для дослідників, журналістів чи правоохоронців.

Ще один приклад – аналітичне агентство Molfar. До повномасштабного вторгнення команда зосереджувалася переважно на корпоративних розслідуваннях, але після 2022 року додала до своєї роботи і військовий напрям [56]. На відміну від попередніх організацій, Molfar працює за гібридною моделлю. Паралельно з відкритими розслідуваннями воєнних злочинів і публікацією результатів практикується надання послуг державним структурам. Особливістю команди є активне застосування відкритої розвідки для ідентифікації конкретного військовослужбовця і встановлення його точного місцезнаходження. Далі ці дані передаються українській розвідці. Показовим тут є випадок, коли в жовтні 2022 року один російський військовий опублікував своє фото у формі з відкритою геолокацією [9]. Аналітики швидко встановили особу і точне місце дислокації підрозділу. Невдовзі після цього по тих координатах було завдано удару.

Одним із напрямів роботи агентства є викриття елітних російських спецпідрозділів, дані про які офіційно є таємними. Прикладом слугує розслідування щодо п’ятьох бійців секретного центру «Сенеж», які загинули на Чернігівщині [2]. Аналітикам вдалося не лише встановити їхні справжні імена,

позивні, військові звання, але й зібрати докази їхньої причетності до вбивства цивільної людини. Цей випадок показує, що навіть найбільш закриті структури залишають цифрові сліди, які за умови системної роботи можна знайти і перевірити. Крім того, Molfar займається дослідженнями, що виходять за межі ідентифікації конкретних осіб. Аналітики виявили закономірність між придбанням супутникових знімків американських компаній та подільшими ракетними ударами по Україні [3; 4]. З'ясувалося, що знімки купувалися через підставних посередників за кілька днів до атак, що дозволило відстежити ланцюги постачання даних для планування воєнних злочинів і поставити питання про відповідальність посередників. Також, дослідники Molfar регулярно діляться своїм досвідом на міжнародному рівні, презентують свої методики та напрацювання.

Таблиця 3.1

Основні OSINT-інструменти, виявлені в досліджених кейсах

Напрями	Короткий опис	Де використовується
Моніторинг соціальних мереж (SOCMINT)	Пошук та аналіз відкртих профілів, фото, геотегів, друзів, коментарів	Усі три проєкти
Геопросторовий аналіз (GEOINT)	Визначення координат за супутниковими знімками, фото, картами	InformNapalm, Molfar
Аналіз витоків даних	Використання зламаних баз для отримання паспортів, телефонів, адрес	«Миротворець», InformNapalm
Аналіз метаданих файлів	Вилучення EXIF-даних з фото (дата, GPS, пристрій)	InformNapalm, Molfar
Геолокація мобільних пристроїв	Відстеження через сервіси Apple Find My, Google Find My Device	Molfar
Соціальна інженерія	Створення фейкових акантів, комунікація з цільовою аудиторією	ImformNapalm

Джерело: складено автором.

Аналіз діяльності «Миротворця», InformNapalm та Molfar дозволяє виокремити набір інструментів та технік, які забезпечують успішну

ідентифікацію цифрової особистості (Додаток Б). Ці інструменти використовуються різними організаціями з різними цілями. Це свідчить про їхню універсальність та практичну ефективність. Загалом, вдалося виокремити шість основних типів інструментів, які зустрічаються в розглянутих кейсах (Табл. 3.1).

Моніторинг соціальних мереж є базовим інструментом для всіх трьох проектів. «Миротворець» використовує його для збору публічної інформації про осіб, які співпрацюють з окупаційними адміністраціями. Сюди входять фотографії, геолокації, списки друзів тощо. InformNapalm за допомогою такого моніторингу відстежував публікації російських військовослужбовців, які навіть через закриті акаунти іноді залишають відкриті коментарі або фото на фоні впізнаваних об'єктів. Molfar в одному з кейсів виявив публікацію з геолокацією, що дозволило пізніше ідентифікувати інших військових з того ж підрозділу. Моніторинг соціальних мереж є універсальним, адже він однаково ефективний для масового збору даних і точкових розслідувань.

Геопросторовий аналіз став ключовим інструментом для верифікації місць подій. InformNapalm неодноразово використовував це для спростування російської пропаганди. Вони робили це шляхом зіставлення відео обстрілів з супутниковими знімками. Molfar застосовував такі інструменти для підтвердження перебування російських військових у різних місцях. Для цього зіставляли їхні фотографії із супутниковими знімками населених пунктів. Хоча «Миротворець» рідше публікує такі розслідування, сайти-агрегатори, які пов'язані з проектом, використовують геолокацію для нанесення даних на інтерактивні мапи. Ефективність геопросторового аналізу полягає в тому, що він не залежить від налаштувань приватності цільової особи. Для цього часто достатньо одного фото на фоні якоїсь впізнаваної будівлі чи об'єкту.

Аналіз витоків даних забезпечує найглибший рівень ідентифікації. «Миротворець» у 2016 році опублікував базу даних журналістів, акредитованих при ДНР, отриману зі зламаного сервера міністерства безпеки терористів. Це дозволило отримати паспортні дані, телефони та адреси тисяч осіб.

InformNapalm у рамках одного з масштабних витоків інформації отримав листування помічника президента РФ. Це дозволило ідентифікувати конкретних осіб, причетних до планування дестабілізації України. Molfar також використовував витік бази даних російської військової частини. Спільним для усіх цих випадків є те, що аналіз витоків дає дані, які неможливо отримати іншим відкритим способом. Це робить цей інструмент критично важливим для глибокої ідентифікації.

