Харківський національний університет імені В.Н. Каразіна
Навчально-науковий інститут комп'ютерних наук та штучного інтелекту
Кафедра кібербезпеки інформаційних систем, мереж і технологій

«Допущено до захисту»
В. о. зав.кафедрою КІСМТ
_____ Марина ЄСІНА
« » червня 2025 р.

Пояснювальна записка

до кваліфікаційної роботи бакалавра
спеціальність: 125 Кібербезпека
на тему: «Дослідження та аналіз застосування методів і механізмів OSINT для забезпечення кібербезпеки інформаційно-комунікаційних систем під час військових конфліктів»

Оцінка « »

Голова ЕК

Мичуда Л. З._____

Керівник к.т.н., доцент Єсіна М. В.
(прізвище та ініціали/підпис)

Рецензент к.т.н., професор Качко О. Г.
(прізвище та ініціали/підпис)

Виконавець: студентка групи КБ-41

Крижановська А. І._____
(прізвище та ініціали/підпис)

Харків – 2025

РЕФЕРАТ

Пояснювальна записка містить 60 сторінок, 74 джерел, 3 додатка.

Мета роботи: дослідження методів і механізмів OSINT для забезпечення кібербезпеки інформаційно-комунікаційних систем в умовах військових конфліктів, аналіз ключових аспектів застосування OSINT, ефективності існуючих методів та надання рекомендацій щодо їх оптимального використання.

Методи дослідження: аналіз наукової літератури, онлайн-джерел, досвіду аналітиків використання OSINT, порівняльний аналіз методів та інструментів OSINT.

Результати та новизна: систематизовано методи OSINT для кібербезпеки та військової розвідки; виявлено ключові переваги та обмеження різних інструментів; проаналізовано роль OSINT у протидії противнику, дезінформації та документуванні воєнних злочинів; запропоновано рекомендації щодо інтеграції OSINT у стратегії безпеки.

Рекомендації щодо використання результатів: застосування комбінації пасивних і активних методів OSINT; системна перевірка цифрового сліду організацій; використанні OSINT для контррозвідки; використання автоматизації для обробки великих обсягів даних; впровадження OSINT у системи кібербезпеки організацій; розвиток міжнародної співпраці для боротьби з кіберзагрозами.

Значущість роботи: дослідження доводить критичну роль OSINT у сучасних конфліктах та цифрових загрозах, пропонує практичні рішення для його використання та вказує на необхідність подальшого розвитку цієї галузі.

Напрямки подальших досліджень: вдосконалення методів аналізу даних за допомогою ШІ; розробка стандартів етичного використання OSINT; адаптація OSINT-інструментів до нових технологій (ШІ, квантові обчислення).

Ключові слова: OSINT, КІБЕРБЕЗПЕКА, ВІДКРИТІ ДЖЕРЕЛА, ВІЙСЬКОВІ КОНФЛІКТИ, РОЗВІДКА, ДЕЗІНФОРМАЦІЯ, ІНФОРМАЦІЙНА ВІЙНА, КРАУДСОРСИНГ, ВОЄННІ ЗЛОЧИНИ, ІКС.

ABSTRACT

The explanatory note contains 60 pages, 74 sources, 3 appendix.

Purpose: to study the methods and mechanisms of OSINT to ensure cybersecurity of information and communication systems in military conflicts, to analyze the key aspects of OSINT application, the effectiveness of existing methods and to provide recommendations for their optimal use.

Research methods: analysis of scientific literature, online sources, analysts' experience in using OSINT, comparative analysis of OSINT methods and tools.

Results and novelty: OSINT methods for cybersecurity and military intelligence are systematized; key advantages and limitations of various tools are identified; the role of OSINT in countering the enemy, disinformation and documenting war crimes is analyzed; recommendations for integrating OSINT into security strategies are proposed.

Recommendations for the use of the results: application of a combination of passive and active OSINT methods; systematic verification of the digital footprint of organizations; use of OSINT for counterintelligence; use of automation for processing large amounts of data; implementation of OSINT in cybersecurity systems of organizations; development of international cooperation to combat cyber threats.

Significance of the work: the study proves the critical role of OSINT in modern conflicts and digital threats, offers practical solutions for its use, and indicates the need for further development of this field.

Areas for further research: improving methods of data analysis using AI; developing standards for the ethical use of OSINT; adapting OSINT tools to new technologies (AI, quantum computing).

Keywords: OSINT, CYBERSECURITY, OPEN SOURCES, MILITARY CONFLICTS, INTELLIGENCE, DISINFORMATION, INFORMATION WARFARE, CROWDSOURCING, WAR CRIMES, CIS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ ТА СИМВОЛІВ

API	– Application Programming Interface
CIDR	– Classless Inter-Domain Routing
CLI	– Command-Line Interface
COMINT	– Communications Intelligence
CYBINT / CYINT	– Cyber Intelligence
DNS	– Domain Name System
FININT	– Financial Intelligence
GEOINT	– Geospatial Intelligence
GPS	– Global Positioning System
GUI	– Graphical User Interface
HUMINT	– Human Intelligence
IoT	– Internet of Things
IP	– Internet Protocol
MASINT	– Measurement and Signature Intelligence
NASA FIRMS	– The National Aeronautics and Space Administration The Fire Information for Resource Management System
OSINT	– Open Source Intelligence
SIGINT	– Signals Intelligence
T4p	– Tribunal for putin
TECHINT	– Technical Intelligence
URL	– Uniform Resource Locator
ЄС	– Європейський Союз

ЗМІ	– Засоби Масової Інформації
ІДІЛ	– Ісламська Держава Іраку та Леванту
ІКС	– Інформаційно-Комунікаційні Системи
ОРДЛО	– Окремі райони Донецької і Луганської Областей
ПЗ	– Програмне Забезпечення
США	– Сполучені Штати Америки
ШІ	– Штучний Інтелект

ВСТУП

Сучасний світ стрімко розвивається під впливом різних інформаційно-комунікаційних технологій, що проникають у всі сфери життєдіяльності людини. Швидкі темпи збільшення активних користувачів Інтернету, зростання цифрової взаємодії, поширення соціальних медіа, розвиток глобальних мереж водночас спричиняють появу нових викликів у сфері кібербезпеки. Особливо гостро ця проблема постає в умовах політичних, економічних криз та військових конфліктів, коли інформаційна війна відіграє вирішальну роль у формуванні суспільної думки, координації військових операцій та захисті критичної інфраструктури. У цьому контексті використання методів OSINT набувають надважливого значення.

На відміну від звичайного збору розвідувальної інформації, що залежить від таємної діяльності, Open Source Intelligence стосується процесу збору, аналізу та обробки інформації з відкритих джерел, тобто загальнодоступної інформації. Технологія часто асоціюється з національною безпекою та розвідувальними операціями, її роль у кібербезпеці є водночас критичною та все більш поширеною. Завдяки отриманому аналізу, фахівці можуть своєчасно виявляти загрози для функціонування інформаційно-комунікаційних систем (ІКС), прогнозувати можливі інциденти та ефективно реагувати на них. Також слід зазначити, що OSINT-технології знаходять широке застосування і у журналістських розслідуваннях та перевірці фактів щодо корупції, шахрайських схем та іншого, що також впливає як на суспільство держави, так і на нацбезпеку.

Використання OSINT у сфері кібербезпеки відкриває можливості для моніторингу діяльності зловмисників, виявлення вразливостей у ІКС та протидії інформаційним атакам. У військових умовах OSINT є не лише засобом розвідки, а й потужним інструментом стратегічного аналізу, що сприяє оперативному плануванню та ухваленню рішень, і внаслідок цього – зміцненню національної безпеки.

Тож метою цієї дипломної роботи є дослідження методів і механізмів OSINT для забезпечення кібербезпеки інформаційно-комунікаційних систем в

умовах військових конфліктів. У межах дослідження будуть розглянуті ключові аспекти застосування OSINT, оцінено ефективність існуючих методів і надано рекомендації щодо їх оптимального використання.

Основні завдання дипломної роботи:

1. Огляд, аналіз та досвід застосування технології OSINT та її роль у забезпеченні кібербезпеки.
2. Дослідження та аналіз методів та механізмів OSINT у забезпеченні кібербезпеки.
3. Дослідження та аналіз особливостей використання OSINT у військових конфліктах.
4. Порівняння існуючих методів OSINT та їх ефективності. Рекомендації із застосування та висновки.

1 ОГЛЯД, АНАЛІЗ ТА ДОСВІД ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ OSINT ТА ЇЇ РОЛЬ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ

1.1 Основні поняття технології OSINT

Для розвідувальної діяльності використовується велика кількість спеціальних засобів та методів, що включають в себе:

- HUMINT (Human Intelligence), що базується на зборі даних через людські джерела;
- SIGINT (Signals Intelligence), що використовує перехоплення електронних сигналів;
- MASINT (Measurement and Signature Intelligence), що фокусується на зборі масиву сигнатур фіксованих або динамічних цільових джерел, таких як радіаційне випромінювання, акустичні сигнали, оптичні дані;
- GEOINT (Geospatial Intelligence), що базується на використанні географічних даних і супутникових знімків для збору розвідувальної інформації про фізичні об'єкти та зміни на місцевості;
- FININT (Financial Intelligence), що збирає дані з фінансових транзакцій для виявлення підозрілих або незаконних операцій;
- TECHINT (Technical Intelligence), що зосереджено на зборі розвідки про технічні засоби, як-от зброя і техніка [1];
- CYBINT / CYINT (Cyber Intelligence), що зосереджується на зборі інформації, пов’язаної із загрозами та операціями в кіберпросторі. Це включає в себе аналіз мережевих даних, зловмисних дій і кібератак;
- COMINT (Communications Intelligence), що стосується перехоплення й аналізу комунікацій між окремими особами чи групами, таких як телефонні дзвінки, електронні листи, радіоповідомлення тощо. Це підкатегорія SIGINT (розвідка сигналів), але зосереджена виключно на людському спілкуванні [2].

Ці засоби та методи збору розвідданих взаємодіють між собою і дають можливість отримувати точнішу інформацію для аналізу ситуацій і прийняття обґрунтованих рішень. В наш час особливу увагу приділяють новим

можливостям, що відкривають доступ до публічних даних. Цей метод, відомий як OSINT, який відіграє важливу роль у сучасній розвідці.

Розвідка з відкритих джерел (OSINT) – це процес збору та аналізу інформації з публічно доступних джерел для створення аналітичних висновків. Дана розвідка відіграє ключову роль у сфері національної безпеки, діяльності правоохоронних органів, бізнес-розвідці та журналістиці [3]. Аналіз та інтерпретація даних означає виявлення зв'язків і закономірностей, які призводять до дієвих висновків, незалежно від того, чи це компанія, яка проводить дослідження ринку для ребрендингу, чи правоохоронний орган, який виявляє потенційні загрози безпеці, чи аналітик, який досліджує політичного кандидата. Оскільки OSINT покладається на загальнодоступну інформацію, то її можна зібрати швидко, дозволяючи користувачам бути в курсі поточних подій та інших ситуацій, що розвиваються. Тим часом для збору та перевірки інших форм розвідки можуть знадобитися дні або навіть тижні, і на той час інформація може бути застарілою та марною [4]. Таким чином, ефективність OSINT значною мірою залежить від джерел, з яких отримується інформація. Умовно ці джерела можна поділити на шість основних категорій інформаційних потоків, кожна з яких відіграє свою роль у процесі збору та аналізу даних:

- Засоби масової інформації: друковані газети, журнали, радіо та телебачення з усіх країн і між ними.
- Інтернет: онлайн-публікації, блоги, дискусійні групи, громадські ЗМІ (відео з мобільного телефону та створений користувачами вміст), YouTube та інші веб-сайти соцмедіа (Facebook, Twitter, Instagram тощо). Це джерело також випереджає ряд інших джерел завдяки своїй своєчасності та простоті доступу.
- Дані державного управління: звіти державного уряду, бюджети, слухання, телефонні довідники, прес-конференції та виступи. Хоч це джерело є офіційним, воно є загальнодоступним і може використовуватися вільно.
- Професійні та наукові публікації: інформація, отримана з журналів, конференцій, симпозіумів, наукових статей, дисертацій та тез.

- Комерційні дані: комерційні зображення, фінансові та промислові оцінки та бази даних.
- Сіра література: технічні звіти, препринти, патенти, робочі документи, ділові документи, неопубліковані роботи та інформаційні бюлетені [3].

Однак самих джерел інформації недостатньо – важливим є і сам процес збору, аналізу та перевірки отриманих даних. Для кращого розуміння варто розглянути, як саме працює розвідка з відкритих джерел і які етапи вона включає. Незалежно від того, чи OSINT використовують команди з кібербезпеки, правоохоронні органи чи небезпечні особи, для розслідування зазвичай використовують п’ять таких кроків (рис. А.1).

Планування та постановка завдань означає, що перш ніж збирати будь-яку інформацію, важливо визначити мету та обсяг розслідування. Цей крок допомагає переконатися, що зусилля залишаються цілеспрямованими та етичними, водночас мінімізуючи ризики, такі як розкриття особи слідчого. Застосування цього кроку: фінансова установа, яка проводить перевірку потенційного постачальника, визначила б свою мету як оцінку надійності постачальника через аналіз публічних записів та минулої історії порушень.

На етапі збору даних слідчий збирає загальнодоступні дані з різних OSINT-джерел, що були згадані вище, з пошукових систем, платформ соціальних мереж і т. д. Застосування цього кроку: дослідник кібербезпеки, який розслідує фішингову кампанію, може збирати деталі реєстрації домену з баз даних WHOIS, сканувати загальнодоступні сховища коду на наявність шкідливих сценаріїв і аналізувати профілі соціальних мереж на пошук підказок про зловмисників.

Обробка та організація даних, важливі, бо необроблені дані часто неструктуровані та великі. Слідчі використовують інструменти OSINT для структурування зібраних даних, усунення надмірностей і перевірки автентичності. Застосування цього кроку: групи безпеки, які відстежують сукупність програм-вимагачів, можуть обробляти тисячі журналів чату з форумів Darknet, класифікуючи згадки про конкретні класи зловмисного програмного забезпечення (ПЗ), вимоги щодо оплати та методи атак.

На етапі аналізу та кореляції даних, дослідник виявляє зв’язки, розкриває закономірності, визначає релевантність зібраних розвідувальних даних. Цей крок допомагає перетворити необроблену інформацію на корисну. Точність має вирішальне значення: неправильно витлумачені або неповні дані можуть призвести до хибних висновків, тому OSINT-результати слід перевіряти за кількома джерелами. Застосування цього кроку: аналітик з кібербезпеки, який досліджує поверхню атаки на компанію, може співвіднести витік облікових даних від минулого зламу з активними обліковими записами користувачів, знайденими під час сканування OSINT, визначаючи потенційні точки входу.

Останнім кроком є звітування та розповсюдження, що передбачає зведення результатів у структурований звіт і представлення його зацікавленим сторонам, чи то групам безпеки, чи то керівникам або правоохоронним органам. Звіт має містити детальну інформацію, докази, оцінку ризиків і рекомендовані дії. Він може бути підсумком оцінки ризику, розвідувальним брифінгом або звітом про технічні загрози, залежно від аудиторії та цілей. Застосування цього кроку: команда корпоративної безпеки, яка оцінює ціль M&A (Mergers and Acquisitions), може надати звіт із висвітленням минулих інцидентів безпеки, ризиків третіх сторін і потенційних порушень відповідності, допомагаючи керівникам приймати обґрунтовані рішення [5].

1.2 Історія розвитку OSINT

На даний момент найцінніший ресурс у світі, який створюється щоденно – дані і саме їхнє ефективне збирання, аналіз і використання є важливим інструментом у різних сферах діяльності. Проте концепція збору інформації з відкритих джерел має глибоке історичне коріння.

Використання OSINT було задокументовано в середині 19 століття в Сполучених Штатах, де відбувалася Громадянська війна (1861-1865 рр.) і опубліковані подробиці про чисельність військ, положення, моральний стан, легко використовували як оперативну розвідку обидві сторони, що шукали стратегічну інформацію у формі загальної філософії, кінцевої мети та запланованих проміжних кроків. У 1863 році було створено Бюро військової

пропаганди Великобританії, яке систематично використовувало інформацію з преси і у 1864 році проводило майже щоденні брифінги щодо змісту провідної преси Конфедерації, які все частіше використовували під час прийняття рішень.

