https://doi.org/10.31891/2307-5732-2025-355-77
УДК 355.4:004.912

КОРОБЕЙНІКОВА ТЕТЯНА
Національний університет «Львівська політехніка»
https://orcid.org/0000-0003-2487-8742
e-mail: tetianakorobeinikova@gmail.com
СИМАК ІГОР
Національний університет «Львівська політехніка»
e-mail: ihor.symak.mkbbi.2024@lpnu.ua

OSINT-РОЗСЛІДУВАННЯ: МОДЕЛЬ ЦИКЛУ РОЗВІДКИ ТА МЕТОДИ ПОБУДОВИ МІЖОБ'ЄКТНИХ ЗВ'ЯЗКІВ

Стаття пропонує вдосконалений цикл OSINT-розслідування, доповнений методом міжоб'єктних зв'язків, що системно встановлює взаємодії між ключовими сутностями (особа, місце, організація, подія, дія, продукт/система) у процесі збору даних. Деталізовано обробку об'єкта «особа» за різними вхідними параметрами, що підвищує результативність пошуку та знижує ризик пропуску критичної інформації. Рішення актуальне для військової й правоохоронної розвідки, журналістики та корпоративної безпеки й закладає основу для AI-автоматизації та дашбордів реального часу.

Ключові слова: OSINT-розслідування, цикл розвідки Гібсона, метод міжоб'єктних зв'язків, етап збору даних, об'єкт «особа», військова розвідка, структурування та аналіз даних, результативність пошукових робіт.

KOROBEINIKOVA TETIANA
Lviv National Technical University
SYMAK IHOR
Lviv Polytechnic National University

SECURE ACCESS TO INFORMATION SYSTEM SERVERS, ENABLED BY AN ML MODEL FOR BLOCKING MALICIOUS REQUESTS

This article focuses on addressing the task of improving the effectiveness of OSINT investigations, particularly in the context of the war in Ukraine. The study aims to analyze and enhance existing methods and tools for establishing inter-object relationships in the field of intelligence data collection. As a result of examining modern OSINT (Open Source Intelligence) technologies and their capabilities, Gibson's intelligence cycle model was chosen as the baseline. The well-known six-level Gibson intelligence cycle model has been analyzed and expanded, and an improvement is proposed by introducing the method of inter-object relationships during the data collection process. The proposed inter-object relationships method allows for structuring and monitoring the interconnections among the main OSINT entities (person, place, organization, event, action, product/system), thereby enabling a comprehensive evaluation of heterogeneous information. Particular attention is paid to the "person" entity, for which a detailed scheme of applying the inter-object relationships method has been developed, depending on the available input parameters (name, alias, address, phone number, email, etc.). The practical significance of this scheme is evidenced by the increased effectiveness of search operations, more flexible search settings, and a reduced risk of overlooking critical information. The approaches described are relevant to military intelligence, law enforcement agencies, investigative journalism, and corporate security. The presented results may serve as a foundation for expanding the data sources, automating the inter-object relationships process using artificial intelligence, and developing intelligent dashboards for real-time information visualization and monitoring. The research is based on analytical work with up-to-date literature sources and various types of information resources, as well as on the practical application of OSINT methods during intelligence data collection.

Keywords: OSINT investigation, Gibson intelligence cycle, inter-object relationship method, data-collection phase, Person entity, military intelligence, data structuring and analysis, search performance.

Стаття надійшла до редакції / Received 27.05.2025
Прийнята до друку / Accepted 26.06.2025

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

В сучасному світі інформація стає ключовим ресурсом, а її збір та аналіз відіграють важливу роль у різних сферах: розвідку, бізнес, журналістику та наукові дослідження. Технології OSINT надають потужні інструменти для збору та аналізу інформації з відкритих джерел, таких як веб-сайти, соціальні мережі, публічні бази даних та інші онлайн-ресурси. Історія розвитку технологій OSINT складається з чотирьох етапів [1-10], перший з яких датується 1941 роком. В цьому напрямку працюють чимало відомих організацій, зокрема такі як: Bellingcat, The Atlantic Council's Digital Forensic Research Lab (DFRLab), The Citizen Lab, Forensic Architecture, Trace Labs, InformNapalm, Bellingcat Ukraine, Molfar, Ukrainian Cyber Alliance та Bihus.Info [11-20]. Деякі осередки, як-от Molfar та Ukrainian Cyber Alliance, не зосереджуються виключно на OSINT-розслідуваннях, але використовують їх у своїй роботі.

В умовах війни в Україні, отримання розвідданих стає критично важливим завданням для забезпечення національної безпеки та оборони держави [2]. Традиційні методи розвідки, такі як агентурна діяльність та супутникове спостереження, часто є дорогими, складними та небезпечними. Водночас технології OSINT пропонують гнучкий, доступний та етичний інструмент для збору розвідданих з відкритих джерел. Оскільки соціальні мережі, сервіси та інші онлайн ресурси стали невід'ємною частиною сучасного життя, люди, зокрема громадяни рф, нічого не підозрюючи, публікують велику кількість особистої та військової інформації в Інтернеті, що робить її цінним джерелом даних для OSINT-розслідувань. Враховуючи

вищезазначене, дослідження методів пошукових робіт та інструментів OSINT є надзвичайно актуальним в умовах війни в Україні.

Таким чином, існує потреба у аналізі та вдосконаленні моделей циклу розвідки. Основна увага приділяється 1) розробці розширеного процесу збору даних на основі методу міжоб'єктних зв'язків та 2) вдосконаленню процесу пошукових робіт для об'єкта типу «особа».

Технологічний ланцюжок процесу OSINT розслідування

Існує багато різних підходів до формалізації процесу OSINT розслідування. З метою перетворення необроблених даних на оперативну розвідувальну інформацію, Офіс директора Національної розвідки США (Office of the Director of National Intelligence) розробив модель під назвою "цикл розвідки" (intelligence cycle) [21]. Ця модель застосовується до всіх джерел розвідданих, включаючи OSINT, і була прийнята Гібсоном [22], а згодом із деякими модифікаціями, Хассаном та Хіджазі [23]. Базелл пропонує практичну інтерпретацію цієї моделі, яка використовується урядовими установами США як обов'язковий навчальний посібник [24].