Аналіз метаданих файлів є доволі простим з технічної точки зору. Для його використання достатньо онлайн-сервісів. Попри простоту його ефективність підтверджується великою кількістю успішних кейсів. InformNapalm використовував аналіз метаданих для перевірки відео, наданих російською стороною. Внаслідок такої перевірки було виявлено, що дата створення файлу не відповідає даті заявленої події. Тобто відбулася фальсифікація інформації. Схожим чином працювали аналітики Molfar. Вони аналізували метадані фото, які публікували російські військові, щоб отримати GPS-координати навіть коли користувач сам не ставив геолокацію. Обмеженням інструменту є те, що більшість соціальних мереж автоматично видаляють метадані при завантаженні. Водночас, коли фотографії публікуються на форумах або в месенджерах, ці дані часто зберігаються.

Геолокація мобільних пристроїв є одним з найбільш специфічних інструментів. У розглянутих кейсах він з’являється лише в діяльності Molfar [52]. Використання спеціалізованих сервісів з пошуку пристроїв дало змогу простежити переміщення викраденого пристрою та встановити точну адресу, за якою перебував злочинець Цей інструмент демонструє, що відкрита розвідка виходить за межі лише добровільно опублікованих даних і використовує технічні можливості, які людина не завжди може повністю контролювати. Складністю застосування такого методу полягає в необхідності доступу до потрібного облікового запису або наявності фізичного пристрою, що робить інструмент менш доступним порівняно з іншими.

Соціальна інженерія виходить за межі класичного OSINT, але є не менш ефективним, оскільки технічних інструментів іноді недостатньо. Використання його в одному з проектів InformNapalm. Створивши фейковий акаунт російського військового, аналітики спілкувалися з дружинами військовослужбовців. Це надало їм доступ до облич, прізвищ та місць служб осіб, які навмисно приховували себе в мережі. Соціальна інженерія є повільним та дуже ризиковим методом, але вона дає можливість отримати унікальну інформацію, яку не можна видобути іншими шляхами.

Таким чином, аналіз трьох українських організацій, що спеціалізуються на розслідуваннях із відкритих джерел, дав змогу виділити основні дослідницькі методи. Якщо заглибитися в окремі кейси, стають помітними конкретні інструменти. У сукупності вони формують базовий набір, яким так чи інакше послуговується OSINT-дослідник в Україні. Різні команди вибудовують власні комбінації цих інструментів залежно від ситуації та отримують відповідні результати. Це, своєю чергою, підтверджує їхню універсальність і ефективність.

3.2. Оцінювання ефективності та ризиків застосування OSINT-інструментів у сфері цифрової ідентифікації: пропозиції щодо вдосконалення політики безпеки та цифрового суверенітету України

Для забезпечення системного підходу до оцінювання інструментів відкритої розвідки необхідно мати чіткі критерії, які враховують специфіку різних дослідницьких завдань. Не менш важливо окреслити можливі ризики використання цих інструментів.

Аналізуючи кейси «Миротворця», InformNapalm та Molfar, можна виокремити п’ять критеріїв оцінки ефективності інструментів (Табл. 3.2), які використовуються в дослідженні. Критерії сформовані на основі практичних питань які виникають перед аналітиками. Для кожного критерію запропоновано п’ятибальну шкалу, де 1 – найнижчий показник, а 5 – найвищий. Оскільки різні

завдання мають різні пріоритети, дослідник сам визначає, які критерії є для нього найбільш важливими залежно від мети його дослідження.

Таблиця 3.2.

Критерії оцінювання ефективності OSINT-інструментів

Критерій	**Визначення**	**Шкала оцінювання (1 –найнижчий, 5 – найвищий)**
Швидкість	Час від моменту отримання вихідних даних до отримання потрібної інформації	1 – тижні, місяці; 2 – дні; 3 – години; 4 – хвилини; 5 – секунди (автоматизовано)
Достовірність	Ймовірність правильного визначення з невеликою похибкою	1 – дуже низька (часті помилки); 2 – низька; 3 – середня (потребує верифікації); 4 – висока; 5 – абсолютна (унікальний ідентифікатор)
Глибина ідентифікації	Обсяг персональних даних, які можна отримати за допомогою OSINT-інструменту	1 – лише псевдонім, нікнейм; 2 – загальна геолокація; 3 – фото, ПІБ; 4 – адреса, місце роботи; 5 – паспортні дані, родинні зв’язки, переміщення
Доступність	Можливість використання OSINT-інструменту пересічним дослідником без спеціальних дозволів чи значних витрат	1 – потребує спецдозволу або зламу; 2 – платний або важкодоступний; 3 – частково доступний; 4 – безкоштовний, але потребує навичок; 5 – цілком безкоштовний і публічний
Можливість обходу	Здатність цільової особи уникнути ідентифікації шляхом зміни своєї поведінки або налаштувань	1 – дуже легко обійти; 2 – легко; 3 – середньо; 4 – важко; 5 – майже неможливо (дані не залежать від волі особи)

Джерело: складено автором.

Перший критерій – швидкість, тобто час необхідний для отримання результату. У всіх розглянутих кейсах швидкість відігравала важливу роль. У випадку Molfar інформацію потрібно було отримати і передати за лічені години, адже застарілі дані втрачали сенс. InformNapalm могли працювати

довше, оскільки це були повноцінні розслідування з розгорнутими опублікованими результатами. Тобто в цьому випадку якість переважала над швидкістю роботи. «Миротворець» функціонує як архів, тому темп додавання нових записів невисокий, але це й не має великого значення. Для них головне – це наявність повної та достовірної інформацію про осіб. Швидкість важлива, але її значущість залежить від мети дослідження. Щоб оцінити інструмент за цим критерієм потрібно визначити скільки часу в середньому триває його застосування від моменту отримання вихідних даних до видачі потрібної інформації. Загалом, OSINT-інструменти, які працюють автоматично отримують вищу оцінку, ніж ті, що потребують ручного аналізу.