Німецька військова частина Секція IIIb була створена в 1889 році і у мирний час відповідала лише за збір інформації, тоді як аналіз був завданням інших департаментів Генерального штабу. Секція поширювала свої висновки кожні два тижні серед кількох вищих командувань німецької армії і черпала інформацію з іноземних газет. Зусилля військової частини мали заздалегідь визначені військові, політичні та економічні цілі, а записи, що збереглися, показують методичні підходи, такі як таємне придбання газет із Франції та використання широкого вибору газет із російської та Британської імперій. Таким чином, ці зусилля в Німеччині чітко відповідають визначенню OSINT [6].

У 1939 році була заснована Служба моніторингу військового часу BBC Monitoring і спеціалізувалась вона на моніторингу та аналізу іноземних радіопередач. Основною метою було збирати новини, пропаганду та військову інформацію з різних джерел, і надавати своєчасні та точні звіти британському уряду. Спеціальна команда лінгвістів, аналітиків і радіотехніків відстежувала та перекладала трансляції з усього світу, охоплюючи кілька мов і регіонів [7].

Більш офіційний OSINT у Сполучених Штатах бере свій початок із створення у 1941 році Служби моніторингу іноземного мовлення, тобто агентства, відповідального за моніторинг іноземного мовлення. Прикладом їхньої роботи стала кореляція змін цін на апельсини в Парижі з успішними бомбардуваннями залізничних мостів під час Другої світової війни. Після Другої світової війни OSINT поступово відіграє ключову роль у притягненні до відповідальності винних у міжнародних порушеннях. Наприклад, починаючи з 1945 року фотографія та кіно були критичними доказами під час Нюрнберзького процесу. У 1993–1994 роках документація з каналів новин, онлайн-форумів і супутникових зображень призвели до створення Міжнародних кримінальних трибуналів для колишньої Югославії та Руанди.

У липні 2004 року, після терактів 11 вересня, Комісія 11 вересня рекомендувала створити розвідувальне агентство з відкритим кодом. У березні 2005 року Комісія з розвідки Іраку рекомендувала створити директорат з відкритим кодом у Центральному розвідувальному управлінні. І у листопаді 2005 року директор національної розвідки оголосив про створення Центру відкритого коду, що створений для збору інформації, доступної з Інтернету, баз даних, преси, радіо, телебачення, і комерційних зображень [3].

Починаючи з 2000-х років, фотографії та відео з мобільних телефонів, інструменти географічної прив’язки, дрони та соціальні медіа збирали інформацію, важливу для гібридних інтернаціоналізованих трибуналів у конфліктах у Сьєрра-Леоне та Камбоджі у 2001 році та в Лівані у 2009 році. Нарешті, у березні 2011 року зображення зіткнень у провінції Дар’а, на півдні Сирії, змінилися все, породивши першу «цифрову війну у всіх на очах». Під час сирійського конфлікту OSINT відігравав ключову роль у коригуванні воєнних наративів, особливо щодо використання режимом Асада хімічної зброї [8]. З появою Інтернету та цифрових технологій обсяг доступних відкритих даних значно зріс, що розширило можливості їх застосування. Особливо це стало помітно під час «Зеленої революції» в Ірані у 2009 році, коли соціальні мережі та інші онлайн-платформи стали важливими джерелами реальної інформації. Громадяни використовували ці платформи для координації протестів та обміну інформацією, демонструючи силу OSINT у нову цифрову епоху [9].

Сьогодні OSINT є невід'ємною частиною діяльності не лише урядів, але й бізнесу, журналістики та кібербезпеки. Він використовується для виявлення загроз, аналізу ринків, розслідувань та багатьох інших цілей, підкреслюючи його універсальність та важливість у сучасному світі. Таким чином, історія OSINT демонструє його постійну адаптацію та зростаюче значення в умовах швидко змінюваного інформаційного середовища.

1.3 Використання OSINT в кібербезпеці

У контексті кібербезпеки OSINT найчастіше застосовується для збору публічних даних про компанію з відкритих джерел, причому до таких даних

відноситься не тільки електронна пошта співробітників, але й інформація про IP-адреси, DNS-імена, домени та субдомени, зареєстровані за компанією, відкриті порти та сервіси на них, публічні експлойти до знайдених сервісів, наявні механізми безпеки, факти компрометації поштових адрес, конфіденційні документи тощо.

Через вдосконалення методів злому зростає кількість кіберінцидентів, від яких страждають організації та окремі користувачі мережі Інтернет. Завдяки доступності послуг типу Ransomware-as-a-Service або Phishing-as-a-Service, які не вимагають володіння широкими технічними знаннями, зростає і кількість кіберпорушників, а доступність інструментів OSINT дозволяє їм довгий час накопичувати інформацію про ціль і планувати кібератаку, залишаючись непоміченими. Це створює загрозу для організацій, більшість з яких навіть не здогадується про значну кількість інформації про неї, доступну в мережі [10].

OSINT є інструментом, який може використовуватися як для захисту, так і для атак. В етичному хакерстві він допомагає спеціалістам з кібербезпеки ідентифікувати цифрові сліди та оцінювати вразливості під час тестування на проникнення в ІКС, аналізу загроз чи соціальної інженерії. Використовуючи загальнодоступні джерела, організації можуть виявляти критичні витоки інформації та запобігати можливим атакам. Водночас зловмисники також застосовують OSINT для збору даних про свою ціль, виявлення слабких місць та планування атак. Наприклад, зламані облікові дані відіграють важливу роль у відстеженні витоку даних організації та платформ, які використовують компанії. Соціальні мережі можуть стати потужним інструментом для зловмисників у зборі даних про співробітників цільової особи чи організації. Отримуючи інформацію, таку як електронна пошта, номер телефону, посада або зв’язки, вони можуть здійснювати цілеспрямовані фішингові та смішинг-атаки. Використовуючи підроблені посилання або оманливі повідомлення, атакуючі намагаються змусити жертву надати конфіденційні дані або отримати несанкціонований доступ до корпоративних систем.

Під час розвідки етичний хакер/фахівець із безпеки збирає інформацію про ціль, таку як домен, субдомен, особу, організацію та конфіденційну ідентифікаційну інформацію співробітника, взаємопов'язані пристрої, відкриті порти, ПЗ, загальнодоступні бізнес-записи, каталоги веб-сайтів та інші незахищені активи, а також витік інформації, наприклад, облікові дані співробітників, комерційні секрети/записи тощо в будь-яких попередніх порушеннях або доступні через Darknet для виявлення конфіденційних, незахищених даних, вразливих точок доступу та прогалин у безпеці для їх усунення.

Розвідка з відкритим кодом дозволяє легко збирати всю цю інформацію найшвидшим і найпростішим способом. Та ж розвідка допомагає робити цифрові сліди на цілі; залежно від підходу, він може бути активним або пасивним. Багато дослідників із безпеки зазвичай дотримуються пасивного процесу, оскільки він не дозволяє цілі знати про активність і не попереджає синю команду (blue team). Наприклад, під час оцінки соціальної інженерії фахівці з безпеки шукають деталі співробітників, такі як соціальні мережі та інші профілі, наприклад Trello, Dropbox, Outlook, щоб відстежувати їхню діяльність на предмет фішингу, смішинг-атак. Таким же чином розкриті та скомпрометовані облікові дані допомагають запускати різноманітні атаки на пароль, наприклад, перекидання облікових даних, атаки грубої сили тощо, щоб мати зловмисний доступ до систем, програм, серверів і т. д.

Подібним чином, у захисному підході, група з розвідки загроз організації або окремих осіб може відстежувати свої дані та секрети, використовуючи дані із відкритих джерел про те, чи були вони витоком або вразливістю. Якщо співробітники або будь-які інші конфіденційні облікові дані були зламані або розголошені під час будь-якої кібератаки чи витоку даних, вони можуть швидко скинути пароль і розгорнути елементи керування безпекою. Організації використовують методології OSINT для збору всієї загальнодоступної інформації для аналізу даних і проведення аналізу загроз. Використовуючи правильний підхід до OSINT, за умови правильної інтерпретації, організації можуть мати

контекстне розуміння відкритої та придатної для використання інформації, що допомагає проаналізувати шкоду та ризик атаки через дані [11].

У минулому кібербезпека була переважно реактивною, тобто фахівці з безпеки реагували на кібератаки лише після того, як вони відбувалися, часто коли вже було завдано значної шкоди. Хоча на початку це було нормою, деякі організації все ще покладаються на цей застарілий підхід, залишаючи себе вразливими до невиявлених вторгнень і атак, які можуть залишатися непоміченими протягом тривалого часу [12]. На даний час вже існує такий підхід як розвідка кіберзагроз (Threat Intelligence) суть якої полягає в отриманні розвідувальних даних із відкритих джерел, зокрема технічної інформації, яка дає змогу організаціям приймати рішення та покращувати свої оборонні можливості. Прикладом застосування OSINT в межах розвідки кіберзагроз є те, що на початку 2024 року, дослідивши характеристики скомпрометованого роутера (який український уряд пов’язав із діяльністю групи APT28) та відкриті технічні дані, аналітики змогли виявити тисячі інших вразливих маршрутизаторів із аналогічними ознаками злому [13]. Цей випадок демонструє, що зв’язок між OSINT і Threat Intelligence дозволяє не лише реагувати на поодинокі інциденти, але й розкривати ширші кампанії атакувальників, проактивно захищаючи інформаційно-комунікаційні системи.

1.4 Інформаційно-комунікаційна система та її роль у кібербезпеці

Відповідно до Закону України «Про захист інформації в інформаційно-комунікаційних системах», інформаційно-комунікаційна система (ІКС) – це сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле [14]. Тобто, ІКС об’єднує комп’ютерні системи, мережі зв’язку, канали передачі даних і ПЗ, що забезпечують збір, обробку і передачу інформації. Структурно ІКС включає в себе апаратні компоненти (сервери, маршрутизатори, термінали тощо), телекомунікаційну інфраструктуру (мережеві канали, супутниковий та радіозв’язок) і ПЗ, що гарантує функціонування мережі. Оскільки ІКС оперує над секретною та службовою інформацією, вона також передбачає заходи технічного та

криптографічного захисту, організаційні процедури доступу та моніторинг підозрілої активності.

У структурі Збройних Сил України (ЗСУ) ІКС відіграє центральну роль в організації управління та зв'язку. За визначенням Міністерства оборони, війська зв'язку та кібербезпеки відповідають за планування та забезпечення розгортання, функціонування систем зв'язку та інформаційних систем, систем бойового управління та оповіщення. Зокрема, вони надають послуги зв'язку для забезпечення функціонування єдиного інформаційного середовища Збройних Сил України [15]. Єдине інформаційне середовище означає взаємосумісну мережу, у межах якої команди від командирів поширюються до підлеглих через захищені канали, а зворотна інформація оперативно передається вгору. Як наголошується в офіційних військових документах, для успішного ведення бою необхідно використовувати «єдиний інформаційний простір», що складається з взаємосумісних систем, які забезпечують захищений обмін інформацією між підрозділами [16]. Завдяки цьому ІКС забезпечують інтеграцію даних з різних командних центрів, швидку передачу наказів і збір розвідувальної інформації, що є критичним у сучасних умовах війни та кризових ситуаціях.

В умовах повномасштабного збройного конфлікту інформаційно-комунікаційні системи стають одним із найпріоритетніших цілей противника. Основні загрози для ІКС – це кібератаки, спрямовані на викрадення, порушення доступності та цілісності інформації. Звіт Держспецзв'язку за 2024 рік констатує, що основною метою противника є викрадення чутливої інформації, а також знищення даних та інформаційних систем [17]. Зокрема, фахівці відзначають, що серед найефективніших інструментів кібершпигунства – фішинг та зараження пристроїв шкідливим ПЗ, оскільки найслабшою ланкою в цьому випадку є людина. Таким чином, через особисті облікові записи та корпоративні месенджери зловмисники надсилають відеозаписи, документи чи пропозиції «рекрутингу», що містять небезпечні вкладення. Крім того, ворог може націлюватися на енергетичну, транспортну та інші критичні інфраструктурні об'єкти, які пов'язані з ІКС (наприклад, операторів зв'язку) [17, 18]. Військові

ЗСУ підкреслюють, що обробка та захист інформації в ІКС є складовою критичної інфраструктури оборони. Тому забезпечення кібербезпеки ІКС є завданням першочергової важливості, адже від їхньої безперебійної роботи залежить оперативне управління військами та недопущення втрати стратегічної переваги. І саме в цьому випадку методи та інструменти OSINT можуть допомогти у вдосконаленні заходів безпеки та постійного моніторингу захищеності ІКС.

1.5 Практичні приклади використання OSINT

Враховуючи широкі можливості OSINT у виявленні загроз, аналізі кіберінцидентів та оцінці вразливостей, його ефективність підтверджується численними реальними випадками застосування. Від розслідувань кіберзлочинів та моніторингу даркнету до ідентифікації військових пересувань та виявлення дезінформації. Розглянемо деякі практичні приклади його використання, що ілюструють, як саме цей метод застосовується для отримання критично важливої інформації у різних сферах нашого життя.

Відстеження бойовиків ІДІЛ через соціальні мережі у 2015 році через їхній промах у соціальних мережах, призвів до виявлення одного з таємних тренувальних таборів у Сирії. Військові ІДІЛ ділилися фотографіями, відео в Інтернеті, демонструючи себе в уніформі з впізнаваними пам’ятками на задньому плані. Дописи мали на меті залякати та вербувати, але вони ненавмисно надали достатньо даних, щоб OSINT-розслідувач зміг їх знайти. OSINT-експерти використовували ці зображення для дослідження орієнтирів, рослинності і рельєфу, щоб звузити місцезнаходження до району в сирійській пустелі, поблизу м. Ракка. Процес передбачав накладання зображень у Google Earth та їх перехресне порівняння з іншими загальнодоступними супутниковими зображеннями. Тобто розслідувачі знаходили метадані зображень, геолокацію та перехресні посилання з профілями в соціальних мережах, що дало змогу ідентифікувати людей з того району, додатково підтверджуючи розташування табору. Інформація, яку було отримано, було передано розвідувальним службам для формування розуміння операцій ІДІЛ у Сирії [19].

Bellingcat та The Sunday Times ідентифікували Крістофера Кінехана-старшого, одного з лідерів організованого міжнародного наркокартелю, через його активність у Google Reviews (рис. А.2). Він залишав відгуки про ресторани та готелі під псевдонімом «Крістофер Вінсент», що допомогло дослідникам простежити його маршрути та встановити особу Кінехана шляхом співставлення метаданих, публічних записів та супутникових знімків. Використання однієї електронної пошти для бронювань і коментарів підтвердило зв’язок між його обліковим записом і реальними переміщеннями. OSINT-дослідники також порівняли зображення місць, які він відвідував, з його минулими поїздками, що підтвердило його перебування в Об’єднаних Арабських Еміратах, Туреччині та інших країнах. Це розслідування продемонструвало, як необережна цифрова активність може викрити навіть найбільш розшукуваних злочинців [20].

Стаття OSINT Industries описує, як дослідник Julian використовував OSINT для розслідування глобальної кризи, пов'язаної з фентанілом. Він виявив зв’язок між китайськими компаніями, які постачають прекурсори для наркотиків з представниками Комуністичної партії Китаю. Julian використовував Google Dorking, відкриті бізнес-записи та соціальні мережі, щоб виявити компанії, які рекламували речовини для виробництва фентанілу. Він знайшов оголошення про продаж хімікатів, співставив домени компаній з урядовими IP-адресами та ідентифікував осіб, які керують цими підприємствами. Розслідування показало, що такі компанії працюють під прикриттям законних фірм, використовуючи захищені домени, соцмережі та обхідні шляхи в реєстраційних документах [21].