Інші дослідження зосереджуються на зборі та аналізі інформації, пропонуючи моделі, орієнтовані на ці завдання. До них належать комплексна триетапна модель, розроблена Пастором [25], та модель Табатабаеї [26]. Розглянемо модель циклу розвідки Гібсона, оскільки вона є найбільш повною та активно використовується Національною розвідкою США (рис. 1).

Модель циклу розвідки Гібсона складається з шести етапів, що виконуються циклічно. Шостий крок, оцінка (яка має на меті отримання зворотного зв'язку від користувачів) проводиться для кожного з інших п'яти етапів окремо і для розвідки в цілому.

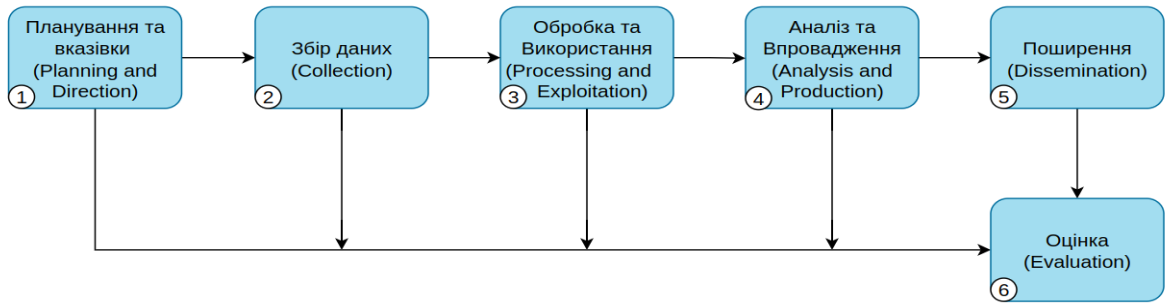

Рис. 1 – Модель циклу розвідки Гібсона

1) Планування та вказівки. Цей етап є фундаментом циклу розвідки. Це відправна точка, з якої запускаються усі інші дії циклу. Часто, вказівки передують безпосередньому плануванню. Зазвичай, у таких випадках споживач потребує конкретного продукту. Цей продукт може бути повним звітом, графічним зображенням або сирими даними, які збираються та поширюються, але оминають етап аналізу та обробки;

2) Збір даних. Етап, на якому отримуються необроблені дані, необхідні для створення кінцевого продукту. Збір даних проводиться для того, щоб зібрати невпорядковану інформацію, що стосується п'яти основних джерел розвідки (геопросторової розвідки (GEOINT), людської розвідки (HUMINT), розвідки за вимірювальними ознаками та сигналами (MASINT), розвідки з відкритих джерел (OSINT) та сигнальної розвідки (SIGINT)). Джерелами необроблених даних можуть бути новини, аерофотознімки, супутникові зображення, урядові та публічні документи;

3) Обробка та використання. Етап перетворення необроблених даних на зрозумілий формат, придатний для створення кінцевого продукту. Цей етап передбачає залучення висококваліфікованого спеціалізованого персоналу та використання технологічно складного обладнання для перетворення сирої інформації на зрозумілі та корисні відомості. Переклад даних, їх розшифровка та інтерпретація відзнятих зображень – це лише декілька методів перетворення даних, що зберігаються на плівці, магнітних носіях або інших носіях, в інформацію, готову до аналізу та обробки кінцевого продукту;

4) Аналіз та впровадження – це етап інтеграції, оцінки, аналізування та підготовки обробленої інформації для включення її до кінцевого продукту. Цей етап також потребує залучення висококваліфікованого та спеціалізованого персоналу (аналітиків), завдання яких полягає у наданні сенсу обробленій інформації та визначенні її пріоритетності відповідно до відомих вимог. Синтезування обробленої інформації у готовий, дієвий розвідувальний продукт дозволяє зробити цю інформацію корисною для замовника. Варто зазначити, що в деяких випадках цикл розвідки може оминати цей етап (наприклад, коли споживачеві потрібна лише конкретна звітна інформація або продукти, такі як необроблені зображення);

5) Поширення – це етап доставлення кінцевого продукту замовнику, який його запросив, а також іншим зацікавленим сторонам. Замовник отримує готовий продукт, зазвичай, через електронну передачу. Поширення інформації зазвичай здійснюється такими засобами, як веб-сайти, електронна пошта, інструменти співпраці та розповсюдження друкованих матеріалів. Кінцевий, готовий продукт називається "завершеною розвідкою" (finished intelligence). Після розповсюдження продукту можуть бути виявлені додаткові прогалини в розвідувальних даних, і цикл розвідки починається знову;

Оцінка – це процес постійного збору відгуків протягом циклу розвідки та їх аналізу для

вдосконалення кожного окремого етапу та циклу загалом. Постійне оцінювання та відгуки від споживачів є надзвичайно важливими, оскільки вони дозволяють учасникам циклу розвідки коригувати та покращувати свою діяльність та аналіз, щоб краще відповідати мінливим та зростаючим інформаційним потребам споживачів.

Формулювання мети роботи

Метою роботи є вдосконалення результативності OSINT-розслідування та демонстрації зв'язків між об'єктами розслідування за рахунок впровадженого методу міжоб'єктних зв'язків.

Процес збору даних на основі об'єктів та метод міжоб'єктних зв'язків

З метою вдосконалення результативності OSINT-розслідування та демонстрації зв'язків між об'єктами розслідування на даному етапі важливо дати відповідь на питання: яким є об'єкт(и) дослідження; як об'єкти пов'язані чи не пов'язані; який план збору на основі операційних вимог.

Розіб'ємо етап збору даних за допомогою зв'язків між об'єктами дослідження. Це дасть змогу зрозуміти як різні сутності/речі можуть бути пов'язані або не пов'язані та розпочати пошуки залежно від конкретного об'єкта. На рисунку 2 зображено схему методу міжоб'єктних зв'язків.