Другий критерій – достовірність. Помилки трапляються в будь-яких розслідуваннях, тому для дослідника важливо звести це до мінімуму. Найгучніші скандали тут пов’язані з «Миротворцем». Траплялося, що на основі неперевірених даних від анонімних джерел у базі опинялися люди, які не мали жодного стосунку до того, що їм приписували. InformNapalm демонструє значно вищий рівень достовірності, завдяки тому, що перевіряє інформацію через кілька незалежних джерел. Крім того, Molfar також практикує підтвердження даних через комбінування різних методів. Критерій достовірності оцінює ймовірність похибки інструменту. Інструменти з високою достовірністю дають однозначну відповідь при наявності достатніх вихідних даних. Інструменти з низькою достовірністю потребують додаткової перевірки.

Третій критерій – глибина ідентифікації. У кейсі з крадіжкою AirPods Molfar зміг встановити особу, її переміщення та домашню адресу. Аналізи витоків у «Миротворці» давав паспортні дані та номери телефонів. Цей критерій визначає наскільки далеко може зайти дослідник з допомогою конкретного інструменту. Тобто чи вдасться знайти якісь розширені дані. Глибина є важливою, якщо метою є не просто знайти особу, а повноцінно ідентифікувати її (наприклад для правоохоронних органів).

Четвертий критерій – доступність. Моніторинг соціальних мереж доступний кожному, для цього достатньо мати акаунт. Геопросторовий аналіз

теж цілком доступний завдяки безкоштовним супутниковим знімкам. Аналіз витоків вимагає купівлі баз на чорному ринку або участі в певних групах, що робить його малодоступним для пересічного дослідника. Геолокація пристроїв практично недоступна без спеціальних дозволів або облікового запису жертви. Соціальна інженерія потребує часу, навичок комунікації і створення фейкових акаунтів, що також створює перешкод. У цьому дослідження доступність оцінюється за шкалою від цілком публічних і безкоштовних до тих, що потребують спеціальних прав або участі у нелегальних діях.

П’ятий критерій – можливість обходу. Тобто наскільки легко цільова особа може уникнути ідентифікації. Деякі інструменти легко обходяться, наприклад, закриттям профілю у соціальній мережі, вимкненням геолокації на телефоні чи видаленням метаданих з фото перед публікацією. Проте інші інструменти обійти складніше, якщо особу вже внесено до зламаної бази даних, то видалити свої дані звідти неможливо. Якщо використовується супутниковий знімок, особа ніяк не зможе на нього вплинути. Критерій можливості обходу оцінює наскільки інструмент стійкий до свідомого приховування слідів з боку цільової особи.

Використання інструментів відкритої розвідки завжди має ризики, навіть якщо ці інструменти є технічно ефективними. Уникнути їх повністю майже неможливо, проте кожен дослідник повинен намагатися зменшити їхній вплив на кінцевий результат. Проведений аналіз кейсів українських OSINT-проектів допомагає виокремити кілька типів ризиків, які виникають під час ідентифікації цифрової особистості. Юридичні ризики виникають через невизначеність меж дозволеного. Етичні ризики полягають у тому, що навіть технічно доступна інформація не завжди має бути оприлюдненою, адже це може зашкодити невинним особам. Технічні ризики стосуються самих даних. Вони можуть неповними, застарілими, сфальсифікованими тощо. Після поширення результатів дослідження з’являються ризики для репутації дослідника чи організації у разі публікації неправдивої інформації. Також можуть виникати ризики для цільової особи. Публікація її персональних даних може становити

загрозу для її безпеки чи життя. Тому перед застосуванням будь якого інструменту варто зважити очікувану користь і потенційну шкоду.

Проведений аналіз дає змогу сформулювати кілька практичних рекомендацій. Усі вони, по суті, спрямовані на дві речі: підвищити якість і безпеку застосування відкритої розвідки в Україні та створити умови, за яких інструменти цифрової ідентифікації особи використовуватимуть відповідально. Ключовим напрямом буде формування спеціалізованого законодавства у сфері OSINT. Відсутність правового регулювання є проблемою для самих аналітиків і правоохоронних органів. Доцільно було б розробити базовий закон, який би чітко окреслив визначення OSINT, перелік дозволених інструментів, порядок фіксації та подання отриманих даних як доказів у суді, а також межі відповідальності за оприлюднення неперевірених персональних даних. Цей закон повинен встановлювати базові вимоги до відкритої розвідки, але при цьому не блокував громадські ініціативи.

Ще одним важливим кроком може стати створення експертної ради з етики OSINT. Логічно було б заснувати її при Міністерстві цифрової трансформації. Річ у тім, що жоден закон не в змозі передбачити всіх нюансів з якими стикається дослідник в сфері відкритих даних. Тому виникає потреба у постійно діючому дорадчому органі, який розглядатиме спірні ситуації. До його складу варто включити практикуючих OSINT-дослідників, правозахисників, юристів. Це дасть змогу врегульовувати етичні суперечки оперативно, в робочому порядку.

Також не варто забувати про стимулювання міжнародної співпраці. Українські OSINT-команди вже мають певний авторитет закордоном, тож цим треба користуватися. Для того, щоб підвищити і закріпити авторитет українських експертів потрібно посилювати взаємодію з закордонними партнерами, проводити спільні розслідування, укладати двосторонні угоди про обмін даними тощо. Окремо слід звернути увагу на залучення іноземних фахівців до навчання українських аналітиків. З одного боку, це підвищить якість підготовки, а з іншого – зміцнить позиції України на міжнародній арені й

допоможе стати одним із лідерів у східноєвропейському регіоні у питаннях розвідки з відкритих джерел.

Отже, проведений аналіз дозволяє стверджувати, що ефективність інструментів відкритої розвідки залежить від конкретних завдань дослідження та пріоритетності відповідних критеріїв. Жоден з розглянутих інструментів не є універсальним, тому дослідник має свідомо обирати, ті з них, що найкраще відповідають його меті. Також не варто забувати про ризики, що супроводжують діяльність у сфері відкритої розвідки. Їх неможливо уникнути повністю, однак можна мінімізувати через відповідальне ставлення до збору, перевірки та публікації даних. На основі виявлених проблем запропоновано практичні пропозиції для підвищення якості відкритої розвідки в Україні та зміцненню довіри до вітчизняних організацій.