Стаття «MH17: The Open Source Evidence» від Bellingcat представляє детальний аналіз відкритих джерел, які доводять, що рейс MH17 був збитий 17 липня 2014 року російським зенітно-ракетним комплексом «Бук», перевезеним з росії на підконтрольну бойовикам територію України. Завдяки аналізу знімків із соціальних мереж та журналістських розслідувань вдалося простежити його рух із території росії (курськ) на Донбас (Донецьк, Сніжне) (рис. А.3). Відео та фотографії з різних локацій уздовж маршруту підтверджували його переміщення, а порівняння особливих деталей (наприклад, унікальних відміток на корпусі)

дозволило довести, що це той самий комплекс 53-ї зенітно-ракетної бригади росії. Ключовим доказом став аналіз фотографій запуску ракети, що підтвердив здійснення пострілу із поля біля м. Сніжне, що узгоджується з супутниковими знімками та повідомленнями очевидців. Також було розшифровано перехоплені телефонні розмови, у яких бойовики обговорювали доставку та використання «Бука». Розслідування включало аналіз авіаційних уламків, траєкторії польоту ракети та балістичних характеристик вибуху. Всі докази вказували на те, що літак був збитий ракетою 9М38М1, запущеною саме з «Бука». У звіті Bellingcat демонструє, як відкриті джерела можуть бути використані для реконструкції складних подій, навіть якщо офіційні органи заперечують свою причетність. Докази, зібрані у ході OSINT-розслідування, стали важливими в судових процесах, зокрема в міжнародних трибуналах, що розглядали справу MH17 [22].

Інша стаття Bellingcat описує розслідування, яке зосереджено на анонімному торговці дикими тваринами, відомому як BK, що роками продає рідкісних і зникаючих тварин через соцмережі. Використовуючи OSINT-методи, включаючи аналіз рекламних постів, метаданих і клієнтських відео, дослідники Bellingcat змогли визначити, що BK працює з Малайзії та зв’язати його діяльність з міжнародною контрабандою екзотичних тварин. Для збору доказів, дослідники застосували методи геолокації, проаналізувавши відео покупців, що дозволило встановити, що один з них був знятий у Бангкоку (рис. А.4). Вони також знайшли зв'язок між різними обліковими записами BK, що дало більше інформації про його діяльність, хоча й не дозволило повністю розкрити його особу чи точне місце роботи. Це розслідування показує, як OSINT можна використовувати для викриття нелегальних угруповань, що займаються торгівлею дикими тваринами, і як Інтернет-платформи можуть стати важливим інструментом для злочинців, що залишаються непоміченими протягом довгого часу [23].

2 ДОСЛІДЖЕННЯ ТА АНАЛІЗ МЕТОДІВ ТА МЕХАНІЗМІВ OSINT У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ

2.1 Методи та методології, що використовуються в OSINT

Під час дослідження онлайн-простору кожен з нас неодмінно натрапляє на інформацію з відкритих джерел: дані, які є загальнодоступними для перегляду, збору та аналізу. Цей тип інформації є дуже корисним для онлайн-дослідників завдяки своїй доступності. Все, що потрібно зробити, – це ввести кілька слів у пошукову систему, щоб знайти мільйони ресурсів, що містять детальні відомості на потрібну тему.

Проте на деяких веб-сайтах і платформах доступ до даних з відкритим кодом може бути ускладнений. Хоча загалом Інтернет залишається доступним для користувачів, сучасні веб-ресурси та популярні соціальні медіа тепер вимагають реєстрації облікових записів для входу. У такому захищеному онлайн-середовищі аналітики та дослідники більше не можуть пасивно збирати всі дані OSINT. Натомість, вони змушені створювати облікові записи та обходити бар'єри доступу для отримання потрібної інформації. Це і є основною різницею між пасивним та активним методами збору інформації OSINT.

Пасивний і активний OSINT вимагають різних зусиль і рівня точності від онлайн-користувача. Якщо розглядати слово «пасивний», то можна уявити собі пасивного OSINT збирача, який просто спостерігає і поглинає інформацію в Інтернеті. Пасивно зібрані дані можуть включати заголовки новин або популярні пости на публічних сторінках у соціальних мережах. Під час пасивного OSINT дослідники часто намагаються не привертати до себе уваги, бажаючи залишитися невидимими для об'єктів дослідження, щоб уникнути потенційних наслідків. Протилежним до пасивного методу є активний метод збирання, що передбачає динамічний підхід до збору даних. Для активного OSINT дослідники зазвичай потребують облікових даних, таких як електронні адреси або імена користувачів, щоб мати можливість заходити на сайти з цінною інформацією [24]. Користувачі можуть заповнювати складніші запити, щоб зібрати, наприклад, незрозумілу

інформацію та метадані з баз даних та мережевої інфраструктури. Вони також можуть заповнити форму або заплатити, щоб отримати додаткову інформацію.

У деяких випадках активний OSINT може навіть передбачати звернення безпосередньо до джерел для отримання додаткової інформації, яка не є загальнодоступною чи видимою. Хоча активний OSINT, швидше за все, надасть користувачам детальну інформацію в режимі реального часу, ніж пасивний OSINT, це набагато складніше зробити таємно, і це може призвести до юридичних проблем, якщо методи збору даних не є обережними [25].

Під час OSINT-досліджень може використовуватись інша класифікація методів збору інформації, що можуть використовуватись з різною метою:

- Інтернет-дослідження: передбачає використання пошукових систем, інших онлайн-інструментів для пошуку інформації з статей новин, публікацій в наукових журналах, досліджень, урядових звітів і офіційних документів пов’язаних з певною темою. Крім того, Інтернет-дослідження включає пошук у різноманітних публічних базах даних, що містять корисну інформацію, таку як юридичні справи, фінансові звіти, звіти з корпоративних веб-сайтів і навіть старі публікації в архівах.
- Моніторинг соціальних медіа: може включати пошук за певними хештегами, ключовими словами або користувачами, моніторинг тенденцій, а також аналіз активності користувачів і взаємодії в Twitter, Facebook, Instagram, LinkedIn та інших. Моніторинг соцмедіа часто використовується для виявлення актуальних подій, вивчення громадської думки, виявлення впливових осіб у певних сферах або навіть для відслідковування ворожнечі чи дезінформації.
- Веб-збирання: використання спеціалізованих програмних інструментів (веб-скрейперів) для автоматизованого збору даних з різних веб-ресурсів. Процес збору даних полягає в автоматичному витягуванні потрібної інформації, наприклад, контактних даних, фінансових звітів, списків товарів або коментарів на форумах.
- Аналіз даних: для обробки можуть використовуватися інструменти статистичного аналізу, візуалізації даних та алгоритми машинного навчання для

передбачення та класифікації інформації. Алгоритми машинного навчання, можуть допомогти автоматизувати виявлення специфічних патернів у даних, що важко побачити вручну, і значно покращити точність прогнозів [26].

Для досягнення успішного збору та аналізу даних в OSINT важливо не лише правильно вибрати методи збору інформації, але й використовувати ефективні методології та підходи, які допомагають систематизувати процеси дослідження та отримання результатів:

- F3EAD (Find, Fix, Exploit, Analyze, Disseminate / Знайти, Зафіксувати, Використати, Проаналізувати, Поширити) – загальна мета полягає в тому, щоб надати структурований підхід для виявлення, фіксації, аналізу і поширення інформації щодо кіберзагроз. Цей цикл комбінує елементи операцій безпеки і розвідки кіберзагроз, забезпечуючи ефективну стратегію для реагування на кіберінциденти, щоб знизити їхній вплив на організацію [27].
- SWOT (Strengths, Weaknesses, Opportunities, Threats / Сильні, Слабкі сторони проєкту, Можливості та Загрози) – використовується для виявлення та оцінки сильних і слабких сторін, можливостей і загроз, пов'язаних із кібербезпекою в організації. Метою є створення стратегічної рамки, яка допомагає пріоритизувати зусилля з пом’якшення ризиків, ефективно розподіляти ресурси та покращувати рівень безпеки. Визначаючи внутрішні сильні (надійна інфраструктура, кваліфікований персонал) та слабкі сторони (застаріла технологія, недостатнє навчання), можливості (новітні технології кібербезпеки) і загрози (шкідливе ПЗ, фішинг), організації можуть приймати рішення для зменшення ризиків і підготовки до потенційних кіберзагроз [28].
- PESTEL (Political, Economic, Social, Technological, Legal, Environmental / Політичні, Економічні, Соціальні, Технологічні, Правові, Екологічні фактори) – мета полягає в тому, щоб систематично оцінювати зовнішні фактори, які можуть впливати на організацію або середовище, в якому вона функціонує. Аналіз PESTEL допомагає аналітикам розвідки розуміти політичні, економічні, соціальні, технологічні, екологічні та правові впливи, що визначають ситуацію в конкретній сфері чи регіоні. Цей підхід дає можливість аналітикам отримати

всебічне розуміння ситуації, що дозволяє ефективно приймати стратегії та управлінські рішення, орієнтуючись на зміни в зовнішньому середовищі [29].

- Використання вже відомих дисциплін збору розвідданих HUMINT, FININT, GEOINT, COMINT, CYBINT та ін.

Комбінація цих та інших методологій дозволяє OSINT аналітикам ефективно збирати, аналізувати та використовувати інформацію, а також адаптуватися до швидко змінюваних умов сучасного інформаційного простору [30].

2.2 Найбільш популярні механізми для роботи із OSINT

Розвиток технологій та зростання обсягів доступної інформації в Інтернеті створюють нові можливості для збору та аналізу даних з відкритих джерел. Використання таких механізмів стало важливим інструментом у кібербезпеці, дозволяючи виявляти потенційні загрози, аналізувати інфраструктуру та моделювати атаки на ІКС маючи відкриті дані про неї. Розглянемо найбільш популярні механізми для роботи з OSINT, включаючи інструменти для збору даних, механізми аналізу та їх інтеграцію у системи кібербезпеки. Огляд цих інструментів дозволить краще зрозуміти їх роль у забезпеченні захисту інформаційних систем і виявленні нових кіберзагроз.

SpiderFoot – це система, що автоматизує процес збору та аналізу інформації для цілей OSINT, що можна використовувати в наступальних цілях (наприклад, у вправах червоної команди чи тесті на проникнення) для розвідки Вашої цілі або в захисних цілях для збору інформації про те, що Ви або Ваша організація могли залишити в просторі Інтернету. Інструмент надає безліч модулів для збору інформації, що націлена на отримання доменних/субдоменних та хостових імен, номерів телефонів, електронних адрес, CIDR, а також адрес криптовалют. Крім того, він інтегрується з популярними API, такими як Shodan, HaveIBeenPwned, GreyNoise та іншими. SpiderFoot має вбудований веб-сервер, що дозволяє користувачам працювати через зрозумілий веб-інтерфейс, або ж здійснювати сканування через командний рядок. Інструмент інтегрує різноманітні джерела даних і автоматизує процес розвідки, що робить його ефективним для збору

інформації про цільові системи та збереження результатів у вигляді графіків або звітів. Завдяки можливостям, які він надає, SpiderFoot є важливим інструментом для дослідників безпеки та спеціалістів з кібербезпеки, а також для людей, які займаються виявленням загроз в Інтернеті [31, 32].

Maltego – це ПЗ для збору інформації, яке використовується для автоматизації процесу пошуку зв’язків між різними даними в Інтернеті. Воно дозволяє аналізувати профілі в соціальних мережах, адреси електронної пошти, номери телефонів, домени, а також визначати геолокацію і особисті дані, що робить його незамінним інструментом для розслідувань у криміналістиці та кібербезпеці. Maltego будує графи, де кожен елемент є об'єктом (Entities), а зв’язки між ними – це Links, з використанням Transforms, що дістає та інтерпретує знайдену інформацію. Maltego доступний у кількох версіях, включаючи безкоштовну версію Maltego CE для навчальних цілей, а також комерційні версії, як Maltego Classic та Maltego XL, які надають розширену підтримку і більші графи для аналізу. Ці версії дозволяють працювати з великими масивами даних і використовувати платні Transforms для більш глибокого аналізу, таких як інтеграція з сервісами Shodan та DomainTools [33]. З його допомогою аналітики можуть виявити, чи перетинаються у соціальних мережах співробітники різних підрозділів (різних сторін конфліктів) або чи присутній суперечливий контент, що може свідчити про компрометацію Вашої ІКС.

Recon-ng – це інструмент з відкритим вихідним кодом, призначений для збору інформації за допомогою Open Source Intelligence. Recon-ng є потужним веб-розвідувальним інструментом, який надає командний інтерфейс, схожий на Metasploit, і включає безліч модулів для збору даних. Recon-ng дозволяє працювати з базами даних, інтерактивною довідкою, а також має можливості для збору інформації про веб-сайти та домени. Це робить інструмент зручним і ефективним для збору даних про ціль, а також для пошуку вразливостей у веб-застосунках і на сайтах. ПЗ підтримує модулі для пошуку субдоменів, зворотного пошуку IP-адрес, сканування портів, захоплення банерів, пошуку DNS, а також для роботи з гео-IP і WHOIS-записами. Крім того, Recon-ng може

використовуватися для сканування пристроїв через Shodan, а також для виявлення лазівок у коді веб-застосунків. Завдяки своїм можливостям, Recon-ng стає незамінним інструментом для пентестерів та фахівців з кібербезпеки для оцінки вразливостей та збору важливої інформації про цільові ресурси [34].

Shodan – це пошукова система, яка дозволяє знаходити різні типи пристроїв, підключених до Інтернету, таких як веб-камери, маршрутизатори, сервери та інші системи, використовуючи різноманітні фільтри. Вона збирає дані переважно з веб-серверів (HTTP, HTTPS), а також з таких протоколів як FTP, SSH, Telnet, IMAP, SMTP і RTSP, що дає можливість доступу до відеопотоків з веб-камер та інших типів пристроїв. Shodan було запущено в 2009 році Джоном Мазерлі з метою створити пошукову систему для пристроїв, підключених до Інтернету. Система дозволяє знайти пристрої на основі метаданих, таких як банери сервісів, що надають інформацію про ПЗ, параметри сервісів і навіть попереджувальні повідомлення. Shodan може бути використана для виявлення вразливих систем в Інтернеті, зокрема таких, як системи керування водними установками, енергетичні мережі, системи безпеки та відеоспостереження. Пошук через Shodan може допомогти дослідникам безпеки, фахівцям з кібербезпеки та правоохоронним органам ідентифікувати місця в мережах та пристроях, що підключені до Інтернету, що є елементами ІКС, які є невідомими для адміністраторів або піддавані атакам. Попри корисність, Shodan також може бути використана зловмисниками, що робить її важливим інструментом у боротьбі з кіберзлочинністю. Веб-сайт надає обмежену кількість результатів без облікового запису, і для отримання розширених можливостей користувачам необхідно створити обліковий запис або сплатити комісію [35].

Google Dorks – це потужний механізм збору інформації через використання спеціальних запитів до пошукової системи Google для знаходження чутливих або прихованих даних, які можуть бути не доступні за допомогою стандартного пошуку. В основі цього методу лежить використання різних операторів пошуку (наприклад, «filetype:», «intitle:», «inurl:», «site:») для того, щоб знаходити специфічні файли, конфігураційні документи, бази даних, або навіть

конфіденційні дані, що залишились доступними в Інтернеті через недосконалі налаштування безпеки. Це дає змогу виявляти вразливості в веб-застосунках, доступ до яких не був обмежений, і навіть знаходити Інтернет-ресурси, що містять приватні дані. Використання Google Dorks у контексті OSINT дозволяє спеціалістам з кібербезпеки, розвідникам, аналітикам і журналістам швидко знаходити важливу інформацію про цільові системи, відкриті бази даних, конфіденційні файли та інші потенційно небезпечні ресурси. Наприклад, завдяки Google Dorks можна виявити незахищені файли на сервері, відкриті бази даних, що містять чутливу інформацію, або ж визначити конфігурації сервісів, які можуть бути використані зловмисниками для атак. Це робить Google Dorks важливим інструментом у розслідуваннях та забезпеченні безпеки [36].

The Harvester – це інструмент для збору інформації OSINT, що спеціально розроблений для допомоги тестувальникам на проникнення на ранніх етапах тестування безпеки. Він дозволяє швидко знаходити адреси електронної пошти, субдомени, хости, порти, імена співробітників та банери, використовуючи відкриті джерела. Інструмент працює за допомогою пошукових систем і ресурсів, включаючи Google, Bing, LinkedIn, Exalead та інші, що дає змогу здійснювати точне і детальне сканування на наявність чутливої інформації. The Harvester простий у використанні і має інтегровані пасивні модулі для збору даних, наприклад, за допомогою Shodan для пошуку банерів на хостах, або Censys для сертифікатів та субдоменів. Інструмент підтримує активні модулі для брутфорс-сканування та створення знімків екрана знайдених субдоменів. Зокрема, він може бути корисним для пентестерів, розслідувачів, бо дає можливість ефективно ідентифікувати потенційні загрози та вразливості через аналіз публічних даних, які організації можуть випадково або свідомо оприлюднювати [37, 38].