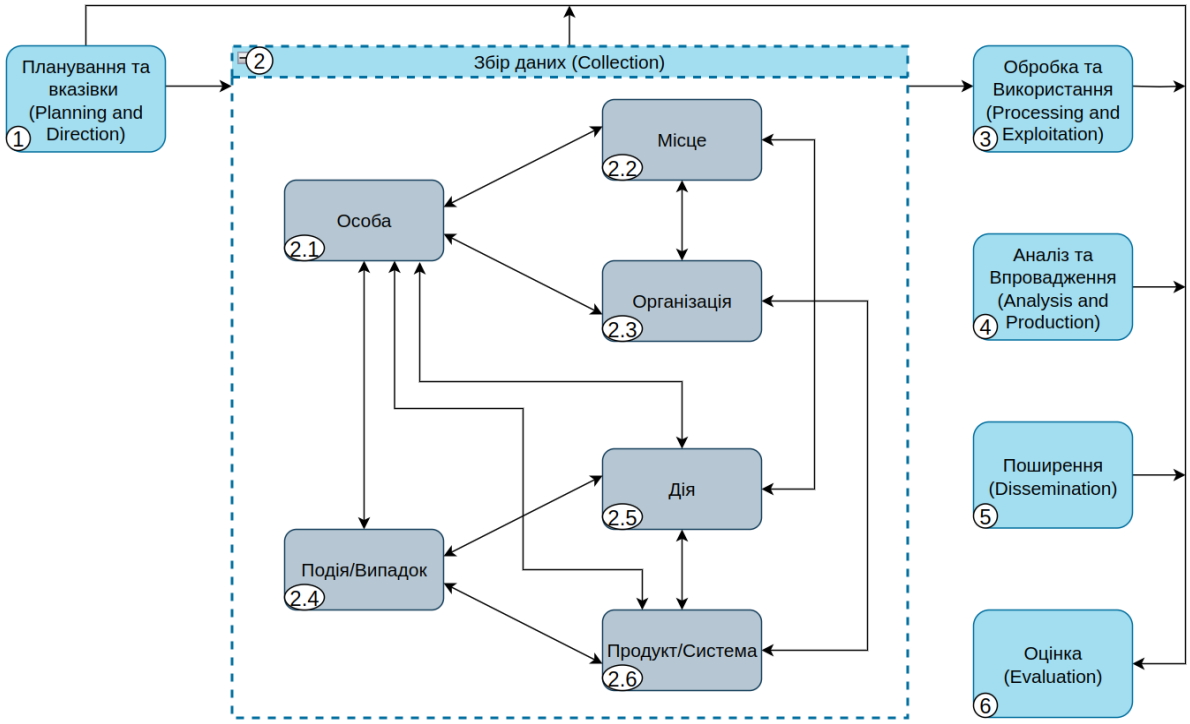

Рис. 2 – Схема методу міжоб'єктних зв'язків

Розглянемо детально запропонований метод міжоб'єктних зв'язків. Він використовує сутності:

– Особа (2.1): Людина, яка брала участь у тій чи іншій події, наприклад, свідок, виконавець або жертва;

– Місце (2.2): Фізична локація, де відбулася подія, наприклад, вулиця, місто, країна або будівля;

– Організація (2.3): Компанія, уряд, або інша група осіб, яка пов'язана з подією, наприклад, поліція, лікарня або школа;

– Подія (2.4): Це те, що сталося, наприклад, злочин, аварія або стихійне лихо. Також до подій можна віднести інциденти в інформаційних системах;

– Дія (2.5): Будь-який навмисний чи не навмисний вид діяльності, що спричинив певну подію;

– Продукт/Система (2.6): Це може бути товар, послуга або система, яка пов'язана з подією, наприклад, транспортний засіб, корпоративна мережа або ПЗ.

Схема методу показує, як ці сутності пов'язані між собою. Міжоб'єктні зв'язки можна описати так:

– Особа-Подія: зв'язок між людьми та подіями, в яких вони беруть участь, свідками яких є або які їх стосуються. Особа може бути учасником, свідком, жертвою або організатором події. Подія може бути злочином, аварією, стихійним лихом, кібератакою або будь-якою іншою подією. Наприклад, свідок може бути присутній на місці злочину, жертва може бути постраждалою від аварії, журналіст бере інтерв'ю у свідка злочину;

– Особа-Дія: зв'язок між людьми та діями, які вони здійснюють, свідками яких є або які їх стосуються. Особа може бути виконавцем, ініціатором, свідком, або жертвою дії. Наприклад, працівник, що залишив паролі на робочому місці;

– Особа-Організація: стосунки між людьми та організаціями, до яких вони належать, або з якими співпрацюють. Наприклад, співробітник компанії, член громадської організації, студент навчального закладу;

– Особа-Продукт/Система: зв’язок між людьми та продуктами або системами, які вони використовують, створюють або обслуговують. Наприклад, користувач соціальної мережі, розробник ПЗ, водій транспортного засобу;

– Особа-Місце: зв’язок між людьми та місцями, де вони живуть, працюють, навчаються, проводять час або були присутні під час певних подій;

– Подія-Дія: зв'язок між подіями та діями, які їх спричинили, супроводжували або були наслідком. Наприклад, злочин – крадіжка, аварія – зіткнення транспортних засобів, компрометація даних – витік інформації;

– Подія-Продукт/Система: зв'язок між подіями та продуктами або системами, які були задіяні, спричинили або стали наслідком події. Продукт або система може бути інструментом, причиною, наслідком або супутнім фактором події. Наприклад, пожежа – система пожежогасіння, компрометація даних – програмне забезпечення;

– Місце-Організація: зв'язок між місцями та організаціями, які розташовані в цих місцях, володіють ними або ведуть там свою діяльність. Місце може бути адресою, територією, географічною локацією або віртуальним простором. Наприклад, школа в певному районі міста, штаб-квартира компанії в певному місті;

– Місце-Дія: зв'язок між місцями та діями, які відбуваються в цих місцях. Наприклад, злочин, скоєний в певному районі міста, аварія на певному відрізку дороги;

– Організація-Продукт/Система: зв'язок між продуктами або системами та організаціями, які їх розробляють, виробляють, продають, обслуговують або використовують. Наприклад, програмне забезпечення, розроблене певною компанією, комп'ютерна мережа, що використовується в певному навчальному закладі, операційна система, що використовується в державних установах;

– Продукт/Система-Дія: зв’язок між діями та продуктами або системами, які використовуються, створюються або обслуговуються внаслідок цих дій. Продукт або система може бути інструментом, причиною, наслідком або супутнім фактором дії. Наприклад, кібератака, яка спричинила витік даних, збої в роботі корпоративної мережі або вихід з ладу системи електроживлення.