Висновки до третього розділу

Аналіз діяльності трьох українських організацій («Миротворця», InformNapalm, Molfar) показав, що попри спільне поле роботи кожна з них вибудовує власну систему інструментів відповідно до своїх цілей. Саме мета дослідження визначає, які критерії оцінювання є важливішими. Водночас розгляд конкретних кейсів засвідчив, що максимальна результативність досягається комбінуванням інструментів. Зіставлення інструментів за запропонованими критеріями дало змогу побачити не лише сильні сторони кожного підходу, а й вразливості, які зазвичай залишаються поза увагою. Цей набір критеріїв виявився найбільш універсальним для українських реалій. Окрему увагу приділено ризикам та важливості мінімізації їхнього впливу на хід дослідження.

Ключовий практичний висновок полягає в тому, що без чітко окресленого правового поля відкрита розвідка в Україні й надалі розвиватиметься стихійно. Спеціалізоване законодавство мало б встановити межі відповідальності. Без таких системних кроків подальше застосування OSINT не зможе набути сталості та передбачуваності.

ВИСНОВКИ

У результаті проведення дослідження, присвяченого використанню інструментів відкритої розвідки у процесах ідентифікації цифрової особистості в Україні, вдалося виконати всі поставлені завдання та отримати низку теоретичних та практичних результатів.

Для визначення сутності основних понять дослідження було опрацьовано наукові та прикладні джерела, у яких розкрито зміст понять «OSINT», «цифрова особистість», «цифрова ідентифікація», «цифровий слід», «цифрова тінь». Порівняльний аналізрізних наукових підходів дав змогуо не лише виявити їхні спільні та відмінні риси, а й сформулювати робочі визначення, що враховують специфіку застосування методів відкритої розвідки до завдань ідентифікації особи. Зокрема, визначення поняття OSINT у роботі розуміється як сукупність методів збору, аналізу та інтерпретації загальнодоступної цифрової інформації, спрямованих на встановлення особи. Цифрову особистість розглянуто як сукупність даних, онлайн-профілів та віртуальних проявів, що відображають присутність людини в цифровому середовищі. Під цифровим слідом розуміється сукупність відкритих даних, сформованих у процесі взаємодії користувача з цифровим середовищем, а цифрова тінь трактується як інформація, що формується без його безпосередньої участі та не підлягає прямому контролю. Сформований поняттєво-категорійний апарат зафіксовано в узагальнюючій таблиці, що стала основою для всього подальшого аналізу.

Унаслідок систематизації та класифікації інструментів OSINT здійснено їх поділ за типом джерел інформації, за функціональним призначенням та за етапами дослідження. Така класифікація дозволила впорядкувати різноманітний інструментарій і забезпечила теоретичне підґрунтя для подальшого оцінювання ефективності конкретних засобів у контексті ідентифікації цифрової особистості.

У результаті опрацювання нормативної бази вдалося встановити, що правове регулювання цифрової ідентифікації спирається на кілька рівнів.

Конституційний рівень гарантує недоторканність приватного життя й окреслює допустимі межі втручання в особисті дані. Загальні інформаційні акти, передусім Закон України «Про інформацію», визначають правовий режим даних і загальну логіку доступу до них. Спеціальне законодавство про персональні дані та електронну ідентифікацію встановлює правила обробки інформації й надає юридичну силу цифровим процедурам підтвердження особи. Ще один рівень утворюють акти, що регулюють функціонування державних реєстрів і формують інфраструктурне підґрунтя для цифрової ідентифікації.

Отримані результати вказують на те, що при активному практичному використанні OSINT в Україні його правовий статус залишається невизначеним. У законодавстві відсутнє як саме поняття, так і правила його застосування для цілей ідентифікації особи. Відсутність правової визначеності породжує наслідки для всіх суб'єктів дотичних до такої діяльності. Для дослідників така ситуація означає, що аналітична робота спрямована на встановлення суспільно важливих фактів, може за відсутності чітких правових меж трактуватися як порушення законодавства про персональні дані чи втручання у приватне життя. Для правоохоронних органів брак нормативного регулювання ускладнює вирішення питання про допустимість даних з відкритих джерел як доказів у кримінальних справах. Загальним наслідком такої ситуації стає підвищений ризик безконтрольного поширення персональних даних, що не підкріплене ані належною верифікацією, ані дієвими механізмами захисту осіб, яких ця інформація стосується.

Аналіз зарубіжного досвіду засвідчив, що у світовій практиці сформувалися різні підходи до використання OSINT для встановлення особи. . У Сполучених Штатах Америки відкрита розвідка вже тривалий час інтегрована в систему державної безпеки . Її застосовують як розвідувальні служби, так і правоохоронні органи, причому для збору публічно доступних даних отримання судового дозволу не є обов'язковим . У країнах Європейського Союзу Загальний регламент захисту даних (GDPR) встановлює суттєві обмеження щодо роботи з відкритими даними. Зокрема, не

допускається безконтрольне збирання всієї доступної інформації про особу з відкритих джерел із подальшим формуванням детального профілю . Крім того, обсяг зібраних даних має відповідати принципу мінімізації та бути обмеженим лише тією інформацією, яка є необхідною для досягнення визначеної мети. У зв'язку з цим дослідник повинен постійно дотримуватися балансу між ефективністю розслідування та забезпеченням права людини на приватність .