OSINT Framework – це колекція інструментів з відкритим кодом, яка допомагає збирати інформацію з публічних джерел в Інтернеті. Структура фреймворку організована таким чином, щоб надавати чіткий, систематизований підхід до збору, аналізу та розслідування даних. Вона включає понад 150 інструментів, які охоплюють різноманітні методи збору інформації, зокрема,

пошук в соціальних мережах, геолокація, аналіз доменів і електронної пошти, а також інструменти для виявлення вразливостей в мережах і веб-застосунках. Важливою особливістю є те, що фреймворк підтримує етичний збір інформації, дотримуючись законодавчих обмежень і конфіденційності. OSINT Framework сприяє розвитку обізнаності про ситуацію, виявленню загроз і допомагає у прийнятті рішень в різних сферах, таких як кібербезпека, бізнес-стратегія та управління ризиками. Крім того, він забезпечує інтеграцію з іншими процесами розвідки, що дозволяє організаціям створювати цілісне розуміння ризиків і можливостей. Усе це дозволяє попереджувати атаки, тобто виявити наявні вразливості в ІКС або зміну поведінки систем задовго до того, як хакери спробують ними скористатися. Фреймворк постійно оновлюється, додаючи нові інструменти та методи, що допомагають адаптуватися до динамічного ландшафту розвідки з відкритим кодом. Це робить його незамінним ресурсом для фахівців, які використовують відкриті джерела для збору даних і прийняття обґрунтованих рішень [39].

BuiltWith – це механізм у сфері OSINT, який використовується для виявлення стеку технологій, що стоять за веб-сайтами, що дозволяє отримувати технічні деталі сайту, зокрема визначати, яку систему керування вмістом, фреймворки, плагіни та інші технології використовує веб-ресурс. Використовуючи пошукову систему BuiltWith, достатньо ввести доменне ім’я сайту, щоб отримати повний технологічний профіль, що включає віджети, плагіни та інші компоненти. BuiltWith є корисним інструментом для бізнес-аналізу, конкурентного дослідження та збору інформації про веб-сайти. Він також надає список бібліотек JavaScript і CSS, які використовуються на сайті, що дозволяє глибше зрозуміти його структуру. Цей інструмент особливо ефективний для неформальних досліджень і може бути корисним для підприємств, які хочуть вивчити внутрішню технологічну архітектуру конкурентів. Для посилення безпеки, BuiltWith можна комбінувати з інструментами для сканування вразливостей, такими як WPScan, що дозволяє виявляти поширені вразливості на веб-сайті і забезпечити його максимальний захист [40, 41].

Intelligence X – це перша у своєму роді служба архівування та пошукова система, яка зберігає не лише історичні версії веб-сторінок, але й цілі набори даних, що витікають, які іншим чином видаляються з Інтернету через неприйнятний характер вмісту або юридичні причини. Хоча це може здатися схожим на те, що робить Wayback Machine Internet Archive, Intelligence X має деякі суттєві відмінності, коли справа доходить до типу вмісту, на якому зосереджується служба [40]. Цільовими клієнтами є компанії будь-якого розміру та уряди. Intelligence X відрізняє себе від інших пошукових систем такими унікальними способами:

- Пошук працює за допомогою селекторів, тобто конкретних пошукових термінів, таких як адреси електронної пошти, домени, URL-адреси, IP-адреси, CIDR, адреси Bitcoin, геші IPFS тощо.
- Він шукає в таких місцях, як даркнет, платформи для обміну документами, дані WHOIS, публічні витоки даних тощо.
- Він зберігає архів історичних даних із результатами, подібно до того, як Wayback Machine з archive.org зберігає історичні копії веб-сайтів [42].

HavIbeenPwned – це один із основних інструментів для кожного дослідника безпеки. Він підтримує базу даних про витік паролів, електронних листів і номерів телефонів за останні кілька років. Останнім часом порушення безпеки відбуваються дуже часто, що вимагає від спеціалістів безпеки постійно бути пильними. HaveIbeenPwned може бути корисним, для перевірки, чи має обліковий запис публічний злом. Однією з привабливих функцій для організації є пошук домену, що сповіщатиме власників доменів щоразу, коли система знаходитиме дані, які зламуються щодо домену. Але, щоб скористатися цією функцією, потрібно спочатку підтвердити, що він є власником саме цього домену. Після цього HaveIbeenPwned надсилатиме автоматичні електронні листи кожного разу, коли система знаходитиме дані у зламаних [40].

2.3 Виклики та обмеження OSINT у кібербезпеці

Використання OSINT у кібербезпеці відкриває широкі можливості для збору розвідувальної інформації з відкритих джерел, однак цей процес

супроводжується низкою викликів та обмежень, що можуть знизити ефективність розвідки. Перш за все, існує проблема обробки великих обсягів даних, де важливо не лише зібрати, але й перевірити достовірність отриманої інформації, оскільки багато відкритих джерел можуть бути ненадійними або спотвореними. Крім того, існують юридичні та етичні бар'єри, пов'язані з приватністю і законністю збору інформації з публічних платформ, що може порушити права людини або суперечити регулюванням. Окрему увагу потребує обхід захисних механізмів на онлайн-платформах, що ускладнює збір даних і вимагає від аналітиків спеціальних інструментів анонімізації. Важливим є також психологічне навантаження, яке виникає в процесі аналізу великої кількості фрагментованих даних, що може призвести до інформаційного перевантаження і упередженості. Усі ці фактори необхідно враховувати, щоб OSINT був ефективним інструментом.

Проблема перевантаження даних через величезну кількість інформації, доступної через OSINT, може ускладнити фільтрацію потрібної інформації від шуму. Саме тут ефективна організація даних відіграє вирішальну роль, бо саме ефективне ведення нотаток і систематичне керування даними є важливими для вирішення цієї проблеми. Фільтрування шуму має вирішальне значення для визначення того, які дані є цінними, а які можуть бути дезінформацією чи бути суперечливими [43]. У результаті групи аналізу загроз можуть загрузнути в буденних і трудомістких завданнях, витрачаючи надто багато часу на ручний збір, перевірку, усунення дублікатів і стандартизацію даних у Google, каналах OpenStreetMap, Twitter, преміум-провайдерах, звітах тощо. Враховуючи, що більшість даних, з якими мають працювати аналітики, є неструктурованими даними, автоматизація є ключовою. Автоматизація також означає більш ефективну виробничу обробку інформації, а також швидке, надійне вирішення завдань, що мінімізує людські помилки та дозволяє аналітикам зосередитися на інтерпретації та звітності OSINT [44].

Однією з головних проблем OSINT-аналізу є забезпечення точності та надійності даних. Джерела OSINT часто є неперевіреними, тобто дані можуть

бути застарілими, неповними або вводити в оману. Це особливо проблематично, коли цифрові докази потрібні для правових або важливих процесів прийняття рішень, де цілісність даних має першорядне значення. Потенційні ризики неправдивих даних, включаючи неправильні висновки та упереджені звіти розвідки, підкреслюють важливість ретельної перевірки джерела OSINT. Для пом'якшення цих ризиків слід враховувати такі фактори, як авторитетність, точність, об'єктивність, своєчасність і релевантність, а також достовірність джерела та можливість перехресної перевірки інформації [43]. Диверсифікація джерел гарантує, що інформація з багатьох джерел, мов і точок зору оцінюється для отримання більш повного та точного розуміння будь-якої теми, події чи ситуації. Одним із найкращих способів забезпечити різноманітність джерел є збір із джерел різними мовами, але проблема полягає в тому, щоб швидко й ефективно перекладати ці джерела кількома мовами [44].

Доступ до інформації супроводжується значними етичними та правовими проблемами, зокрема щодо конфіденційності та обробки даних. На відміну від традиційних методів розвідки, OSINT спирається на відкрито доступні дані, які можуть розмити межі етичної відповідальності. Враховуючи свою залежність від загальнодоступних даних, OSINT працює в сірій зоні, де інформація, хоча й є легально доступною, все ще може бути етично чутливою. Наприклад, збір особистої інформації з соціальних медіа потенційно може порушити конфіденційність особи, навіть якщо технічно вміст є публічним. Також такі організації як міжнародна організація Wikileaks підкреслюють той факт, що початковий витік інформації може бути незаконним, але подальше її використання знаходиться у сірій етичній зоні. Крім того, у різних юрисдикціях діють різні правила використання даних, як-от Загальний регламент про захист даних (General Data Protection Regulation) у ЄС, спрямований на захист прав особи на конфіденційність. Ці складнощі роблять критично важливим для OSINT-практиків відповідальне проведення збору розвідувальних даних, балансуючи між своїми цілями та дотриманням етичних стандартів. Той факт, що дані доступні в Інтернеті, автоматично не виправдовує їх необмеженого

використання. Ця напруга піднімає важливі етичні питання щодо поваги до приватного життя людей, водночас користуючись перевагами OSINT. Спеціалісти розвідки повинні оцінювати кожен випадок окремо, враховуючи контекст даних і їх потенційний вплив на конфіденційність людей перед їх використанням. Застосування найкращих практик, у тому числі встановлення чіткої етичної основи, забезпечення оперативної безпеки і забезпечення прозорості, допомагає захистити як цілісність розвідувальної діяльності, так і права особи на конфіденційність [45].

Незважаючи на значні досягнення OSINT-інструментів, вони мають недоліки, бо багато з них покладаються на алгоритми збирання та аналізу даних, що можуть пропускати або неправильно інтерпретувати важливу інформацію через технічні обмеження. Наприклад, інструментам обробки мови може знадобитися допомога зі сленгом або діалектами, а ПЗ для розпізнавання зображень може неправильно аналізувати зображення низької якості. Крім того, певні дані, такі як платний вміст, зашифровані повідомлення або дані, що зберігаються в приватних мережах, можуть залишатися недоступними для інструментів OSINT. Крім того, використання сторонніх онлайн-інструментів і застосунків створює додаткові ризики. Ці інструменти можуть зберігати дані віддалено, що викликає занепокоєння щодо безпеки та конфіденційності даних [43].

У результаті, хоча OSINT має величезний потенціал для забезпечення кібербезпеки, його використання супроводжується численними викликами, зокрема через проблему обробки великих обсягів даних, перевірку їх достовірності та юридичні та етичні питання. Важливість ретельної перевірки джерел і даних є ключовою для уникнення помилкових висновків і забезпечення точності отриманих розвідувальних відомостей. Оскільки багато інструментів покладаються на алгоритми, що можуть бути обмежені технічними або етичними факторами, важливо розвивати найкращі практики та стратегії для мінімізації цих ризиків та забезпечення надійності в OSINT.

3 ДОСЛІДЖЕННЯ ТА АНАЛІЗ ОСОБЛИВОСТЕЙ ВИКОРИСТАННЯ OSINT У ВІЙСЬКОВИХ КОНФЛІКТАХ

У цей час, коли інформаційна війна стала невід'ємною частиною збройних протистоянь, здатність швидко і точно збирати та аналізувати дані з відкритих джерел стає критично важливою для успіху військових операцій і національної безпеки. У цьому розділі буде розглянуто роль OSINT в моніторингу ситуації на полі бою, виявленні військових злочинів, боротьбі з дезінформацією, а також у використанні його для стратегії та тактики в умовах військових конфліктів.

3.1 OSINT для ситуаційної обізнаності на полі бою

Ситуаційна обізнаність передбачає ідентифікацію, візуалізацію, контекстуалізацію та розуміння ключової інформації в конкретному фізичному середовищі. У сфері безпеки та розвідувальних операцій розуміння динаміки ситуації створює основу для прийняття ефективних рішень, часто спрямованих на мінімізацію шкоди та руйнувань [46].

Ситуаційну обізнаність було визнано критично важливою для успішного ухвалення рішень у широкому спектрі ситуацій, багато з яких пов'язані із захистом людського життя та майна, включаючи правоохоронні органи, авіацію, управління повітряним рухом, навігацію суден, охорону здоров'я, реагування на надзвичайні ситуації, військове командування та управління операціями, оператори систем передачі, самооборона та управління морськими нафтовими та атомними електростанціями [47]. Завдяки впровадженню передових технологій, таких як супутниковий Інтернет, точна навігація, канали даних у реальному часі, що обробляються OSINT, інтегруються в ІКС і системи управління боєм, створюючи єдину картину бойових дій.

Інтеграція OSINT з ІКС дозволяє отримувати дані в реальному часі з соціальних мереж, супутників та сенсорів, GPS-трекерів, автоматизуючи їх аналіз для прийняття рішень. Наприклад, на початку 2023 року була запроваджена система Delta в Силах оборони, що розроблена за стандартами НАТО, що агрегує OSINT-дані у цифрові карти бою. У цю ІКС був підключений

чат-бот «єВорог», через який українці могли надсилати фото та відео перебування російських військ і техніки. Це дозволяє командирам відстежувати позиції противника та координувати удари. Зокрема ця система була використана під час оборони Києва, знищення крейсера «Москва», звільнення острова Зміїний, та Слобожанського контрнаступу [48].

Поряд із цим активно використовуються комунікаційні мережі та сенсорні системи. Наприклад, мережа супутникового інтернету Starlink забезпечила українським військовим понад 20 000 терміналів зв’язку, що витримують ворожі глушіння сигналу. Швидке розгортання Starlink дозволило підтримувати командні мережі (зокрема в системі Delta) навіть під час обстрілів критичної інфраструктури, а дрони продовжували передавати дані на оперативні пункти. Таким чином ІКС на основі супутникових каналів та мереж зв’язку виконують роль комунікаційної основи для збору та передачі OSINT-інформації [49].

Одним із найяскравіших прикладів інструментів для ситуаційного моніторингу є інтерактивні онлайн-карти конфліктів, які збирають та відображають дані з соціальних мереж. Так, українська платформа LiveUAmap позиціонує себе як незалежний глобальний новинний ресурс, що завдяки даним із соцмереж надає наближену до реального часу інформацію про переміщення військ, обстріли, інциденти насильства та інші події, наносячи їх на карту [50]. Зібрані через соцмедіа повідомлення з геолокацією проходять перевірку аналітиків, після чого відображаються на карті з мінімальною затримкою. Це дозволяє швидко отримати оперативну обізнаність про ситуацію. Карта LiveUAmap (рис. Б.1) для України візуалізує весь спектр подій – від зруйнованої інфраструктури, втрат техніки, обстрілів і повітряних тривог до офіційних повідомлень про звільнення територій. Таким чином, подібні карти виконують роль інформаційних «радарів», які виявляють і контекстуалізують ключові інциденти та надають хронологічний архів для аналізу тенденцій [51, 52].

На прикладі конфлікту в Сирії показано (рис. Б.1), як соціальні медіа-повідомлення (пости, фото, відео), розміщені очевидцями, геолокуються та відображаються на карті з поясненнями. Це дозволяє побачити розташування і

деталізацію подій (удари, бої, переміщення техніки) у реальному часі, підвищуючи ситуаційну обізнаність військових та аналітиків. Волонтери і аналітичні команди OSINT перевіряють достовірність таких повідомлень та зіставляють їх із іншими джерелами, щоб відфільтрувати неправдиві або спам-дані, перш ніж додати їх на мапу [50, 51].

Значення OSINT для ситуаційного моніторингу підтверджує і досвід повномасштабної війни в Україні з 2022 року. За висновками компанії Flashpoint, протягом цього конфлікту розвідка з відкритих джерел відіграє життєво важливу роль, допомагаючи силам безпеки та розвідки отримувати надійне, своєчасне й релевантне розуміння ризиків, пов'язаних з війною. Зокрема, OSINT забезпечує організації даними для польової ситуаційної обізнаності, реагування на кризи, виявлення дезінформації та інших завдань. Швидкість і всеохопність OSINT дозволяє навіть передбачати розвиток подій. Наприклад, ще до вторгнення 2022 року OSINT-спільнота виявила концентрацію російських військ біля України за супутниковими знімками і повідомленнями, що стало попереджувальним сигналом про підготовку агресії. Загалом, можливість черпати інформацію з величезної екосистеми відкритих даних і майже в реальному часі перетворювати її на обізнаність є революційною перевагою OSINT [52, 53, 54].

Таким чином, OSINT у поєднанні з розвиненими інформаційно-комунікаційними системами дає можливість оперативно фіксувати місцезнаходження ворожих сил, розвідувати плани противника та коригувати власні дії. Використання не лише традиційних розвідувальних каналів, а й відкритих соцмереж, супутникових знімків і мобільних застосунків суттєво підвищує ситуативну обізнаність силовиків і волонтерів на полі бою [49].