Важливо зазначити, що всі ці зв'язки можуть бути двосторонніми. Починаючи з сутності «особа» як відправної точки збору даних, можна побачити, як зв'язки з усіма іншими сутностями чітко визначаються цим шляхом. Це допомагає зрозуміти, як вони можуть бути пов'язані (і як їх потім можна відобразити).

З іншого боку, якщо визначити сутність «Дія» (наприклад, хтось напав на щось, а подією є напад), ви можете швидко простежити шляхи її перетину з сутністю «Подія» та встановити прямий зв'язок з «Особою». Через ланцюжок зв'язків другого чи третього порядку, можливо, можна буде встановити зв'язок з «Організацією».

Розглянемо це на прикладі сценарію використання:

1) Починаючи з особи, ми починаємо наше OSINT розслідування у Facebook, Instagram, публічних базах даних, LinkedIn тощо. Ми використовуємо схему особи , щоб отримати відповідну інформацію про особу та реєструвати її структурованим способом;

2) Тепер дивимося на блок-схему і бачимо, що негайно слід розглядати місця та організації як пов’язані сутності та почати збирати інформацію про ті, які пов’язані з досліджуваною особою. Наприклад, ми визначаємо, що особа регулярно відвідує кафе, тому ми збираємо та фіксуємо пов’язану інформацію про організацію та місце. У нас також є можливість реєструвати додаткову інформацію, жодних важливих даних не слід ігнорувати – їх обов’язково занотовуємо;

3) В даному прикладі тепер можна шукати потенційні дії чи події, які відбулися в одному з місць і знаходити пов’язану інформацію та, можливо, розширювати мережу присутніх людей для подальшого розслідування.

Застосування методу міжоб’єктних зв’язків в OSINT-розслідуванні для об'єкта типу «особа»

Оскільки ключовим об’єктом схеми, представленої на рисунку 2 є «особа», зупинимось на ньому більш детально. Для результативного проведення OSINT розслідування потрібно також розуміти зв’язок між типом вхідних даних та джерелами пошуку інформації про особу.

На рис. 3 наведено схема застосування методу міжоб’єктних зв’язків для об'єкта «особа» в залежності від вхідних даних.

Схема застосування методу міжоб’єктних зв’язків для об'єкта «особа» в залежності від вхідних даних (рис. 3) містить такий перелік вхідні дані з яких можна почати OSINT розслідування:

– справжнє ім'я та прізвище (2.1.2): Найважливіший параметр для ідентифікації людини в онлайн-джерелах;

– псевдонім (2.1.3): Додатковий параметр для пошуку людини під різними іменами;

– електронна пошта (2.1.4): Дозволяє знайти профілі в соцмережах, онлайн-рахунки та іншу інформацію;

– адреса (2.1.5): Допомагає знайти місце проживання, роботу та інші пов'язані місця;

– місце роботи (2.1.6): Дозволяє знайти профіль LinkedIn, публікації про роботу та профільні сайти;

– фото (2.1.7): Допомагає візуально ідентифікувати людину та знайти її фото в інших джерелах;

– ідентифікаційний номер (2.1.8): Дозволяє знайти офіційні документи, записи про власність та іншу інформацію;

– родичі/друзі (2.1.9): Допомагає знайти зв'язки людини та розширити коло пошуку;

– номер автомобіля (2.1.10): Дозволяє знайти інформацію про реєстрацію, штрафи та інші дані про власника;

– соціальні мережі (2.1.11): Дають доступ до публікацій, фото, друзів та інших деталей про життя людини;

– мобільний номер (2.1.12): Дозволяє знайти профіль в соцмережах, записи про дзвінки та SMS-повідомлення.