Аналіз діяльності «Миротворця», InformNapalm, Molfar дозволив побачити реальний арсенал засобів, якими вітчизняні дослідники послуговуються для ідентифікації особи. У результаті вдалося виокремити шість напрямів, що виявилися універсальними для української практики: моніторинг соціальних мереж, геопросторовий аналіз, аналіз витоків даних, аналіз метаданих, геолокацію мобільних пристроїв та соціальну інженерію. Розгляд конкретних кейсів засвідчив, що максимальна результативність досягається не окремим напрямом, а їх комбінуванням. Жоден засіб не є універсальним і його ефективність завжди визначається конкретним завданням. На цій основі було запропоновано спосіб порівняння інструментів. Для цього виокремлено п'ять критеріїв: швидкість отримання результату, достовірність, глибина ідентифікації, доступність для дослідника та можливість обходу з боку цільової особи. Кожен із них оцінюється за простою шкалою, що дає змогу співвіднести переваги й обмеження альтернативних засобів і свідомо обрати найдоцільніший для конкретної ситуації.

Розгляд діяльності українських організацій підтверджує, що OSINT завжди супроводжується значними ризиками. Юридичні ризики зумовлені передусім відсутністю чіткого правового регулювання, що ставить дослідника у вразливе становище. Етичні ризики пов'язані з імовірністю заподіяння шкоди особам, які не є об'єктом дослідження. Технічні ризики випливають з недоліків самих даних, що може призвести до помилкових висновків. Репутаційні ризики полягають у вразливості дослідника чи організації до втрати довіри у разі оприлюднення неправдивої інформації. Окремо варто наголосити на ризиках для об'єкта ідентифікації, оскільки розкриття персональних даних може

становити загрозу безпеці чи життю особи. Тому для дослідника важливо відповідально поводитися з даними і намагатися зменшити ризики та їхній вплив на результати розслідування.

На основі отриманих результатів сформульовано рекомендації, спрямовані на вдосконалення OSINT-діяльності в Україні. Передусім обґрунтовано потребу в розробленні спеціалізованого законодавства, яке б закріпило на законодавчому рівні відкриту розвідку, порядок подання отриманих даних як доказів та відповідальність за оприлюднення неперевіреної інформації. Доцільним є створення діючої експертної ради з етики OSINT, яка б забезпечувала фахове розв'язання спірних ситуацій. Необхідним є поглиблення міжнародної співпраці, що сприятиме підвищенню якості підготовки фахівців та зміцненню позицій України в цій сфері.

Отже, проведене дослідження показало, що відкрита розвідка в Україні на сьогодні вийшла за межі суто технічного інструментарію. Вона сформувалося в окреме явище зі своєю внутрішньою логікою, усталеними правилами, а також постійними ризиками. Динаміка розвитку відкритої розвідки в Україні виявилася такою, що практичний досвід накопичувався значно швидше, ніж встигали реагувати наука й право. У результаті першочерговим завданням стає не генерування нових знань, а систематизація та нормативне оформлення вже здобутого.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. Аврамова О. Віртуальна (цифрова) особистість: суб'єктивний та об'єктивний. *Збірник наукових праць НДІ ПЗІР НАПрН України.* 2022. С. 52–56.

2. Аналітики Molfar ідентифікували п’ятьох елітних спецпризначенців «Сенежу», ліквідованих в Україні. *Бабель*. URL: https://babel.ua/news/110305-analitiki-molfar-identifikuvali-p-yatoh-elitnih-specpriznachenciv-senezhu-likvidovanih-v-urkajini (дата звернення: 20.04.2026).

3. Аналітики Molfar підтвердили використання росіянами супутникових фото зі США для ударів по Україні. *NGL.media*. URL: https://ngl.media/2024/05/29/analitiki-molfar-pidtverdili-vikoristannya-rosiyanami-suputnikovih-foto-zi-ssha-dlya-udariv-po-ukrayini/ (дата звернення: 20.04.2026).

4. Аутентифікація, авторизація та ідентифікація. *Онлайн-курси від компанії QATestLab*. URL: https://training.qatestlab.com/blog/technical-articles/authentication-authorization-and-identification/ (дата звернення: 05.01.2026).

5. Бушуєв С. Розвиток освітніх програм на основі їх цифрового сліду. *Інформаційні технології і засоби навчання*. 2021. С. 18–32.

6. Волинець В. Цифрові сліди та тіні. IX Всеукраїнська студентська науково – технічна конференція «Природничі та гуманітарні науки. актуальні питання». 2016. С. 34–35.

7. Главацька А., Ангельська О., Опірський І. Дослідження технології використання OSINT як нової загрози з деанонімізації особи в інтернет просторі. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. № 1(25). С. 19–50. DOI: https://doi.org/10.28925/2663-4023.2024.25.1950

8. Гловюк І. Оцінка результатів OSINT у судовій практиці: окремі питання. *Науковий вісник УжНУ. Серія: Право*. 2025. № 91, 4. С. 251–259. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/11/37-3.pdf (дата звернення: 05.01.2026).

9. Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua (дата звернення: 20.03.2026).

10. Дія. URL: https://diia.gov.ua/ (дата звернення: 11.03.2026).

11. Електронний підпис Дія. *«ДІЯ». Кваліфікований електронний підпис*. URL: https://ca.diia.gov.ua/ (дата звернення: 11.03.2026).

12. Івкова В., Опірський І. Дослідження існуючих засобів та підходів до проведення OSINT в контексті інформаційної безпеки особи та держави. *Комп'ютерні мережи та системи*. 2025. № 7(1). С. 143–159. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2025/may/38968/k250473-145-161_0.pdf (дата звернення: 10.01.2026).

13. Ідентифікація – Вікіпедія. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/Ідентифікація (дата звернення: 11.01.2026).

14. ІнформНапалм. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/ІнформНапалм#cite_note-19 (дата звернення: 20.04.2026).

15. Коновалова Д. Особливості використання розвідки на основі відкритих джерел (OSINT) у кримінальному провадженні. *Юридичний науковий електронний журнал*. 2024. № 11. С. 459–462. URL: https://www.lsej.org.ua/11_2024/108.pdf (дата звернення: 11.01.2026).