3.2 Краудсорсинг розвідданих та волонтерські OSINT-спільноти

У війні в Україні вперше в історії зафіксовано настільки масове залучення цивільних осіб до процесу збору розвідданих в режимі реального часу, тобто краудсорсинг розвідки. За даними Babel Street, уже в перші дні вторгнення українська армія звернулася через соцмережі до громадян із закликом

повідомляти про переміщення російських військ. Це фактично стало першим випадком застосування «розвідки натовпу» у воєнній історії. 27 лютого 2022 р. тисячі українців передавали через соціальні платформи координати колони ворожої техніки, що рухалася на Київ, і вже того ж дня цю колону було атаковано та знищено поблизу Бучі (рис. Б.2) [54]. Такий успіх продемонстрував цінність оперативної інформації від очевидців: кожен цивільний зі смартфоном може стати «сенсором» на полі бою. Експерти відзначають, що сьогодні буквально кожен громадянин зі смартфоном є не лише спостерігачем, але й учасником інформаційної війни, здатним фіксувати і передавати важливі дані зі свого оточення. Завдяки соціальним мережам і месенджерам військові можуть отримувати прямі повідомлення від населення про пересування чи дії ворожих підрозділів у їхньому районі, що підвищує прозорість поля бою в реальному часі [55].

Український уряд швидко інституціалізував підходи краудсорсингу розвідки, розробивши спеціальні цифрові інструменти. Міністерство цифрової трансформації запустило чат-бот «єВорог» у додатку «Дія», який гейміфікував процес подачі даних: користувач з підтвердженою особою може надіслати координати й фото ворожої техніки чи військ. Станом на 14 квітня 2022 року було ідентифіковано 570 «підозрюваних», включаючи російських військових і політичних чиновників, міністрів і керівників правоохоронних органів, тобто краудсорсинг приніс дуже швидкі результати. Від початку вторгнення за допомогою таких сервісів українські військові та правоохоронці зібрали гігантський масив повідомлень від громадян – про переміщення ворожих колон, місця ударів, підозрілих осіб тощо. Цей системний краудсорсинг даних, як відзначають експерти, не має прецедентів у сучасній війні. Роль волонтерів, які масово фіксують і передають інформацію з місця подій, стала настільки значущою, що без їх внеску ведення бойових дій і розслідування злочинів було б значно складнішим [56].

Крім офіційно організованих ініціатив, виникло багато незалежних волонтерських OSINT-груп, що координуються через Інтернет. Однією з них є

спільнота GeoConfirmed, яка об’єднала фахівців і ентузіастів для геолокації фото- та відеоматеріалів із зони бойових дій. Проєкт GeoConfirmed був створений волонтерами в перший день повномасштабної війни і націлений на те, щоб додавати «науковий шар геолокаційних даних» до візуального контенту конфлікту. Волонтери аналізують ландшафт, орієнтири та інші деталі на відео чи фото, звіряючи їх із супутниковими знімками та картами, щоб точно визначити місце події. Після верифікації точки наносяться на інтерактивну мапу, яку може переглядати кожен бажаючий [57, 58]. Подібні краудсорсингові OSINT-спільноти діють і в інших вимірах війни: наприклад, міжнародна розвідувальна спільнота InformNapalm (створена ще в 2014 року) збирає дані про російські війська на Донбасі та на територіях інших країн, де розташовані російська армія та озброєння, Oryx (міжнародна група аналітиків) документує фотографічні докази знищеної техніки, а спільнота ІТ-армія України залучає тисячі ІТ-фахівців до кіберрозвідки та протидії ворожим ресурсам. Також потрібно згадати про OSINT-спільноту Molfar, що вкладає свої сили на протидію пропаганді, розслідування та ідентифікацію воєнних злочинців та геопросторову розвідку [59], громадська організація «OsintFlow» має за головну місію збір інформації про воєнні злочини росії вчинені на території України [60], а спільнота OSINT-Бджоли допомагає у відбиванні збройної агресії, у ідентифікації воєнних злочинців рф та колаборантів та у притягненні їх до покарання [61]. Ключовим фактором успіху таких ініціатив є масовість учасників і швидкість обміну інформацією: як зазначає Центр досліджень армії США, незліченні звичайні громадяни з телефонами і GPS мимоволі розкривають у соцмережах деталі про розташування та дієздатність ворожих сил, стан інфраструктури та настрої населення. В результаті командири, що уважно стежать за цими відкритими сигналами, можуть отримати виграш у часі та інформованості порівняно з противником, який покладається лише на традиційну розвідку [50].

Варто зауважити, що краудсорсинг OSINT не позбавлений ризиків. Противник теж усвідомлює силу «розвідки натовпу» і може намагатися наповнювати інформаційний простір хибними повідомленнями, щоб ввести в

оману аналітиків. Тому волонтерські OSINT-спільноти розробляють внутрішні протоколи перевірки даних, а також взаємодіють з офіційними структурами, які можуть підтвердити або спростувати отримані відомості. У цілому ж модель «все бачучого натовпу» зарекомендувала себе надзвичайно ефективно. Як підсумовує журнал CLAWS, війна в Україні стала першою «цифровою» та «соціально-медійною» війною, де «кожен громадянин зі смартфоном – солдат і розвідник», а колективний моніторинг інформаційно-комунікаційних систем у реальному часі забезпечує безпрецедентну прозорість бойових дій [50, 55].

3.3 Протидія дезінформації та інформаційно-психологічним операціям

Інформаційний вимір сучасної війни не менш важливий за суто воєнний. Ворожі країни та групи систематично застосовують дезінформацію та інформаційно-психологічні операції для підриву морального духу, створення хибного наративу та маніпуляції громадською думкою. OSINT відіграє подвійну роль у цій сфері: з одного боку, як джерело виявлення і викриття фейків, а з іншого – як інструмент моніторингу інформаційного поля, що дозволяє відслідковувати кампанії впливу противника.

Напередодні повномасштабного вторгнення в Україну у лютому 2022 року аналітики фіксували різкий сплеск дезінформації проросійських сил у відкритих джерелах. Зокрема, Babel Street задовго до руху військ відзначила помітне зростання антиукраїнської риторики в соцмережах – ще в січні 2021 року, ідентифікувавши розгалужені мережі облікових записів, які розганяли наратив про «утиски російськомовних» та інші приводи для можливої інтервенції. На початку 2022 року цей інформаційний тиск сягнув піку (рис. Б.3): було виявлено понад 500 впливових проросійських облікових записів, які поширювали контент зі звинуваченнями України в агресії та порушеннях прав людини. Серед вкидів, які OSINT-аналітики ідентифікували як частину скоординованої кампанії, були фейки про обстріли й диверсії в «республіках» Донбасу, інсценування вибухів та евакуацій з метою звинуватити Збройні Сили України, неправдиві заяви про відвід російських військ тощо. Ретельний аналіз цифрових слідів цих повідомлень дозволив викрити мережу пов’язаних між собою ресурсів, які

працювали синхронно – це стало раннім індикатором підготовки вторгнення і частиною тактики створення інформаційного прикриття для агресії [54].

Безпосередньо перед нападом росії OSINT-спільнота відіграла важливу роль у спростуванні сфабрикованих приводів для війни. У лютому 2022 року російські державні ЗМІ та пропагандистські Telegram-канали почали масово публікувати постановочні відео «українських атак» – наприклад, нібито підрив хлорного заводу українськими диверсантами чи «напад» українців на машину з цивільними в ОРДЛО. Команда розслідувачів Bellingcat у відповідь створила публічну базу даних, де відстежувала всі такі відео і надавала їх перевірку та спростування. Відкрита інформація часто спростовувала заяви російської сторони: з'ясувалося, що час зйомки багатьох «екстрених» відео не збігається з офіційно заявленим, деякі ролики були зняті за декілька днів до інциденту або навіть походили з інших місць [62]. Завдяки OSINT вдалося викрити ці фейки ще до того, як вони стали приводом для ескалації конфлікту, продемонструвавши світовій спільноті справжню інформаційну картину.

Під час активної фази війни українські та міжнародні OSINT-групи систематично працювали над викриттям російської пропаганди та фальсифікацій. Волонтерські спільноти на кшталт Molfar оперативно реагували на резонансні події, збираючи докази та поширюючи звіти для ЗМІ. Показовим є кейс березня 2022 року, коли російські офіційні особи заперечували бомбардування драматичного театру в Маріуполі (де ховалися сотні цивільних) або намагалися перекласти вину на українських захисників. Аналітики Molfar швидко зібрали всі наявні відкриті дані – супутникові знімки зруйнованої будівлі, фотографії та відео очевидців до і після удару, перехоплені розмови – і склали детальний звіт, який відправили західним журналістам. Як результат, вже 25 березня впливова британська газета The Times опублікувала матеріал, що спирався на ці OSINT-докази і повністю спростовував російські заяви [63]. Таким чином, розвідники з відкритих джерел стали ключовими гравцями інформаційного фронту, негайно реагуючи на брехню і забезпечуючи медіа перевіреними фактами, які не дають спотворити реальність війни.

Наявність чисельних цифрових свідчень війни дозволила OSINT-аналітикам не лише спростовувати неправду, але й формувати правдивий наратив для світової аудиторії. Зокрема, відкриті дані про перебіг бойових дій показали невідповідність між заявами кремлівської пропаганди та реальними втратами росії. Аналітичний проект Oryx від початку війни почав публічно обліковувати підтверджені фотодоказами втрати техніки з обох сторін. Станом на березень 2024 рік Oryx зафіксував понад 15 000 одиниць втраченої російської військової техніки. Ці дані ґрунтуються винятково на візуальних підтвердженнях з відкритих джерел і тому користуються довірою західних експертів, на відміну від голослівних офіційних заяв. Фактично, OSINT-підхід Oryx став «золотим стандартом» прозорості війни, який довів, наскільки руйнівними є втрати агресора [64]. Кремль був змушений визнати силу таких розслідувачів: у липні 2022 року Bellingcat і інші незалежні OSINT-організації були оголошені росією практично ворогами режиму [65], що підтверджує їх ефективність у протидії дезінформації та донесенні правди.

3.4 Документування воєнних злочинів та забезпечення відповідальності

Війна в Україні продемонструвала новий рівень застосування OSINT для збирання доказів воєнних злочинів та порушень прав людини. Кількість цифрових свідчень – відео, фото, супутникових знімків, дописів очевидців – настільки величезна, що це безпрецедентно для будь-якого конфлікту. За словами дослідників, обсяги відкритих даних в Україні «розсіюють туман війни», фіксуючи те, що раніше залишалося прихованим. Ці матеріали стають доказами злочинів, які команди Інтернет-детективів ретельно каталогізують та перевіряють кожен факт, аби він міг бути використаний для притягнення винних до відповідальності [66].

Україна створила цілу екосистему взаємодіючих органів та ініціатив, які займаються документуванням агресії рф з використанням OSINT. Після початку вторгнення Офіс Генерального прокурора запровадив єдиний центр збору воєнних злочинів, куди стікається інформація з різних каналів – у тому числі через урядові застосунки та чат-боти, описані вище. Громадян закликають

фіксувати факти вбивств, поранень, руйнувань цивільних об’єктів, мародерства тощо і надсилати їх зі смартфонів, причому користувачам надаються інструкції щодо геотегування і хронометражу матеріалів, щоб вони мали доказову цінність [56].

Завдяки OSINT до судових кейсів потрапляють унікальні дані. Українська поліція разом із працівниками ІТ створили ІКС SORC, в якій накопичено тисячі доказів російської агресії відносно українського народу. Використовуючи підручні жорсткі диски і документи, слідчі отримали списки особового складу окупантів, накази, журнали, де записувалося «кто отдал приказ стрельнуть», і навіть схеми мародерства. Як зізнається криміналіст Сергій Болвінов, знайдені списки та листи стали доказами у багатьох кримінальних справах щодо воєнних злочинів. Використовуючи дані OSINT, геолокацію, супутникові знімки або розвідку, аналітики встановлюють, з якого населеного пункту був запущений боєприпас, хто там був розміщений і хто віддав наказ на його запуск [67].

Паралельно група з понад сорока правозахисних організацій об’єдналася у ініціативу «Трибунал для путіна» (T4p), навчаючи волонтерів збирати свідчення за міжнародними стандартами (наприклад, відповідають ознакам, передбаченим Римським статутом). Документатори T4p працюють як з відкритими джерелами, так і безпосередньо на місцях. Уся інформація проходить перевірку, її аналізують за допомогою OSINT-методів і систематизують у вигляді окремих кейсів. Серед них є і наймасштабніші атаки рф, зокрема бомбардування Маріупольського драмтеатру, підрив Каховської гідроелектростанції, загрози Запорізькій атомній електростанції, а також удари по релігійних і медичних об’єктах, зокрема по «Охматдиту». Станом на 20 березня 2025 року ініціатива T4p задокументувала 84396 воєнних злочинів (рис. Б.4, Б.5), скоєних під час повномасштабної війни в Україні. Також зафіксовано щонайменше 3745 випадків руйнування або пошкодження об’єктів культурної, релігійної та соціальної інфраструктури – зокрема історичних пам’яток, храмів, лікарень, освітніх і наукових установ. Також 17421 задокументована атака була спрямована по цивільних об’єктах: житлових будинках, підприємствах, школах, дитячих садках та інших спорудах.

За три роки діяльності ініціатива підготувала та передала до Міжнародного кримінального суду дев’ять подань щодо:

- Насильницьких зникнень на тимчасово окупованих територіях України;
- Передачі дітей з України до росії як доказ геноциду;
- Позасудових страт у Бучі та інших частинах України;
- Жорстоких позбавлень свободи на окупованій росією Харківщині;
- Геноциду у Маріуполі;
- Обстрілів України як воєнного злочину росії;
- Мови ворожнечі як злочину проти людяності;
- Розслідування злочинів проти довкілля;
- Катувань, вчинених російськими військовими в Україні [68].

Також верифікація за допомогою OSINT дала свої плоди, бо коли 8 липня 2024 році російська ракета Х-101 влучила в чергову цивільну ціль Охматдит, то аналітики за відкритими даними оперативно ідентифікували тип і траєкторію ракети, не залишивши агресору шансів відбрехатися. Подібним чином в квітні 2022 році з супутникових знімків і відео було доведено, що звірства в Бучі вчинялися саме під час російської окупації (жертви видно на знятих з космосу кадрах ще до відступу військ рф). Такі докази позбавляють кремль можливості замітати сліди і заперечувати очевидне.

Надзвичайно важливо, що зібрані OSINT-докази не лишаються просто в Інтернеті, а інтегруються в юридичні процеси. Вже було створено декілька міжнародних механізмів співпраці: Об’єднана слідча група при Євроюсті та Atrocity Crimes Advisory Group (ЄС, США, Британія) надають українським слідчим підтримку в опрацюванні доказів. У 2024 році Рада Європи започаткувала проєкт «CyberUA» для посилення можливості України в роботі з електронними доказами, пов’язаними з військовими злочинами та грубими порушеннями прав людини. Ці зусилля є частиною так званої «павутини підзвітності», що об’єднує урядові, громадські й приватні суб’єкти задля притягнення винних до суду. За даними RUSI, нині як мінімум 19 OSINT-

розслідувальних груп (серед яких є Berkeley’s Human Rights Lab, Molfar, OSINT for Ukraine, Global Rights Compliance), 6 юридичних фірм, 9 академічних центрів, 17 спеціальних ІТ-проєктів, підмережа з 23 судових органів в Україні та за її межами та 39 громадських організацій докладають зусиль до розслідування злочинів в Україні, використовуючи відкриті джерела. Така широка коаліція – нове явище, яке підсилює традиційну доказову базу показаннями очевидців і експертизою з місця подій.

Накопичений в Україні досвід заклав основу для нових підходів до правосуддя. Відкрита інформація перетворюється на докази в судах: фото, відео, супутникові знімки все частіше визнаються допустимими, якщо їх належно верифіковано та збережено [8]. Хоча залишаються виклики – величезний обсяг даних, вартість їх збереження, потреба у навчанні юристів – вже зрозуміло, що OSINT став невід’ємною частиною механізму справедливості. Безпрецедентне документування війни в Україні, здійснене армією OSINT-волонтерів, закладає прецедент для майбутніх судів і трибуналів, показуючи, що у цифрову епоху сховатися від правди неможливо.