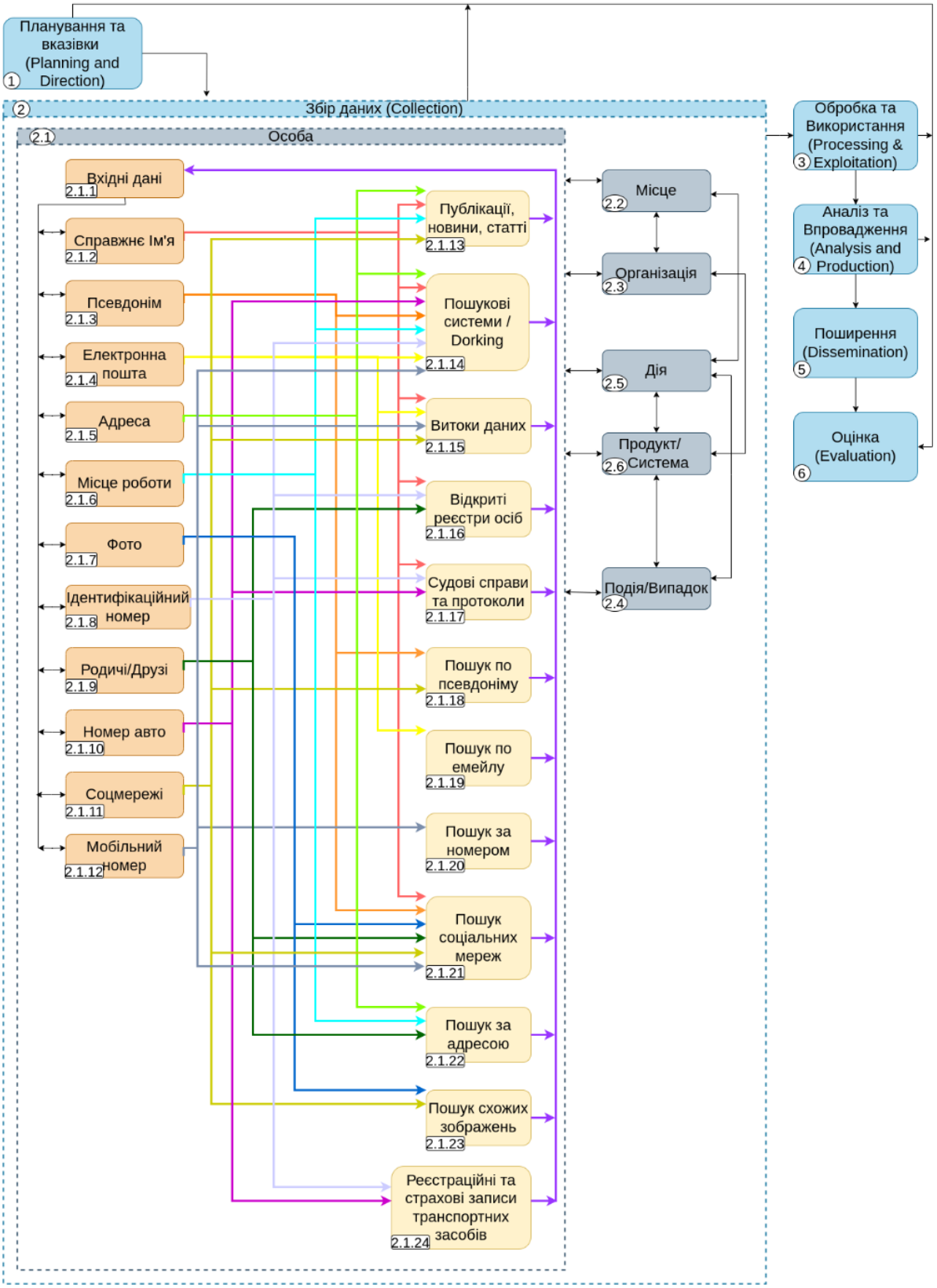

Рис. 3 – Схема застосування методу міжоб'єктних зв'язків для об'єкта «особа» в залежності від вхідних даних

Залежно від наявності, розслідування може ґрунтуватися на одному або декількох параметрах, що значно підвищує його ефективність.

Для кожного з представлених параметрів схема чітко окреслює джерела інформації, демонструючи зв'язок між вхідними даними та конкретними ресурсами.

Пропонується використовувати такі джерела пошуку:

– Пошук статей, новин, публікацій (2.1.13): Використання пошукових систем для пошуку статей, новин, публікацій в блогах та інших згадок про людину в ЗМІ. Використання пошукових систем з ім'ям, псевдонімом, професією, місцем проживання, подіями, в яких людина могла брати участь тощо;

– Пошукові системи та Dorking (2.1.14): Використання пошукових систем з ім'ям, псевдонімом, електронною поштою, номером телефону, місцем проживання, датою народження тощо, щоб знайти згадки про людину в інтернеті. Використання спеціальних операторів, розглянутих у розділі 2.3, для точного пошуку інформації на певних сайтах, в певних форматах. Одне з основних джерел пошуку;

– Витоки даних (2.1.15): Пошук інформації на сайтах, які публікують дані з витоків інформації, хакерських атак, зливів баз даних. Пошук інформації в даркнеті, де можуть продаватися або публікуватися дані про людей, здобуті незаконним шляхом;

– Відкриті реєстри осіб (2.1.16): Пошук інформації в державних реєстрах нерухомості, шлюбу, народжень, смертей, виборців, платників податків тощо. Перегляд комерційних реєстрів компаній, де людина могла бути директором, власником, співробітником;

– Судові справи та протоколи (2.1.17): Пошук інформації в базах даних судових рішень, протоколів засідань, кримінальних справ, де людина могла бути фігурантом, свідком, потерпілим. Перегляд інформації про штрафи, правопорушення, адміністративні стягнення, де людина могла бути зафіксована;

– Пошук по псевдоніму (2.1.18): Аналогічно до пошуку за ім'ям, здійснюється пошук в соціальних мережах, публікаціях, новинах, статтях, форумах, але з використанням псевдоніма людини. Можна використовувати додаткові методи, такі як пошук зображень за псевдонімом, щоб знайти згадки про людину в підписах до фотографій чи зображеннях, створених під цим псевдонімом;

– Пошук по емейлу (2.1.19): Введення електронної пошти в пошукові системи для пошуку згадок про неї в відкритих джерелах, наприклад, на форумах, в коментарях, реєстраціях на сайтах. Перевірка електронної пошти в спеціальних сервісах, які показують, чи є вона в базах даних витоків інформації;

– Пошук за номером (2.1.20): Введення номера телефону в пошукові системи для пошуку згадок про нього в відкритих джерелах, наприклад, в оголошеннях, на сайтах знайомств, форумах. Деякі країни мають публічні бази даних номерів телефонів, де можна знайти інформацію про абонента за номером;

– Пошук соціальних мереж (2.1.21): Використання спеціальних сервісів та інструментів, які дозволяють шукати профілі в соціальних мережах за ім'ям, електронною поштою, номером телефону (розділ 2.4). Іноді можна знайти людину в одній соціальній мережі, використовуючи інформацію з іншої, наприклад, ім'я користувача або фотографію. Перегляд профілів особи, щоб знайти інформацію про її життя, друзів, інтереси, роботу тощо;

– Пошук за адресою (2.1.22): Введення адреси в пошукові системи та карти для того, щоб знайти пов'язану з нею інформацію, наприклад, супутникові знімки, панорами вулиць, публічні записи про власність. Деякі сайти дозволяють шукати людей, які проживають за певною адресою, проте, ця інформація не завжди є достовірною та відкритою;

– Пошук схожих зображень (2.1.23): Завантаження фотографії розшукуваної людини в пошукові системи зображень, щоб знайти схожі зображення. Це може допомогти знайти інші фото людини, зроблені в різний час, під іншими іменами або з іншого ракурсу;

– Реєстраційні та страхові записи транспортних засобів (2.1.24): Деякі країни мають публічні бази даних реєстрації транспортних засобів, де можна знайти інформацію про власника автомобіля за його номерним знаком чи VIN-кодом. Аналогічно, можуть бути доступні бази даних страхових компаній, які дозволяють знайти власника застрахованого транспортного засобу.