16. Костенко О. Електронна юрисдикція, метавсесвіт, штучний інтелект, цифрова особистість, цифровий аватар, нейронні мережі: теорія, практика, перспективи. *Наукові інновації та технології*. 2022. № 2 (4). С. 54–78.

17. Ланде Д. OSINT у кібербезпеці. Київ : ТОВ «Інжиніринг», 2024. 522 с.

18. Миротворець. URL: https://myrotvorets.center/ (дата звернення: 24.04.2026).

19. Міністерство цифрової трансформації України. URL: https://thedigital.gov.ua/ (дата звернення: 11.03.2026).

20. Мосіюк В. О. Проблеми та перспективи цифровізації архівної діяльності органів місцевого самоврядування (на прикладі Луцької міської

ради). *Актуальні питання інформаційної діяльності: традиції та інновації* : зб. матеріалів XI Міжнародної науково-практичної студентської конференції, м. Одеса, 26 березня 2026 р. 2026. С. 96–101.

21. Одерій О., Кожевніков О. Отримання криміналістично значущої інформації шляхом аналізу відкритих інтернет-джерел. *Правовий часопис Донбасу*. 2020. № 4 (73). С. 144–155. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/474ecadd-4472-45e7-bb0c-55541851b4fa/content (дата звернення: 05.01.2026).

22. Право на недоторканність сімейного життя.Конституційний Суд України. *Конституційний Суд України*. URL: https://ccu.gov.ua/storinka-knygy/429-pravo-na-nedotorkannist-simeynogo-zhyttya?utm_source=chatgpt.com (дата звернення: 11.03.2026).

23. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 № 851-IV : станом на 1 січ. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 11.03.2026).

24. Про електронну ідентифікацію та електронні довірчі послуги : Закон України № 2155-VIII : станом на 18 груд. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 11.03.2026).

25. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус : Закон України від 20.11.2012 № 5492-VI : станом на 14 черв. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/5492-17#Text (дата звернення: 11.03.2026).

26. Про інформацію : Закон України від 02.10.1992 № 2657-XII : станом на 20 січ. 2026 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 11.03.2026).

27. Про публічні електронні реєстри : Закон України від 18.11.2021 № 1907-IX : станом на 18 листоп. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/1907-20#Text (дата звернення: 11.03.2026).

28. Рейнська В. Цифровий слід і цифрова гігієна: як захистити персональні дані від зловмисників. *Цифрова трансформація освіти і науки* : матеріали II Всеукр. науково-практ. конф., м. Харків, 14–15 берез. 2024 р. С. 197–200. URL: https://www.researchgate.net/profile/Olena-Yarys/publication/385249056_VIKORISTANNA_STUCNOGO_INTELEKTU_V_BIOLOGICNIH_DOSLIDZENNAH/links/671beb35df4b534d4ef5280e/VIKORISTANNA-STUCNOGO-INTELEKTU-V-BIOLOGICNIH-DOSLIDZENNAH.pdf#page=198 (дата звернення: 09.01.2026).

29. Росіяни купують в Maxar і Planet фото, щоб обстрілювати Україну? Аналітика Molfar за матеріалом The Atlantic. *Molfar intelligence institute*. URL: https://www.molfar.institute/chy-kupuyut-rosiyany-v-maxar-i-planet-foto-shchob-obstrilyuvaty-ukrainu/ (дата звернення: 20.04.2026).

30. Стаття 32 : Конституція України. URL: https://constitution.in.ua/articles/32/ (дата звернення: 11.03.2026).

31. Термін «Ідентифікація».Термінологія законодавства.Законодавство України. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/term/10892 (дата звернення: 11.03.2026).

32. У відповідь за Донбас. Активісти знову опублікували дані російських пілотів, які проводять бомбардування в Сирії. *NV*. URL: https://nv.ua/ukr/world/countries/u-vidpovid-za-donbas-aktivisti-znovu-opublikuvali-dani-rosijskih-pilotiv-jaki-provodjat-bombarduvannja-v-siriji-74959.html (дата звернення: 20.04.2026).

33. Уповноважений Верховної Ради України з прав людини. URL: https://ombudsman.gov.ua/ (дата звернення: 11.03.2026).

34. Чи дійсно «Миротворець» є «списком смерті»?. Factcheck.bg. URL: https://factcheck.bg/uk/chi-dijsno-mirotvorec-ie-spiskom-smerti/ (дата звернення: 20.04.2026).

35. Шевчук В. Використання технологій штучного інтелекту в OSINT як напрям підвищення ефективності розслідування воєнних злочинів. Роль OSINT-досліджень у підвищенні рівня національної безпеки України :

матеріали круглого столу. 2025. С. 239–244. URL: https://dspace.nlu.edu.ua/server/api/core/bitstreams/56d2e22d-9f1f-4ff9-a6f2-5e6fe0c53f60/content (дата звернення: 05.01.2026).

36. «Школа ідентифікації зла» – розслідувачі «Слідство.Інфо» запрошують регіональних журналістів на авторський тренінг. *Слідство.Інфо*. URL: https://www.slidstvo.info/news/slidstvo-info-zaproshuye-regionalnyh-zhurnalistiv-na-avtorski-treningy-vid-komandy-rozsliduvachiv-shkola-identyfikatsiyi-zla (дата звернення: 11.03.2026).

37. Що таке MobileID?. "ДІЯ".Кваліфікований електронний підпис. URL: https://ca.diia.gov.ua/faq2 (дата звернення: 11.03.2026).

38. BankID НБУ. *Національний банк України*. URL: https://bank.gov.ua/ua/bank-id-nbu (дата звернення: 11.03.2026).

39. Bellingcat з'явилися за два дні до катастрофи рейсу MH17 і зробили собі ім'я на цьому розслідуванні. Як усе починалося? Хто допоміг довести причетність Росії?. *Бабель*. URL: https://babel.ua/texts/62094-bellingcat-z-yavilisya-za-dva-dni-do-katastrofi-reysu-mh17-i-zrobili-sobi-im-ya-na-comu-rozsliduvanni-yak-use-pochinalosya-hto-dopomig-dovesti-prichetnist-rosiji-rozpovidaye-zasnovnik-eliot-higgins (дата звернення: 21.04.2026).