3.5 Аналіз супутникових зображень для OSINT-розслідувань

Комбінація GEOINT і OSINT дозволяє не лише збирати супутникові зображення, а й поєднувати їх із даними з інших відкритих джерел, таких як соціальні мережі, відео з полів боїв і повідомлення очевидців. Наприклад, супутникові знімки можуть бути використані для геолокації подій, верифікації матеріалів з відкритих джерел, а також для створення карт ситуаційної обізнаності в реальному часі, що допомагає військовим і розвідникам зрозуміти повну картину бойових дій.

Доступність комерційних супутникових знімків високої роздільної здатності стала справжнім проривом для OSINT у військовій сфері. Якщо під час попередніх конфліктів геопросторова розвідка була властива тільки для наддержав, то тепер компанії на кшталт Maxar, Planet Labs, Iceye, які отримують дані через свої ІКС, публікують або продають зображення зон бойових дій ледь не кожного дня. Це дозволяє відстежувати переміщення військ і техніки,

фіксувати результати ударів, виявляти укріплення або руйнування. Супутникові фото почали викривати те, що противник намагався приховати, наприклад, ще в січні-лютому 2022 року знімки Maxar показали величезні скупчення російських військ біля кордонів України (рис. Б.6), а також розширення військових таборів у тимчасово окупованому Криму (рис. Б.7) [69]. У березні 2022 р. ті ж супутники виявили колону російської техніки довжиною 5 км, що тягнеться за 64 км від Києва (рис. Б.8), надаючи цінну інформацію про масштаби загрози [70].

У контексті північного регіону Гази під час конфлікту на початку 2025 року, супутникові знімки дозволяють оцінити масштаби руйнувань інфраструктури, таких як школи, лікарні та табори для внутрішньо переміщених осіб. Супутникові зображення, що зроблені за допомогою платформ, таких як Planet Labs, показують зруйновані та сильно пошкоджені будівлі, в тому числі місця, що використовувалися як притулки для переміщених осіб. Часто ці зображення показують пошкодження від вогню, а також виявляють масштаби руйнувань в ключових зонах, таких як Бейт-Лахія та Джабалія (рис. Б.9, Б.10) [71].

Щодо громадянської війни в Судані, то Сили швидкої підтримки і Збройні сили Судану ведуть бойові дії за контроль над країною, особливо в регіоні Дарфур. Місто Аль-Фашир стало притулком для понад 190 000 внутрішньо переміщених осіб, що тікали з інших районів. У зв'язку з інтенсивними боями, місто зазнало серйозних руйнувань, що суттєво обмежило доступ до медичної допомоги, їжі та безпечних притулків. Для моніторингу ситуації використовуються супутникові знімки, які дозволяють виявити пошкодження інфраструктури та позиції військ. Відео та фотографії, опубліковані в Інтернеті, перевіряються через супутникові знімки, що допомагає точно геолокувати місця бойових дій. Наприклад, супутникові зображення показали пошкодження критичної інфраструктури, таких як електростанція та лікарні, що використовувалися як притулки для цивільних. Дані з NASA FIRMS також використовуються для виявлення теплових сигналів, які можуть свідчити про пожежі, спричинені бойовими діями. Зокрема, з 10 по 13 травня були зафіксовані теплові сигнали на сході Аль-Фашира, що вказує на ймовірні пожежі в районах

бойових дій (рис. Б.11). Супутникові зображення також дозволяють виявити точні координати військових позицій Сил швидкої підтримки. Це дозволяє спостерігати за рухами військ та визначати найбільш постраждалі райони. Зокрема, у результаті аналізу знімків було виявлено військові бази та укріплення в безпосередній близькості до цивільних районів, що підтверджує високий рівень небезпеки для мирного населення [72].

Все це стало можливим завдяки ІКС космічної та наземної інфраструктури. Космічний сегмент включає не лише супутники-розвідники, а й системи зв'язку (Starlink, традиційні канали зв'язку та ретрансляції). Зображення завантажуються через наземні станції на хмарні платформи (AWS, Google Cloud тощо), де потужні алгоритми обробляють їх у масштабних базах даних. На кожному з цих етапів критичну роль відіграють інформаційно-комунікаційні системи: від мережі супутникового зв'язку Starlink, що передає командуванням «живі» зображення з дронів, до геоінформаційних служб, які надають інструменти аналізу («EO Browser» Sentinel Hub, Google Earth Engine). Завдяки цьому поєднання космічного сегмента, цифрових інструментів і відкритих даних будь-який аналітик OSINT може простежити колишню присутність техніки, підтвердити дату вибухів чи визначити уражені цілі – усе у відкритому доступі для світової спільноти.

Таким чином, супутникова розвідка у відкритому доступі стала очима світу, що спостерігають за конфліктом. Наявність знімків, відкритих для аналізу усіма зацікавленими, серйозно ускладнює здійснення прихованих операцій або інформаційних маніпуляцій. Якщо в минулому столітті світ бачив війну через кілька телеканалів чи газет, то зараз кожен може розглянути поле бою з космосу у різних формах і зробити власні висновки. OSINT-спільнота навчилася швидко витягувати максимум із цих зображень, що дозволяє і краще розуміти хід війни, і накопичувати доказову базу для історії та правосуддя.

4 ПОРІВНЯННЯ ІСНУЮЧИХ МЕТОДІВ OSINT ТА НАДАННЯ РЕКОМЕНДАЦІЙ ІЗ ЗАСТОСУВАННЯ OSINT

У даному розділі буде проведено порівняльний аналіз методів та інструментів OSINT, які використовуються для забезпечення кібербезпеки інформаційно-комунікаційних систем та загалом для аналізу отриманої інформації з відкритих джерел, зокрема в умовах військових конфліктів. Буде розглянуто їхню ефективність, переваги, недоліки та надано рекомендації щодо оптимального застосування на основі аналізу даних із статей та сучасних досліджень.

4.1 Порівняння пасивних і активних методів OSINT

Вже було раніше розглянуто, що методологія OSINT поділяється на пасивні та активні підходи для збору даних. Пасивний OSINT передбачає отримання інформації без прямої взаємодії з ціллю, непомітно для неї. Аналітик діє як спостерігач: переглядає веб-сайти, реєстри, соціальні мережі, не залишаючи слідів своєї присутності. Прикладом пасивного підходу може бути пошук згадок про особу через Google, читання публічних форумів, витяг даних з відкритих баз – без автентифікації чи контакту з об’єктом. Перевага пасивного OSINT – повна непомітність, тобто ціль не дізнається про інтерес до себе, відповідно не вживатиме контрзаходів. Недоліком є обмеженість доступу, бо багато сучасних ресурсів вимагають створення облікових записів, авторизацію та інші додаткові дії. У таких випадках пасивний збір не дозволяє отримати всю потрібну інформацію [24].

Активний OSINT включає певну взаємодію з ціллю чи середовищем, для отримання потрібних даних. Активні методи можуть включати: створення фіктивного облікового запису і додавання цілі в друзі для перегляду її приватних дописів; відправлення запиту на відновлення паролю, щоб отримати підказку; участь у закритій групі чи чаті, де присутня ціль, з метою збору інформації. Активний підхід часто потребує базових облікових записів (електронна пошта, профілі) та може розкривати присутність дослідника. Наприклад, якщо аналітик

завантажує файл з сайту цілі або коментує її пост – це активна дія, що теоретично може бути відслідкована об’єктом. Тому активний OSINT межує з оперативною роботою під прикриттям і в деяких випадках вимагає дозволу та етичного зважування ситуації [24]. Його плюсом є доступ до глибших шарів інформації (того самого контенту за паролем), а мінусом є ризик виявлення та правові нюанси (де проходить межа між дозволеним збором і незаконним вторгненням у приватність). У таблиці В.1 для наочності порівняємо пасивний і активний OSINT за кількома критеріями.

Обидва підходи доповнюють один одного. У типових розслідуваннях спочатку застосовують пасивні методи, тобто це тихий збір всього, що є у відкритому доступі, потім у разі потреби переходять до активних заходів для заповнення прогалин. Наприклад, аналітик може спочатку зібрати всі публічні дані про компанію (адреси, керівництво, домени), а тоді використати активний крок, тобто надіслати співробітникам компанії запити через LinkedIn чи щось інше, для отримання певної реакції чи підтвердження.

4.2 Порівняльний аналіз популярних інструментів OSINT

Для здійснення OSINT-розвідки розроблено сотні інструментів – від простих утиліт до потужних багатофункціональних платформ. Кожен має свою спеціалізацію, переваги і обмеження. У додатку В.2 наведено порівняльну характеристику кількох популярних інструментів, які часто застосовуються у сфері кібербезпеки та розвідки.

Дана таблиця з аналізом інструментів OSINT показує різноманітність підходів та можливостей для збору, аналізу і обробки даних з відкритих джерел. Всі ці інструменти мають свої переваги, але їх ефективність залежить від конкретних завдань і контексту використання.

По-перше, інструменти можуть бути поділені на кілька категорій залежно від типу завдання. Наприклад, для автоматизованого збору даних з різних джерел зручно використовувати інструменти на зразок SpiderFoot або Recon-ng, які дозволяють швидко збирати великі обсяги даних, зокрема для аналізу вразливостей і тестування на проникнення. Ці інструменти пропонують

модульність та гнучкість, що дозволяє налаштовувати збір під конкретні цілі, але вони потребують деяких технічних знань для максимальної ефективності. По-друге, інструменти, які спеціалізуються на візуалізації та аналізі зв'язків, як Maltego, є потужними для аналізу загроз, особливо у контексті соціальних мереж та кіберзлочинності. Візуалізація даних у вигляді графів дозволяє зручно представити складні взаємозв'язки між об'єктами, що робить цей інструмент ефективним для розслідувань, але він має обмеження для початківців через складність використання та платний доступ до деяких функцій. Такі інструменти, як Shodan, що спеціалізуються на пошуку IoT-пристроїв та виявленні вразливостей через сканування портів, є важливими для безпеки мереж і систем. Вони дозволяють виявляти вразливості в Інтернеті, але також мають обмеження у вигляді складного інтерфейсу для новачків та доступу до платних функцій. Ще однією важливою групою є інструменти для пошуку чутливих даних, такі як Google Dorks і theHarvester, які використовуються для виявлення витоків або збору контактних даних. Хоча ці інструменти є доступними і простими у використанні, їх ефективність може бути обмежена через необхідність ручної обробки результатів та обмежену глибину аналізу. А от такі інструменти, як OSINT Framework, забезпечують систематизований підхід до збору інформації, допомагаючи обрати потрібний інструмент для певних завдань. Однак вони не є самостійними засобами збору, а лише служать підмогою для інших інструментів, що знижує їх ефективність у порівнянні з більш спеціалізованими засобами.

Загалом, ефективність кожного інструменту залежить від конкретної задачі, технічних знань користувача та потреби в точності збору даних. Інтеграція різних інструментів в один процес дозволяє максимально використовувати їх потенціал для розслідувань, аналізу загроз та виявлення вразливостей.

4.3 Рекомендації щодо оптимального застосування OSINT у кібербезпеці та розвідці

Беручи до уваги досвід сучасних військових конфліктів, кібервійн та загалом критичних ситуацій, чи то в організаціях, чи то в компаніях, можна

сформулювати низку рекомендацій для ефективного використання методів та інструментів OSINT:

- Більша інтеграція OSINT в загальний цикл розвідки та безпеки для військових штабів, спецслужб і команд кібербезпеки, щоб вони розглядати відкриті джерела як рівноцінний компонент розвідданих, поруч з HUMINT, SIGINT та іншими видами розвідки. Як зазначає Атлантична рада, OSINT може допомогти лідерам отримати швидке та актуальне розуміння свого робочого середовища (хто що робить, де і коли). Тому слід подолати упередження на перевагу лише секретної інформації та активно впроваджувати аналіз відкритих даних у процес прийняття рішень [52]. Зокрема, в кібербезпеці OSINT має стати невід'ємною частиною процедур оцінки загроз, тобто моніторинг даркнет-форумів, витоків у відкритому доступі, соцмереж для індикаторів компрометації та інше.
- Для більш точних даних потрібно поєднувати різні типи джерел – соціальні мережі, технічні сканери, реєстри доменів, витоки баз даних, щоб отримати повнішу картину загроз. Однак, інформація з OSINT не завжди є достовірною або актуальною, тож потрібно критично оцінювати знайдене. Наприклад, дані з Інтернету або форумів варто підтверджувати технічними доказами (скріншотами, гешами файлів, записами трафіку тощо). Тому ІКС мають бути адаптовані до безперервного потоку OSINT-даних через впровадження модулів штучного інтелекту та машинного навчання, які здатні автоматично ідентифікувати підозрілу активність або потенційні вектори атак.
- Для ефективного використання OSINT у кібербезпеці критично важливо інтегрувати відкриті джерела з сучасними ІКС. Через колосальні обсяги інформації автоматизація це необхідність, тож потрібно створювати та розвивати платформи, що агрегують дані з сотень джерел і застосовують машинне навчання для виявлення тенденцій, аномалій, класифікації контенту. Наприклад, системи у партнерстві Talkwalker–Hootsuite вже вміють моніторити 150 млн веб-джерел на 187 мовах і прогнозувати тренди на 90 днів вперед за допомогою ШІ [73]. Військова та урядова розвідка має впроваджувати аналогічні або більш

спеціалізовані рішення, щоб не потонути в інформаційному морі. Особливо корисним є застосування ШІ для автоматичної розшифровки відео, перекладу іноземного контенту, семантичного аналізу (виявлення дезінформації, емоційного забарвлення).

- Сучасні інструменти дозволяють автоматично збирати великі обсяги даних (скрипти, боти, платформи моніторингу). Це підвищує швидкість і охоплення OSINT, але важливо, щоб людина відслідковувала роботу автоматизованих систем [74], бо без належного нагляду скрипти можуть ненавмисно порушити правила користування певним ресурсом або зібрати зайве. Тому потрібно налаштовувати фільтри й критерії збору, регулярно переглядати результати та коригувати роботу автоматизованих рішень.

- Необхідно обмежувати цифровий слід військових, тобто навчити особовий склад не публікувати чутливі фото/пости, використовувати цензурування метаданих при офіційних публікаціях (наприклад, не показувати GPS-теги на фото техніки), щоб ворогам не вдалося скомпроментувати військові ІКС чи їхні частини. Під час операцій слід планувати заходи проти ворожого OSINT: хибні цілі, димові завіси (щоб ускладнити аналіз супутникових знімків), інформаційні вкиди для заплутування ворожих аналітиків (але дуже обережно, щоб не дезінформувати власних громадян), тобто потрібна стратегія, що ускладнила б противнику моніторинг дій і використання чутливих даних із соцмереж.

- Український досвід показав, що масове залучення волонтерів дає величезну кількість даних, які необхідно структурувати і перевіряти. Тож для цього рекомендується створювати такі громадські платформи з контролем експертів, як портал «єВорог», куди громадяни можуть надсилати фото/відео з прив’язкою до карти, а далі аналітики та алгоритми відсіюють фейки і додадуть до бази. Механізми краудсорсингу OSINT слід включити до доктрин оборони і цивільного захисту, щоби з перших годин конфліктів чи інших ситуацій мати налагоджений канал збору інформації від населення.

- Організаціям чи компаніям, що використовують OSINT потрібно мати чіткі протоколи, щоб OSINT-діяльність не порушувала закон, тобто можна розробити керівні принципи поведінки OSINT-фахівця, щодо приватності, використання фейкових облікових записів, взаємодії з третіми особами. Також потрібно врахувати юридичну силу здобутих даних: для судів важливо зберігати ланцюжок автентичності (хто і де скачав відео, щоб доказ не визнали підробкою).
- Для захисту бізнесу і критичної інфраструктури рекомендується проводження постійного моніторингу даркнету та хакерських форумів на згадки про свою організацію (злиті бази, плани атак), перевірки відкритих налаштувань хмарних сховищ (щоб нічого конфіденційного не було злито до Інтернету), OSINT-аудиту кандидатів при взятті на роботу. Великі компанії вже впроваджують ці практики, але середні та малі також мають звернути увагу.
- Не потрібно забувати про підвищення кваліфікації звичайних робітників або працівників, залучених до OSINT, бо середовище відкритих джерел швидко змінюється – з’являються нові платформи (наприклад, чергові соцмережі чи месенджери), інструменти розвідки, методи приховування інформації. Тобто люди повинні бути обізнаними з актуальними техніками OSINT та вміти ними користуватися.