Запропонована хема застосування методу міжоб’єктних зв’язків для об'єкта «особа» в залежності від вхідних даних є загальним описом процесу пошуку інформації про особу в OSINT-аналізі на етапі збору даних. На практиці цей процес може варіюватися залежно від конкретних обставин та цілей дослідження.

Найкращий метод пошуку буде залежати від наявної інформації про шукану людину. Наприклад, якщо є ім'я та прізвище особи, можна почати з пошуку в соціальних мережах, публікаціях, новинах та статтях. Якщо є номер телефону або адреса електронної пошти, можна спробувати знайти людину в публічних базах даних або за допомогою спеціальних сервісів.

Важливо використовувати всі доступні методи пошуку, щоб збільшити шанси на успіх. Також слід пам'ятати, що деякі з цих методів можуть бути платними або потребувати реєстрації.

Обговорення результатів

Розглянуті у статті моделі та підходи до організації процесу OSINT-розслідування, зокрема цикл розвідки Гібсона, підтверджують важливість системного та послідовного збору, обробки й аналізу інформації. Викладений технологічний ланцюжок процесу OSINT дослідження показав, що найбільша ефективність досягається за умови чіткого розподілу ролей і використання відповідних інструментів для кожного етапу.

Запропонований метод міжоб'єктних зв'язків дозволяє структурувати велику кількість невпорядкованих даних та відстежувати ланцюжки взаємозв'язків. У межах розвідки з відкритих джерел це має критичне значення для цілісного розуміння того, як різні суб'єкти та чинники впливають на розслідувану подію. Основною перевагою такого підходу є можливість переходу від одного об'єкта розслідування до іншого через встановлені зв'язки (наприклад, від «особи» до «організації» або від «події» до «системи») з використанням відкритих джерел даних. Це відкриває додаткові шляхи пошуку.

Особливої уваги заслуговує застосування методу міжоб'єктних зв'язків для об'єкта «особа» в залежності від вхідних даних, де детально розглянуто, які вхідні дані можуть стати відправною точкою (реальне ім'я, псевдонім, адреса, мобільний номер тощо) та які джерела пошуку доцільно залучати. Така диференціація методів допомагає швидко визначити найпріоритетніші напрями розслідування, уникнути дублювання зусиль і знизити ризик пропустити важливу інформацію. Практичні кейси демонструють, що чим повніше та точніше визначено початкові характеристики (наприклад, підтверджені дані про місце роботи чи псевдонім), тим вища ймовірність швидкого і результативного отримання потрібних даних.

Результативність OSINT-розслідування залежить від: 1) коректності початкових даних (неповні або помилкові відомості можуть призвести до неправильних висновків чи затримок у розслідуванні); 2) доступності інструментів для збору й обробки даних (використання платних сервісів чи реєстрів може прискорити пошук, однак обмеження в бюджеті чи у відкритому доступі можуть вплинути на результат); 3) навичок аналітика (наліз і трактування знайдених даних потребують кваліфікованого спеціаліста, здатного відрізняти надійну інформацію від фейкової та синтезувати матеріали з різних джерел); 4) дотримання правових норм (важливо враховувати юридичні та етичні аспекти використання інформації з відкритих джерел)

Обмеженнями представлених методів можуть бути ситуації, коли:

- відсутня або закрита велика частина даних через конфіденційність та високі налаштування приватності користувачів;
- існують технічні бар'єри (географічні обмеження, специфіка мови пошуку тощо);
- дані швидко змінюються або видаляються (особливо в динамічному середовищі соціальних мереж).

Попри ці обмеження, розглянута модель циклу розвідки, технологічний ланцюжок процесу OSINT дослідження та метод міжоб'єктних зв'язків із практикою застосування запропонованого методу для об'єкта «особа» в залежності від вхідних даних демонструє вагому практичну цінність. І може бути корисними для державних структур, правоохоронних органів, журналістів-розслідувачів, приватних детективів чи експертів із безпеки, які проводять OSINT-аналіз. Наявність уніфікованої схеми та перелік конкретних джерел спрощує й стандартизує процес, що робить його зрозумілішим і прозорішим для всіх учасників.

Подальші напрями розвитку методу міжоб'єктних зв'язків можуть передбачати:

- автоматизацію пошукових завдань і побудови зв'язків (шляхом впровадження штучного інтелекту та машинного навчання);
- розширення джерельної бази включно з регіонально-специфічними платформами та ресурсами;
- створення інтелектуальних інформаційних панелей (дашбордів) для швидкої візуалізації пов'язаних даних, а також сповіщення про оновлення або можливі ризики.

Таким чином, результати проведеного аналізу підтверджують доцільність використання систематичного підходу до OSINT, що базується на моделі циклу розвідки та методі міжоб'єктних зв'язків. Запропонований метод покращує глибину і точність розслідування та може бути ефективно адаптований до різних сфер застосування – від криміналістики до корпоративної безпеки.

Висновки з даного дослідження
і перспективи подальшого розвитку у даному напрямі

У цій роботі вдалося підвищити результативність пошуку під час OSINT-розслідувань завдяки деталізації та об'єктному підходу до вдосконалення етапу збору даних за рахунок використання запропонованого методу міжоб'єктних зв'язків. Застосування методу міжоб'єктних зв'язків продемонстровано на прикладі об'єкта «особа» в залежності від доступних вхідних даних, що дає змогу гнучко визначати напрямки пошукових робіт та зменшує ризик пропуску важливої інформації.