40. OSINT (Розвідка відкритих джерел) в екосистемі зв`язаних термінів. *DSS BI Consult+*. URL: https://dss-bi.blogspot.com/2019/01/osint.html (дата звернення: 11.01.2026).

41. Bellingcat's Online Investigation Toolkit. *Bellingcat*. URL: https://bellingcat.gitbook.io/toolkit (date of access: 11.03.2026).

42. Bellingcat – the home of online investigations. *Bellingcat*. URL: https://www.bellingcat.com/ (date of access: 11.03.2026).

43. Bozkurt, A., Tu, C-H. Digital Identity Formation: Socially Being Real And Present On Digital Networks. *Educational Media International*. 2016. 53(3). P. 153-167.

44. Bucaj S., Bantan M. Towards a Systematic Literature Review of Common PII Identification labels Patterns Based on OSINT. 2024. URL: https://aisel.aisnet.org/neais2024/15/ (date of access: 10.01.2026).

45. Case mounts against Russians in MH17 crash. *Daily Mail Online*. URL: https://www.dailymail.com/wires/aap/article-3080805/Case-mounts-against-Russians-MH17-crash.html (date of access: 20.04.2026).

46. European Court of Human Rights. *HUDOC*. URL: https://hudoc.echr.coe.int/ukr#%7B"documentcollectionid2":["GRANDCHAMBER", "CHAMBER"]%7D (date of access: 11.03.2026).

47. FBI Seeking Information Related to Violent Activity at the U.S Capitol Building. FBI URL: https://www.fbi.gov/contact-us/field-offices/washingtondc/news/press-releases/fbi-seeking-information-related-to-violent-activity-at-the-us-capitol-building-010621 (date of access: 12.03.2026).

48. General Data Protection Regulation (GDPR) – Legal Text. *General Data Protection Regulation (GDPR)*. URL: https://gdpr-info.eu/ (date of access: 11.03.2026).

49. G R. What is Open-Source Intelligence?. *SANS Institute*. URL: https://www.sans.org/blog/what-is-open-source-intelligence (date of access: 09.01.2026).

50. Hewson J. A Private Company Is Using Social Media to Track Down Russian Soldiers. *Foreign Policy*. URL: https://foreignpolicy.com/2023/03/02/ukraine-russia-war-military-social-media-osint-open-source-intelligence/ (date of access: 10.01.2026).

51. Home.Homeland Security. *U.S. Department of Homeland Security*. URL: https://www.dhs.gov/ (date of access: 11.03.2026).

52. Identification of Russian soldier looter from Bucha by stolen AirPods. *Molfar intelligence institute*. URL: https://www.molfar.institute/en/russian-soldier-looter-bucha/ (date of access: 21.04.2026).

53. InformNapalm. URL: https://informnapalm.org/ (date of access: 28.04.2026).

54. Layton R., Watters P. Automating Open Source Intelligence. Algorithms for OSINT. 2015. 222 p.

55. Mayda M. Digital footprint management in digital visual culture. *Journal of Erciyes Communication*. 2022. Vol. 9, no. 2. P. 1031–1044.

56. Molfar. URL: https://molfar.com/ (date of access: 19.04.2026).

57. Myrotvorets. *Wikipedia*. URL: https://en.wikipedia.org/w/index.php?printable=yes&title=Myrotvorets (date of access: 19.04.2026).

58. Office of the Director of National intelligence. URL: https://www.dni.gov/ (date of access: 09.03.2026).

59. OSINT Framework. URL: https://osintframework.com/ (date of access: 10.03.2026).

60. Shaojie Min, Kebing Liu. From Identification to Obfuscation: A Survey of Cross-Network Mapping and Anti-Mapping Methods. *Computers, Materials and Continua.* 2025. Vol. 86, no. 2. P. 1–23. URL: https://www.sciencedirect.com/org/science/article/pii/S1546221825012408 (date of access: 10.01.2026).

61. The Beginner's Guide to Open-Source Intelligence (OSINT): Techniques and Tools. *Medium*. URL: https://medium.com/@techmindxperts/the-beginners-guide-to-open-source-intelligence-osint-techniques-and-tools-6a91b9c37ee1 (date of access: 11.01.2026).

62. Walkow M., Pohn D. Systematically Searching for Identity-Related Information in the Internetwith OSINT Tools. 9th International Conference on Information Systems Security and Privacy. 2023. P. 402–409. URL: https://www.scitepress.org/publishedPapers/2023/116442/pdf/index.html (date of access: 05.01.2026).

63. Website leaks personal information of more than 4,000 journalists ➜ ZMINA. *ZMINA*. URL: https://zmina.info/en/articles-en/vitik_personalnih_danih_4000_zhurnalistiv_khto_vidpovist-3/#page_menu (date of access: 19.04.2026).

64. What is a digital footprint? Definition & examples. *Norton AntiVirus, Privacy, Identity, & Advanced Scam Protection*. URL: https://us.norton.com/blog/privacy/digital-footprint (date of access: 10.01.2026).

65. What is OSINT Open Source Intelligence? CrowdStrike. *CrowdStrike: We Stop Breaches with AI-native Cybersecurity*. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/open-source-intelligence-osint/ (date of access: 10.01.2026).

66. What is OSINT (Open Source Intelligence)?. *SentinelOne*. URL: https://www.sentinelone.com/cybersecurity-101/threat-intelligence/open-source-intelligence-osint/? (date of access: 10.01.2026).

67. What we investigate?. *FBI*. URL: https://www.fbi.gov/investigate (date of access: 18.04.2026).

68. Williams H. J., Blum I. Defining second generation open source intelligence (OSINT) for the defense enterprise. RAND Corporation, 2018. 48 p.