Запровадження цих рекомендацій дозволить зробити впровадження OSINT більш ефективним і безпечним для організацій та суспільства. І в результаті, відкриті джерела стануть надійним підґрунтям для кіберзахисту, мінімізуючи ризики пропуску важливої інформації або порушення норм. OSINT, впроваджений за кращими практиками, перетворюється на потужний інструмент попередження атак, вчасного реагування та стратегічного планування кібербезпеки.

ВИСНОВКИ

У процесі виконання цієї дипломної роботи було здійснено аналіз методів і механізмів OSINT, а також особливу увагу приділено їхньому значенню для забезпечення кібербезпеки та ролі у контексті збройних конфліктів. Отримані результати підкреслюють важливість OSINT як потужного інструмента у протидії кіберзагрозам та інформаційним атакам, особливо в умовах воєн, кризових ситуацій та збройних протистоянь. У межах роботи було розглянуто ключові аспекти використання OSINT, його історичну еволюцію, сучасні методи й інструменти, а також наведено низку прикладів практичного застосування у військових конфліктах, зокрема в контексті російсько-української війни, де ІКС забезпечують швидкий обмін даними та їх аналіз.

Розвідка з відкритих джерел є інструментом збору та аналізу інформації з публічних ресурсів у режимі реального часу. На відміну від інших форм розвідки, OSINT використовує соціальні мережі, урядові документи, наукові публікації тощо, що робить його доступним для журналістів, аналітиків і фахівців із кібербезпеки. Ефективна робота з OSINT потребує чіткої структури, від формування запиту до перевірки достовірності даних і складання звіту, що неможливо без інтеграції з сучасними ІКС для автоматизації процесів. З часом OSINT еволюціонував від аналізу газет і радіо до складного аналізу соцмереж, супутникових зображень і баз даних. Сьогодні він є ключовим інструментом як для атак, так і для кіберзахисту, дозволяючи виявляти вразливості, витоки даних. Такі інструменти, як SpiderFoot, Maltego, Recon-ng, спрощують і автоматизують процес збору й аналізу інформації. Для глибшого аналізу використовуються методології, як F3EAD, SWOT, PESTEL, що дозволяють систематизувати ризики й адаптуватися до цифрового середовища. А от порівняння пасивного й активного OSINT свідчить про важливість поєднання обох підходів для ефективного збору даних. Вибір інструментів і методів залежить від завдань, технічної підготовки користувача та дотримання етичних і юридичних норм.

OSINT також відіграє критичну роль у військових конфліктах, забезпечуючи ситуаційну обізнаність, а також допомагає документувати злочини,

боротися з дезінформацією і формувати правдиву ситуацію про поле бою чи інші обставини. Волонтерські спільноти та краудсорсинг відіграють значну роль у зборі даних, підвищуючи прозорість бойових дій. У ході повномаштабної війни в Україні, ефективність OSINT отримала підтвердження на практиці: аналітики помічали підготовку до вторгнення ще за місяці до її початку, а під час бойових дій - оперативно збирали розвіддані про пересування і стан військ противника.

Також було сформовано рекомендації щодо впровадження OSINT у діяльність з кіберзахисту, враховуючи отримані результати. Рекомендації наголошують на необхідності дотримуватися кращих практик (юридичні норми, етичність, фокус на цілі, багатоетапна перевірка даних) та інтегрувати OSINT у існуючі процеси безпеки для посилення ефекту. Успіх OSINT-розвідки залежить від правильної організації: коли зусилля аналітиків підтримуються сучасними інструментами, регламентами і навчанням. В умовах військових конфліктів ці аспекти набувають особливого значення, адже кібератаки супротивника часто йдуть пліч-о-пліч з інформаційними операціями, і реагувати на них треба швидко та комплексно. Поєднання методів відкритої розвідки з традиційними засобами інформаційної безпеки дозволяє створити багаторівневу систему захисту, здатну протидіяти як технічним кіберзагрозам, так і маніпулятивному інформаційному впливу. У війнах нового покоління, де розмиті межі між кіберпростором і фізичним полем бою, володіння інформацією стає запорукою стійкості і OSINT може допомогти із цим, відкриваючи доступ до великого масиву даних, що можна використати на свою користь.

Таким чином, впровадження OSINT у систему кібербезпеки є виправданим і необхідним кроком. Організації, особливо в умовах підвищеної загрози через військові дії або геополітичну напругу, повинні активно розвивати компетенції з розвідки відкритих джерел. Це включає інвестиції у відповідні технології, навчання фахівців, налагодження обміну даними з партнерами. Лише за умов використання повного спектру доступної інформації та її обробки в ІКС можна досягти проактивного кіберзахисту, здатного витримати сучасні виклики.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. List of intelligence gathering disciplines. *Wikipedia*. Режим доступу: https://en.wikipedia.org/wiki/List_of_intelligence_gathering_disciplines (дата звернення: 14.03.2025).

2. Introduction to intelligence disciplines. *ACK3*. Режим доступу: https://ack3.eu/introduction-to-intelligence-disciplines/ (дата звернення: 16.04.2025).

3. Open-source intelligence. *Wikipedia*. Режим доступу: https://en.wikipedia.org/wiki/Open-source_intelligence (дата звернення: 05.02.2025).

4. Glover E. What is open source intelligence (OSINT)? *Built In*. Режим доступу: https://builtin.com/articles/open-source-intelligence-osint (дата звернення: 05.02.2025).

5. OSINT framework: how open source intelligence powers cybersecurity. *Bitsight*. Режим доступу: https://www.bitsight.com/learn/osint-framework (дата звернення: 09.03.2025).

6. Block L. The long history of OSINT. *Journal of intelligence history*. 2023. P. 95–109. Режим доступу: https://doi.org/10.1080/16161262.2023.2224091 (дата звернення: 05.03.2025).

7. The historical use of OSINT through the centuries. *IMSL. Intelligence Management Support Services*. Режим доступу: https://www.intelmsl.com/osint-history/ (дата звернення: 09.03.2025).

8. Puzzling pieces: OSINT and war crime accountability in ukraine. *Royal United Services Institute*. Режим доступу: https://www.rusi.org/explore-our-research/publications/commentary/puzzling-pieces-osint-and-war-crime-accountability-ukraine (дата звернення: 27.03.2025).

9. A brief history of open source intelligence. *Bellingcat*. Режим доступу: https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/ (дата звернення: 05.03.2025).

10. Запорожченко М. М. Місце osint в життєвому циклі кібератаки. *Телекомунікаційні та інформаційні технології*. 2023. Т. 78, № 1. С. 53–60. Режим

доступу:https://tit.dut.edu.ua/index.php/telecommunication/article/view/2455/2337 (дата звернення: 09.03.2025).

11. How OSINT is used in cybersecurity - Part One. *IoSENTRIX*. Режим доступу: https://www.iosentrix.com/blog/how-osint-is-used-in-cybersecurity-part-1 (дата звернення: 09.03.2025).

12. Enoch Agbu. The role of OSINT in the evolution of threat intelligence. *The UK OSINT Community*. Режим доступу: https://www.osint.uk/content/the-evolution-of-threat-intelligence (дата звернення: 29.03.2025).

13. OSINT as a vector for cyber threat intelligence, from indicator collection to attribution. *HarfangLab*. Режим доступу: https://harfanglab.io/blog/methodology/osint-vector-cyber-threat-intelligence-indicator-collection-attribution/ (дата звернення: 29.03.2025).

14. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР: станом на 20 квіт. 2025 р. Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-вр (дата звернення: 06.05.2025).

15. Війська зв'язку та кібербезпеки. *МОУ*. Режим доступу: https://mod.gov.ua/pro-nas/vijska-zv-yazku-ta-kiberbezpeki (дата звернення: 06.05.2025).

16. ТАКТИЧНИЙ ЗВ'ЯЗОК: Настанова від 24.12.2020. Режим доступу: https://sprotyvg7.com.ua/wp-content/uploads/2024/03/2_ВКДП-6-11003.01-НАС-ТАТКТ-ЗВ.pdf (дата звернення: 06.05.2025).

17. CERT-UA минулого року опрацювала 4315 кіберінцидентів. *Держспецзв'язку*. Режим доступу: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv?fbclid=IwY2xjawHsV4FleHRuA2FlbQIxMAABHYnNezsqBJiQZNSaZEkbMEH4_DqJ7mjCbcGEu24c1ceX_iwn2_MNROBv8g_aem_Lt6kfy2eaNHvrEa2Zc3GTg (дата звернення: 07.05.2025).

18. Interfax-Ukraine. Атаки на ЗСУ й органи влади трапляються дедалі частіше, їх реалізують через людей, які користуються месенджерами - звіт Держспецзв'язку про російські кібероперації. *Інтерфакс-Україна*. Режим доступу: https://interfax.com.ua/news/telecom/1015696.html (дата звернення: 07.05.2025).

19. Gupta V. K. Case studies of successful OSINT investigations. *LinkedIn*. Режим доступу: https://www.linkedin.com/pulse/case-studies-successful-osint-investigations-vijay-gupta--0b7cc (дата звернення: 09.03.2025).

20. Kinahan cartel: wanted narco boss exposes whereabouts by posting google reviews. *Bellingcat*. Режим доступу: https://www.bellingcat.com/news/2024/03/30/kinahan-cartel-wanted-narco-boss-exposes-whereabouts-by-posting-google-reviews/ (дата звернення: 09.03.2025).

21. Julian, an OSINT investigator exposing the truth about chinese fentanyl. *OSINT Industries*. Режим доступу: https://www.osint.industries/project/case-study-osint-unveils-link-between-silicon-firms-and-global-fentanyl-crisis (дата звернення: 09.03.2025).

22. MH17 the open source evidence. *Bellingcat*. Режим доступу: https://www.bellingcat.com/app/uploads/2015/10/MH17-The-Open-Source-Evidence-EN.pdf (дата звернення: 12.03.2025).

23. The hunt for malaysia's elusive wildlife trafficker. *Bellingcat*. Режим доступу: https://www.bellingcat.com/news/2025/02/11/the-hunt-for-malaysias-elusive-wildlife-trafficker/ (дата звернення: 14.03.2025).

24. Defining Active vs. Passive OSINT. *Ntrepid*. Режим доступу: https://ntrepidcorp.com/managed-attribution/defining-active-vs-passive-osint/ (дата звернення: 16.03.2025).

25. Shelby Hiter. Open source intelligence (OSINT) guide. *EWEEK*. Режим доступу: https://www.eweek.com/big-data-and-analytics/open-source-intelligence-osint/ (дата звернення: 16.03.2025).

26. TechMindXperts. The beginner’s guide to open-source intelligence (OSINT): techniques and tools. *Medium*. Режим доступу: https://medium.com/@techmindxperts/the-beginners-guide-to-open-source-intelligence-osint-techniques-and-tools-6a91b9c37ee1 (дата звернення: 16.03.2025).

27. Warner C. F3EAD cycle in cyber threat intelligence. *Medium*. Режим доступу: https://warnerchad.medium.com/f3ead-cycle-for-cti-e15a42194faa (дата звернення: 16.03.2025).

28. How to perform a SWOT analysis for cyber risk quantification. *Scrut Automation*. Режим доступу: https://www.scrut.io/post/how-to-perform-a-swot-analysis-for-cyber-risk-quantification (дата звернення: 16.03.2025).

29. Zubic E. How PESTEL analysis can enhance OSINT research strategies. *Medium*. Режим доступу: https://publication.osintambition.org/how-pestel-analysis-can-enhance-osint-research-strategies-06ad86efc108 (дата звернення: 16.03.2025).

30. OSINT – що це таке, суть, визначення та приклади, види, методи та інструменти розвідки на основі відкритих джерел. *Termin.in.ua*. Режим доступу: https://termin.in.ua/osint-rozvidka-na-osnovi-vidkrytykh-dzherel/ (дата звернення: 16.03.2025).

31. Rajput S. Spiderfoot(OSINT). *Medium*. Режим доступу: https://medium.com/@sr0504526/spiderfoot-osint-45411d16d270 (дата звернення: 20.03.2025).

32. SpiderFoot. *GitHub*. Режим доступу: https://github.com/smicallef/spiderfoot?tab=readme-ov-file (дата звернення: 20.03.2025).

33. Maltego частина 1. Принципи роботи та можливості, 4 релізи. *HackYourMom*. Режим доступу: https://hackyourmom.com/kibervijna/zbir-informacziyi-pro-suprotyvnyka/osint-akademiya/4-relizy-maltego-prynczypy-roboty-ta-mozhlyvosti/ (дата звернення: 20.03.2025).

34. Recon-ng Information gathering tool in Kali Linux. *GeeksforGeeks*. Режим доступу: https://www.geeksforgeeks.org/recon-ng-installation-on-kali-linux/ (дата звернення: 20.03.2025).

35. Shodan (website). *Wikipedia*. Режим доступу: https://en.wikipedia.org/wiki/Shodan_(website) (дата звернення: 20.03.2025).

36. Ravenstone K. Google Dorks на службі у OSINT. *KR. Laboratories*. Режим доступу: https://kr-labs.com.ua/blog/google-dorks-for-osint/ (дата звернення: 20.03.2025).

37. E-mails, subdomains and names Harvester - OSINT. *GitHub*. Режим доступу: https://github.com/laramies/theHarvester (дата звернення: 20.03.2025).

38. What is The Harvester Tool and how to run a Harvester Tool? *Secuneus Tech*. Режим доступу: https://www.secuneus.com/the-harvester-tool/ (дата звернення: 20.03.2025).

39. OSINT Framework. *Neotas*. Режим доступу: https://www.neotas.com/osint-framework/ (дата звернення: 20.03.2025).

40. Pathak A. OSINT Tool to know. *Medium*. Режим доступу: https://medium.com/nerd-for-tech/osint-tool-to-know-768834d32898 (дата звернення: 20.03.2025).

41. Найкращі інструменти для розвідки на основі відкритих джерел (OSINT) у 2023 році. *TheTransmitted*. Режим доступу: https://thetransmitted.com/security/najkrashhi-instrumenti-dlya-rozvidki-na-osnovi-vidkritih-dzherel-osint-u-2023-roczi/ (дата звернення: 20.03.2025).

42. Intelligence X is a search engine and data archive. *Intelligence X*. Режим доступу: https://intelx.io/about (дата звернення: 20.03.2025).

43. Wright P. The Challenges in OSINT Analysis Concerning Digital Evidence. *LinkedIn*. Режим доступу: https://www.linkedin.com/pulse/challenges-osint-analysis-concerning-digital-evidence-paul-wright-yutrc (дата звернення: 22.03.2025).

44. How to solve the top 3 challenges of open-source intelligence. *Silobreaker*. Режим доступу: https://www.silobreaker.com/blog/cyber-threats/solutions-to-common-osint-challenges-using-open-source-intelligence/ (дата звернення: 22.03.2025).

45. Collyer D. OSINT and Ethics: Navigating the Challenges of Responsible Intelligence Gathering. *SOS Intelligence*. Режим доступу: https://sosintel.co.uk/osint-and-ethics-navigating-the-challenges-of-responsible-intelligence-gathering/ (дата звернення: 22.03.2025).

46. Souberbielle J. Enhancing Operational Success: The Role of Situational Awareness in OSINT. *Skopenow*. Режим доступу: https://www.skopenow.com/news/enhancing-operational-success-the-role-of-situational-awareness-in-osint (дата звернення: 23.03.2025).

47. Ситуаційна обізнаність. *Вікіпедія*. Режим доступу: https://uk.wikipedia.org/wiki/Ситуаційна_обізнаність (дата звернення: 24.03.2025).

48. Дельта (система ситуаційної обізнаності) – Вікіпедія. *Вікіпедія*. Режим доступу: https://uk.wikipedia.org/wiki/Дельта_(система_ситуаційної_обізнаності) (дата звернення: 07.05.2025).

49. Putrenko V., Pashynska N. Military Situation Awareness: Ukrainian Experience. *Applied Cybersecurity & Internet Governance*. 2024. Режим доступу: https://doi.org/10.60097/acig/190341 (дата звернення: 08.05.2025).

50. Rasak M. J. Event Barraging and the Death of Tactical Level Open-Source Intelligence. *Army University Press*. Режим доступу: https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2021/Rasak-Open-Source-Intelligence/ (дата звернення: 24.03.2025).