Основні завдання, виконані в межах дослідження: 1) проведено детальний аналіз моделі циклу розвідки Гібсона; 2) розроблено й упроваджено розширений процес збору даних, що базується на методі міжоб'єктних зв'язків, для підвищення результативності пошуку та наочної демонстрації взаємодії між різними об'єктами розслідування; 3) спроєктовано детальну схему пошукових робіт для об'єкта типу «особа», яка дає змогу локалізувати напрямки пошуку й таким чином посилює ефективність OSINT-розслідування.

Наукова новизна дослідження полягає в удосконаленні відомої шестирівневої моделі циклу розвідки Гібсона за рахунок використання методу міжоб'єктних зв'язків під час збору даних. Це уможливлює:

- комплексне відстеження взаємодій між ключовими сутностями розслідування (особа, місце, організація, подія, дія, продукт/система);
- точніше визначення й логічну візуалізацію ланцюжків причиново-наслідкових зв'язків.

Практична цінність роботи полягає у можливості впровадження описаних методів та інструментів для вдосконалення OSINT-розслідувань, насамперед у сфері військової розвідки, але також і в правоохоронних органах, журналістських розслідуваннях чи корпоративній безпеці.

Результати дослідження можуть бути використані для:

- покращення існуючих методів та інструментів OSINT-розслідувань;
- підготовки фахівців у галузі OSINT;
- проведення розслідувань у різних сферах, що потребують оперативного аналізу великих обсягів відкритих даних.

Загалом, робота розширює методологічну базу виконання етапу збору даних у межах OSINT-розслідувань за допомогою:

- удосконаленого етапу збору даних, орієнтованого на зв'язки між об'єктами;
- розробленого методу міжоб'єктних зв'язків для об'єкта «особа» в залежності від наявних вхідних даних.

Отримані результати не лише сприяють підвищенню точності й швидкості пошукових робіт, а й можуть стати поштовхом для подальшого розвитку технологій автоматизації та аналітики в галузі OSINT, особливо важливих у військовій розвідці й суміжних сферах.

Література

1. Schaurer, F., & Störger, J. (2013). The evolution of open source intelligence (OSINT). Computers in Human Behavior, 19, 53–56.

2. Орел, О. В., & Мідіна, А. С. (2023). OSINT як ключ до нових можливостей у правовому полі під час війни. Актуальні питання використання методів і засобів OSINT у роботі підрозділів захисту національної державності, 1, 18–21. Retrieved from https://nasbu.edu.ua/uploads/p_57_61186644.pdf

3. Hwang, Y. W., Lee, I. Y., Kim, H., Lee, H., & Kim, D. (2022). Current status and security trend of OSINT. Wireless Communications and Mobile Computing, 2022. https://doi.org/10.1155/2022

4. Crosston, M., & Valli, F. (2017). An intelligence civil war: "HUMINT" vs. "TECHINT". Cyber, Intelligence, and Security, 1(1), 67–82.

5. Johnson, L. (2010). Evaluating "Humint": The role of foreign agents in US security. Comparative Strategy, 29(4), 308–332.

6. Яровой, Т. (2019). OSINT, як перспективний інструмент контролю за лобістською діяльністю в контексті державної безпеки. Expert: Paradigm of Law and Public Administration, 6(2019–4(6)), 201–208. Retrieved from https://doi.org/10.32689/2617-9660-2019-4(6)-201-208

7. Виходець, Ю. О., & Тетерятник, Г. К. (2022). Окремі питання використання OSINT при розслідуванні злочинів в умовах військової агресії рф. Правові новели, 70.

8. Мороз, А., & Поліщук, К. (2023). Роль сучасних технологій у системі протидії засобам застосування ІПСО рф в широкомасштабній війні проти України. Scientific Collection «InterConf», 152, 594–602.

9. Korobeinikova T., Zhuravel I., Bodak A., & Borodenko, D. (2024). Концепція нульової довіри: сучасні методи забезпечення кібербезпеки в корпоративних мережах. Вісник Львівського державного університету безпеки життєдіяльності, 30, 67-77. Retrieved із https://journal.ldubgd.edu.ua/index.php/Visnuk/article/view/2769

10. Калугін, В. Ю. (2023). Основні методи OSINT, що використовуються в кримінальному аналізі (Doctoral dissertation, Одеський державний університет внутрішніх справ).

11. Bellingcat. (n.d.). Official website. Retrieved from https://uk.bellingcat.com/

12. The Atlantic Council's Digital Forensic Research Lab (DFRLab). (n.d.). Official website. Retrieved from https://www.atlanticcouncil.org/programs/digital-forensic-research-lab/

13. The Citizen Lab. (n.d.). Official website. Retrieved from https://citizenlab.ca/

14. Forensic Architecture. (n.d.). Official website. Retrieved from https://forensic-architecture.org/

15. Trace Labs. (n.d.). Official website. Retrieved from https://www.tracelabs.org/

16. InformNapalm. (n.d.). Official website. Retrieved from https://informnapalm.org/ua/

17. Bellingcat Ukraine. (n.d.). Official website. Retrieved from https://uk.bellingcat.com/tag/ukraine-en/

18. Molfar. (n.d.). Official website. Retrieved from https://molfar.com/

19. DOU.ua. (2023). «Цивільне населення завжди брало участь у війнах: хтось працює в тилу, хтось проводить диверсії». Інтерв'ю з учасником «Кіберальянсу» про хакерів на війні та сумнівні правила «Червоного хреста». Retrieved from https://dou.ua/lenta/interviews/ukrainian-cyber-alliance-at-full-scale-war-2023/

20. Bihus.Info. (n.d.). Official website. Retrieved from https://bihus.info/

21. Office of the Director of National Intelligence (ODNI). (2011). U.S. National Intelligence – An Overview 2011. Retrieved from https://www.dni.gov/files/documents/IC_Consumers_Guide_2011.pdf

22. Bayerl, P., Sampson, F., & Akhgar, B. (2017). Open Source Intelligence Investigation: From Strategy to Implementation. Springer International Publishing AG.