ДОДАТКИ

Додаток А

Сертифікат участі у XI Міжнародній науково-практичній студентській конференції «Актуальні питання інформаційної діяльності: традиції та інновації» в Національному університеті «Одеська політехніка»

Міністерство освіти і науки України
Національний університет "Одеська політехніка"

СЕРТИФІКАТ

учасника конференції

цим сертифікатом підтверджується, що

Вікторія МОСІЮК

успішно пройшла професійну програму
підвищення кваліфікації 15 годин (0,5 кредиту ECTS)

у формі участі в роботі XI Міжнародної науково-практичної студентської конференції "Актуальні питання інформаційної діяльності: традиції та інновації", підготовки індивідуального проєкту – доповіді за тематикою конференції та керівництва науковою роботою здобувача освіти

Голова оргкомітету,
Заслужений працівник освіти України,
Президент Національної спілки
документознавців України

Василь СПРІНСЯН

№ OP-IDMK-SC-2026-033

м. Одеса
26 березня 2026

Додаток Б

OSINT-інструменти для ідентифікації цифрової особистості

Назва інструменту	URL	Тип даних	Опис
Blackbird	github.com/p1ngul1n0/blackbird	Юзернейм	Шукає акаунти за нікнеймом на 600+ платформах (аналог Sherlock).
Clarity Project	clarity-project.info	ПІБ, компанія	Зв'язки людей з компаніями, статутні фонди, судові процеси.
DeHashed	dehashed.com	Email, ім'я, телефон, хеш	Пошук по злитих базах, показує фрагменти даних (паролі хешовані).
Epieos	epieos.com	Email, телефон	Пошук пов'язаних акаунтів Google, Skype, Zoom за email.
ExifTool	exiftool.org	Метадані файлів	Читає та записує метадані фото, документів (GPS, дата, камера).
FaceCheck.ID	facecheck.id	Обличчя	Пошук облич у соцмережах, новинах, відео.
Ghidra	ghidra-sre.org	Аналіз ПЗ (для цифрової криміналістики)	Інструмент зворотної розробки від NSA; корисний при аналізі шкідливого ПЗ.
Google Images	images.google.com	Зображення	Зворотний пошук за зображенням (перетягніть файл або вставте URL).
Have I Been Pwned	haveibeenpwned.com	Email, телефон	Перевірка, чи потрапила адреса або номер у відомі зливи баз даних.
Hunter.io	hunter.io	Email за доменом	Пошук корпоративних email-адрес за назвою компанії/домену.
Instant Username Search	instantusername.com	Юзернейм	Шукає профілі з однаковим нікнеймом на тисячах платформ.
IntelX	intelx.io	Email, домен, IP, URL	Пошукова машина по даркнету, зливах і відкритим джерелам.
LeakCheck	leakcheck.net	Email, логін, пароль	База даних зливів, пошук по email/логіну.
Maltego	maltego.com	Графи зв'язків (ПІБ, email, домен)	Платформа для візуалізації зв'язків між об'єктами (люди, компанії, сайти).
Namechk	namechk.com	Юзернейм, домен	Перевіряє доступність імені в соцмережах та доменах.
NumLookup	numlookup.com	Номер телефону	Визначення оператора, регіону, типу лінії (мобільний/стаціонар).

Продовження Додатка Б

OpenDataBot	opendatabot.ua	ПІБ, код ЄДРПОУ	Перевірка компаній, ФОП, судових справ, податкового боргу.
OSINT Framework	osintframework.com	Довідник інструментів	Деревоподібна мапа OSINT-ресурсів за категоріями.
PhoneInfoga	github.com/sundowndev/phoneinfoga	Номер телефону	Сканер номерів: пошук в Google, соцмережах.
PimEyes	pimeyes.com	Обличчя, фото	Знаходить фото, де з'являється людина.
Recon-ng	github.com/lanmaster53/recon-ng	Домени, контакти, IP	Консольний Python-фреймворк для розвідки, подібний до Metasploit.
Sherlock (GitHub)	github.com/sherlock-project/sherlock	Юзернейм	Консольна утиліта Python для пошуку нікнейму на 400+ сайтах.
Shodan	shodan.io	Пристрої, IP, сервіси	Пошук пристроїв, підключених до інтернету.
SnusBase	snusbase.com	Email, нікнейм, хеш	Пошук по понад 500 колекціям зламаних баз.
Social Searcher	social-searcher.com	ПІБ, нік, ключові слова	Моніторинг згадок у соцмережах у реальному часі.
SpiderFoot	spiderfoot.net	IP, домен, email, ПІБ	Автоматизований OSINT-збір інформації, понад 200 модулів.
theHarvester	github.com/laramies/theHarvester	Email, ім'я, субдомени	Збір email-адрес, імен, піддоменів із відкритих джерел.
TinEye	tineye.com	Зображення	Пошук за точним збігом зображення.
Truecaller	truecaller.com	Номер телефону	Глобальна база номерів, показує ім'я абонента, регіон, оператора.
Wayback Machine	web.archive.org	Історія веб-сторінок	Перегляд архівних копій сайтів, профілів, блогів.
WhatsMyName	https://whatsmyname.me/	Юзернейм	Перевіряє наявність нікнейму на 600+ вебсайтах одночасно.
Zlookup	zlookup.com	Номер телефону	Визначення власника номера через месенджери та соцмережі.
База розшуку МВС	wanted.mvs.gov.ua	ПІБ, дата зникнення	Офіційний пошук зниклих безвісти, боржників, злочинців.
Судовий реєстр України	reestr.court.gov.ua	ПІБ, назва справи	Пошук судових рішень за учасниками, суддями, адвокатами.
ЄДРПОУ пошук	usr.minjust.gov.ua	ПІБ, код ЄДРПОУ	Офіційний портал Мін'юсту: перевірка юридичних осіб та ФОП.