51. Live Universal Awareness Map displays events related to Russia's invasion of Ukraine. *European data*. Режим доступу: https://data.europa.eu/en/news-events/news/live-universal-awareness-map-displays-events-related-russias-invasion-ukraine (дата звернення: 24.03.2025).

52. NATO must recognize the potential of open-source intelligence. *Atlantic Council*. Режим доступу: https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-must-recognize-the-potential-of-open-source-intelligence/ (дата звернення: 24.03.2025).

53. The Role of OSINT in Russia's Invasion of Ukraine. *Flashpoint*. Режим доступу: https://www.flashpoint.io/resources/report/role-of-osint-russia-invasion-of-ukraine/ (дата звернення: 24.03.2025).

54. Baffa R. The Ukraine-Russia War Confirms the Value of OSINT. *Babel Street*. Режим доступу: https://www.babelstreet.com/blog/the-ukraine-russia-war-confirms-the-value-of-osint (дата звернення: 24.03.2025).

55. Vishwasrao Sanjay P. Rising Role of OSINT in Conflict/War. *CLAWS Journal*. 2023. Т. 16, № 2. С. 86–98. Режим доступу:

https://www.ssoar.info/ssoar/bitstream/handle/document/97176/ssoar-claws-2023-2-vishwasrao-Rising_Role_of_OSINT_in.pdf (дата звернення: 26.03.2025).

56. Bergengruen V. How Ukraine Is Crowdsourcing Digital Evidence of War Crimes. *Time*. Режим доступу: https://time.com/6166781/ukraine-crowdsourcing-war-crimes (дата звернення: 26.03.2025).

57. Homepage - Geoconfirmed. *Geoconfirmed*. Режим доступу: https://geoconfirmed.org/ (дата звернення: 26.03.2025).

58. Geolocating Visual Media in Conflict Zones. *Maps Mania*. Режим доступу: https://googlemapsmania.blogspot.com/2024/10/geolocating-visual-media-in-conflict.html (дата звернення: 26.03.2025).

59. Розвідувальна агенція Molfar. *Molfar*. Режим доступу: https://molfar.com/ (дата звернення: 26.03.2025).

60. Про нас. *OsintFlow*. URL: https://osintflow.com/ (дата звернення: 26.03.2025).

61. OSINT-бджоли Знайдемо кожного. *OSINT-бджоли*. Режим доступу: https://osintbees.com/ (дата звернення: 26.03.2025).

62. Documenting and Debunking Dubious Footage from Ukraine's Frontlines. *Bellingcat*. Режим доступу: https://www.bellingcat.com/news/2022/02/23/documenting-and-debunking-dubious-footage-from-ukraines-frontlines/ (дата звернення: 27.03.2025).

63. Старосек А. OSINT в Україні: хто і як допомагає фронту під час війни? *Українська правда*. Режим доступу: https://www.pravda.com.ua/columns/2023/01/23/7386112/ (дата звернення: 27.03.2025).

64. York C. Russian equipment losses in Ukraine surpass 15,000, says Oryx OSINT group. *The Kyiv Independent*. Режим доступу: https://kyivindependent.com/russian-equipment-losses-in-ukraine-surpass-15-000-says-oryx-osint-group/ (дата звернення: 27.03.2025).

65. Open-source intelligence in the Russian invasion of Ukraine. *Wikipedia*. Режим доступу: https://en.wikipedia.org/wiki/Open-

source_intelligence_in_the_Russian_invasion_of_Ukraine (дата звернення: 27.03.2025).

66. Amos D. Open source intelligence methods are being used to investigate war crimes in Ukraine. *NPR*. Режим доступу: https://www.npr.org/2022/06/12/1104460678/open-source-intelligence-methods-are-being-used-to-investigate-war-crimes-in-ukr (дата звернення: 27.03.2025).

67. Ukraine: The Database Helping Solve War Crimes. *Institute for War & Peace Reporting - IWPR*. Режим доступу: https://iwpr.net/global-voices/ukraine-database-helping-solve-war-crimes (date of access: 07.05.2025).

68. «Ми мріємо стати непотрібними»: ініціатива «Трибунал для Путіна» (T4P) презентувала результати роботи за три роки - Українська Гельсінська спілка з прав людини. *Українська Гельсінська спілка з прав людини*. Режим доступу: https://www.helsinki.org.ua/articles/my-mriiemo-staty-nepotribnymy-initsiatyva-trybunal-dlia-putina-t4p-prezentuvala-rezultaty-roboty-za-try-roky/ (дата звернення: 27.09.2025).

69. Maxar опублікувала нові супутникові знімки російських військ у Білорусі та окупованому Криму (ФОТО). *Detector.media*. Режим доступу: https://detector.media/infospace/article/196127/2022-02-02-maxar-opublikuvala-novi-suputnykovi-znimky-rosiyskykh-viysk-u-bilorusi-ta-okupovanomu-krymu-foto/ (дата звернення: 27.03.2025).

70. Орлова В. Супутники зафіксували величезну колону російської військової техніки біля Києва (знімки). *УНІАН*. Режим доступу: https://www.unian.ua/war/suputniki-zafiksuvali-velicheznu-kolonu-rosiyskoji-viyskovoji-tehniki-bilya-kiyeva-znimki-novini-kiyeva-11723149.html (дата звернення: 27.03.2025).

71. Satellite Imagery Shows Schools and Hospitals Destroyed in Northern Gaza. *Bellingcat*. Режим доступу: https://www.bellingcat.com/news/2025/02/04/satellite-imagery-shows-schools-and-hospitals-destroyed-in-northern-gaza/ (дата звернення: 27.03.2025).

72. Civilians Trapped in Al Fashir as Rapid Support Forces Advance. *Bellingcat*. Режим доступу: https://www.bellingcat.com/news/africa/2024/06/12/sudan-darfur-war-conflict-civilians-trapped-in-al-fashir-el-fasher-rsf-saf-genocide/ (дата звернення: 27.03.2025).

73. 15 Best OSINT (Open Source Intelligence) Tools for 2025. *Talkwalker*. Режим доступу: https://www.talkwalker.com/blog/best-osint-tools (дата звернення: 29.03.2025).

74. Open-Source Intelligence (OSINT). *Imperva*. Режим доступу: https://www.imperva.com/learn/application-security/open-source-intelligence-osint/ (дата звернення: 29.03.2025).

ДОДАТОК А

ТЕОРЕТИЧНІ ОСНОВИ OSINT ТА ЙОГО ЗАГАЛЬНІ ПРИКЛАДИ

Рисунок А.1 – П’ять кроків OSINT-розслідування

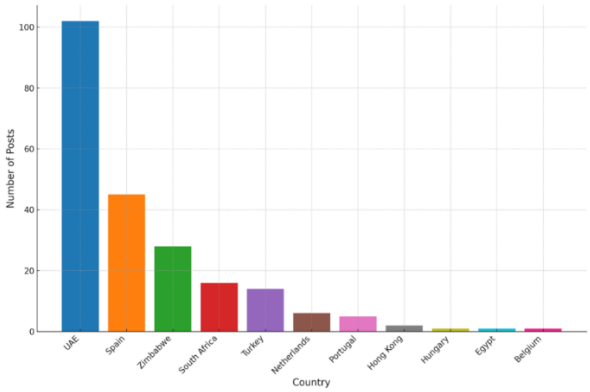

Рисунок А.2 – Графік, що показує країни, про які Крістофер Кінахан-старший опублікував відгуки Google

Рисунок А.3 – Частина шляху ідентифікованого військового конвою, який прямував з курська до міллерово (росія) у період з 23 по 25 червня

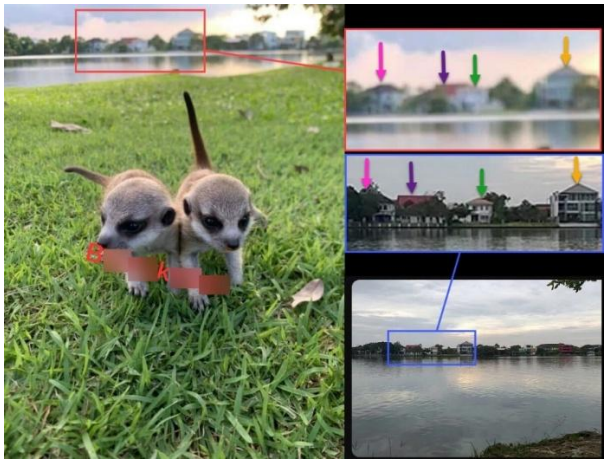

Рисунок А.4 – Скріншот відео за яким визначили місце зйомки тварин для продажу (Зліва: фотографія, зроблена одним із клієнтів ВК, на якій зображені два сурикати. Праворуч угорі: обрізка будівель на фоні фотографії ліворуч. Внизу праворуч: зображення села Саммакорн, Бангкок, Таїланд, на якому показано той самий ряд будівель)

ДОДАТОК Б

ЗАСТОСУВАННЯ OSINT ПІД ЧАС ВІЙСЬКОВИХ КОНФЛІКТІВ

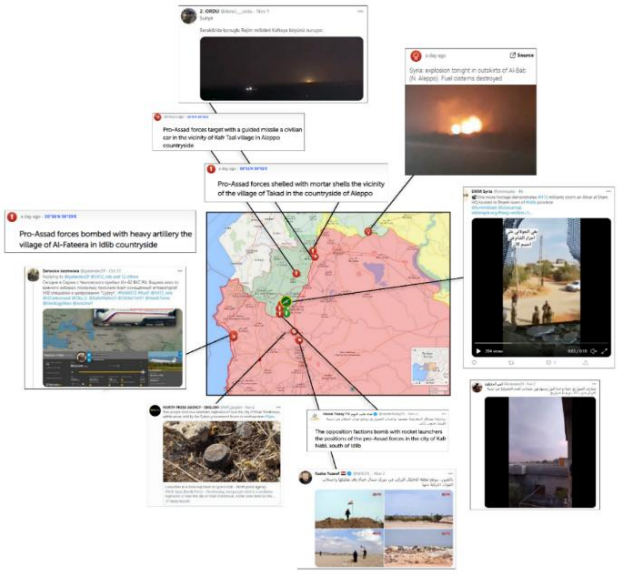

Рисунок Б.1 – Приклад карти Live Universal Awareness Map: Сирія, 3 листопада 2020 р. (рисунок створено автором за знімками екрана, зробленими з Live Universal Awareness Map)

Рисунок Б.2 – Розбита військова колона, що стрімко просувалася на Київ, розбили на вулиці Вокзальній

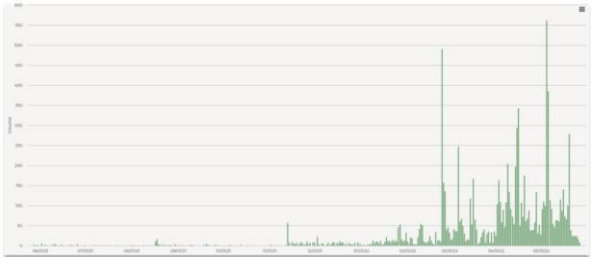

Рисунок Б.3 – Сплеск антиукраїнських повідомлень, поширених проросійськими мережами в соціальних мережах

Рисунок Б.4 – Категоріювання задокументованих ініціативою Т4р воєнних злочинів (взято із брошури з результатами роботи Т4р)

Рисунок Б.5 – Категоріювання задокументованих ініціативою Т4р воєнних злочинів (взято із брошури з результатами роботи Т4р)

Рисунок Б.6 – Розташування баз з військами рф (фото Maxar)

Рисунок Б.7 – Розширення військового табору у тимчасово окупованому Криму (фото Maxar)

Рисунок Б.8 – Колона російської військової техніки (фото Maxar)

Рисунок Б.9 – Місцезнаходження великого наметового табору для внутрішньо переміщених осіб на околиці Джабалії в Північній Газі, до операції Армії оборони Ізраїлю (Супутникові знімки Planet Labs)

Рисунок Б.10 – Місцезнаходження великого наметового табору для внутрішньо переміщених осіб на околиці Джабалії в Північній Газі, після операції Армії оборони Ізраїлю (Супутникові знімки Planet Labs)

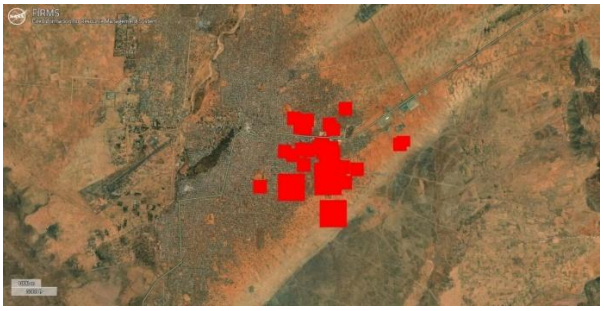

Рисунок Б.11 – Дані NASA FIRMS показують смуги теплових сигналів над східною частиною Аль-Фашира в період з 10 по 13 травня (Карта NASA FIRMS)

ДОДАТОК В

АНАЛІЗ OSINT МЕТОДІВ ТА ІНСТРУМЕНТІВ

Таблиця В.1 – Порівняння пасивного та активного методів OSINT

Критерій оцінки	Пасивний OSINT	Активний OSINT
Взаємодія з об’єктом дослідження	Немає прямого контакту з ціллю; збір вже опублікованих даних	Прямий контакт або вплив на ціль (сканування, комунікація)
Обсяг інформації	Обмежується загальнодоступними даними (публічні профілі, витоки, пости)	Може включати закриті дані, отримані шляхом взаємодії (відповіді систем, людей)
Непомітність	Висока – об’єкт, як правило, не дізнається про збір інформації	Низька – дії можуть бути зафіксовані (логи систем, сповіщення) і можуть видати розвідника
Юридичні ризики	Мінімальні, якщо дотримано законності (використання відкритих джерел)	Можливі порушення закону при несанкціонованому доступі чи введенні в оману; потрібна обережність
Приклади використання	Аналіз соцмереж, пошук у Google, перевірка DNS-записів, читання статей	Сканування портів і сервісів, фішингові листи для збору інформації, спілкування під виглядом іншої особи

Таблиця В.2 – Порівняльний аналіз популярних інструментів OSINT

Інструмент	Призначення	Інтерфейс	Переваги	Недоліки	Ефективність
SpiderFoot	Автоматизований збір даних з багатьох джерел	GUI або CLI	Багатозадачність, інтеграція з API (Shodan, HaveIBeenPwned)	Можливе зловживання даними	Висока (комплексний аналіз)
Maltego	Аналіз зв’язків, розвідка в соцмережах	Веб	Візуалізація даних у графіках, інтеграція з API	Складність, платна версія для повного	Висока (аналіз загроз)

				функціонал у	
Recon-ng	Збір даних про домени, субдомени	CLI	Гнучкість, модульність, підтримка активного сканування	Вимагає технічних знань	Висока (тестування на проникнення)
Shodan	Пошук IoT-пристроїв, сканування портів	GUI або API	Швидкий доступ до даних про підключені пристрої, геолокація	Не відкритий код, складний для новачків, може бути використаний зловмисниками	Висока (виявлення вразливостей)
Google Dorks	Пошук чутливих даних через запити	Веб	Доступність, швидкість виявлення вразливостей	Вимагає знання операторів, ручна обробка	Середня (виявлення витоків)
theHarvester	Збір email, субдоменів, IP	CLI	Простота, швидкість збору даних із пошукових систем	Обмежена глибина аналізу, можливе зловживання даними	Середня (початковий збір)
OSINT Framework	Колекція інструментів для збору даних	Веб	Систематизований підхід, широкий спектр методів	Не є окремим інструментом, залежить від якості інтегрованих засобів	Середня (універсальність)

BuiltWith	Аналіз технологій веб-сайтів	Веб	Швидке визначення CMS, плагінів, бібліотек	Обмежена сфера (лише веб-технології), платні функції	Середня (аналіз веб-вразливостей)
IntelligenceX	Архівування та пошук у витоках, даркнеті	Веб	Унікальний пошук за селекторами (email, IP), доступ до історичних даних	Платний доступ, етичні питання через чутливі дані	Висока (аналіз витоків)
HaveIBeenPwned	Перевірка витоків паролів, email	Веб	Простота, актуальна база витоків, сповіщення про домени	Обмежена функціональність, лише пасивний аналіз	Висока (захист від витоків)