23. Hassan, N. A., & Hijazi, R. (2018). The evolution of open source intelligence. In Open Source Intelligence Methods and Tools (pp. 1–20). Berkeley, CA: Apress. https://doi.org/10.1007/978-1-4842-3213-2_1

24. Bazzell, M. (2016). Open source intelligence techniques: Resources for searching and analyzing online information (5th ed.). Self-published.

25. Pastor-Galindo, J., et al. (2020). The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. IEEE Access, 8, 10282–10304. https://doi.org/10.1109/ACCESS.2020.2965257

26. Tabatabei, F., & Wells, D. (2016). In B. Akhgar, P. S. Bayerl, & F. Sampson (Eds.), Open Source Intelligence Investigation: From Strategy to Implementation (pp. 213–231). Springer..

References

1. Schaurer, F., & Störger, J. (2013). The evolution of open source intelligence (OSINT). Computers in Human Behavior, 19, 53–56.

2. Orel, O. V., & Midina, A. S. (2023). OSINT yak kliuch do novykh mozhlyvostei u pravovomu poli pid chas viiny. Aktualni pytannia vykorystannia metodiv i zasobiv OSINT u roboti pidrozdiliv zakhystu natsionalnoi derzhavnosti, 1, 18–21. Retrieved from <https://nasbu.edu.ua/uploads/p_57_61186644.pdf>

3. Hwang, Y. W., Lee, I. Y., Kim, H., Lee, H., & Kim, D. (2022). Current status and security trend of OSINT. Wireless Communications and Mobile Computing, 2022. <https://doi.org/10.1155/2022>

4. Crosston, M., & Valli, F. (2017). An intelligence civil war: "HUMINT" vs. "TECHINT". Cyber, Intelligence, and Security, 1(1), 67–82.

5. Johnson, L. (2010). Evaluating "Humint": The role of foreign agents in US security. Comparative Strategy, 29(4), 308–332.

6. Yarovoi, T. (2019). OSINT, yak perspektyvnyi instrument kontroliu za lobistskoiu diialnistiu v konteksti derzhavnoi bezpeky. Expert: Paradigm of Law and Public Administration, 6(2019–4(6)), 201–208. Retrieved from <https://doi.org/10.32689/2617-9660-2019-4(6)-201-208>

7. Vykhodets, Yu. O., & Teteriatnyk, H. K. (2022). Okremi pytannia vykorystannia OSINT pry rozsliduvanni zlochyniv v umovakh viiskovoi ahresii rf. Pravovi novely, 70.

8. Moroz, A., & Polishchuk, K. (2023). Rol suchasnykh tekhnolohii u systemi protydii zasobam zastosuvannia IPSO rf v shyrokomasshtabnii viini proty Ukrainy. Scientific Collection «InterConf», 152, 594–602.

9. Korobeinikova, T., Zhuravel, I., Bodak, A., & Borodenko, D. (2024). Kontseptsiia nuliovoi doviry: suchasni metody zabezpechennia kiberbezpeky v korporatyvnykh merezhakh. Visnyk Lvivskoho derzhavnoho universytetu bezpeky zhyttiediialnosti, 30, 67–77. Retrieved from <https://journal.ldubgd.edu.ua/index.php/Visnuk/article/view/2769>

10. Kaluhin, V. Yu. (2023). Osnovni metody OSINT, shcho vykorystovuiutsia v kryminalnomu analizi (Doctoral dissertation, Odeskyi derzhavnyi universytet vnutrishnikh sprav).

11. Bellingcat. (n.d.). Official website. Retrieved from <https://uk.bellingcat.com/>

12. The Atlantic Council's Digital Forensic Research Lab (DFRLab). (n.d.). Official website. Retrieved from <https://www.atlanticcouncil.org/programs/digital-forensic-research-lab/>

13. The Citizen Lab. (n.d.). Official website. Retrieved from <https://citizenlab.ca/>

14. Forensic Architecture. (n.d.). Official website. Retrieved from <https://forensic-architecture.org/>

15. Trace Labs. (n.d.). Official website. Retrieved from <https://www.tracelabs.org/>

16. InformNapalm. (n.d.). Official website. Retrieved from <https://informnapalm.org/ua/>

17. Bellingcat Ukraine. (n.d.). Official website. Retrieved from <https://uk.bellingcat.com/tag/ukraine-en/>

18. Molfar. (n.d.). Official website. Retrieved from <https://molfar.com/>

19. DOU.ua. (2023). «Tsyvilne naselennia zavzhdy bralo uchast u viinakh: khtos pratsiuie v tylu, khtos provodyt dyversii». Interv'iu z uchasnykom «Kiberaliancy» pro khakeriv na viini ta sumnivni pravyla «Chervonoho khresta». Retrieved from <https://dou.ua/lenta/interviews/ukrainian-cyber-alliance-at-full-scale-war-2023/>

20. Bihus.Info. (n.d.). Official website. Retrieved from <https://bihus.info/>

21. Office of the Director of National Intelligence (ODNI). (2011). U.S. National Intelligence – An Overview 2011. Retrieved from <https://www.dni.gov/files/documents/IC_Consumers_Guide_2011.pdf>

22. Bayerl, P., Sampson, F., & Akhgar, B. (2017). Open Source Intelligence Investigation: From Strategy to Implementation. Springer International Publishing AG.

23. Hassan, N. A., & Hijazi, R. (2018). The evolution of open source intelligence. In Open Source Intelligence Methods and Tools (pp. 1–20). Berkeley, CA: Apress. <https://doi.org/10.1007/978-1-4842-3213-2_1>

24. Bazzell, M. (2016). Open source intelligence techniques: Resources for searching and analyzing online information (5th ed.). Self-published.

25. Pastor-Galindo, J., et al. (2020). The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. IEEE Access, 8, 10282–10304. <https://doi.org/10.1109/ACCESS.2020.2965257>

26. Tabatabei, F., & Wells, D. (2016). In B. Akhgar, P. S. Bayerl, & F. Sampson (Eds.), Open Source Intelligence Investigation: From Strategy to Implementation (pp. 213–231). Springer.

27. Prevent SQL Injection Attack. *Journal of Karary University for Engineering and Science*. DOI:10.54388/jkues.v2i1.141