КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.25.1950
УДК 316.776:004.58

Главацька Анастасія Любомирівна
студентка кафедри «Захист інформації»
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0009-0001-2975-8689
anastasiia.hlavatska.kb.2021@lpnu.ua

Ангельська Оксана Василівна
студентка кафедри «Захист інформації»
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0009-0004-4836-3772
oksana.anhelska.kb.2021@lpnu.ua

Опірський Іван Романович
д.т.н., професор, завідувач кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0000-0002-8461-8996
ivan.r.opirskyi@lpnu.ua

ДОСЛІДЖЕННЯ ТЕХНОЛОГІЇ ВИКОРИСТАННЯ OSINT ЯК НОВОЇ ЗАГРОЗИ З ДЕАНОНІМІЗАЦІЇ ОСОБИ В ІНТЕРНЕТ ПРОСТОРІ

Анотація. У цій статті здійснюється ґрунтовне дослідження технології Open Source Intelligence (OSINT), яка відіграє значну роль у сучасному інформаційному суспільстві, пропонуючи нові методи збору та аналізу даних. Особлива увага приділяється аналізу загроз, пов'язаних з деанонімізацією осіб через використання відкритих джерел інформації в інтернет-просторі. Використання OSINT дозволяє збирати величезні обсяги даних з різних джерел, таких як соціальні мережі, форуми, новинні сайти та інші публічні ресурси, що може порушувати приватність користувачів. Детально розглядаються методи збору інформації з відкритих джерел, які можуть бути використані для деанонімізації осіб. Аналізуються потенційні ризики для конфіденційності, що виникають внаслідок доступу до великої кількості персональних даних. Обговорюються різні аспекти загроз, включаючи можливості для шахрайства, маніпуляцій та навіть шантажу, що можуть виникати через збір і аналіз відкритих даних. Також розглядається, як особиста інформація, публікувана користувачами в інтернеті, може використовуватися зловмисниками для здійснення різних видів атак. Оцінюється ефективність існуючих інструментів OSINT, представлено методики та практичні приклади їх використання. Стаття містить рекомендації для покращення цифрової безпеки користувачів, включаючи вдосконалення технічних засобів захисту інформації та підвищення обізнаності громадян про цифрову грамотність. Розглядаються можливості розробки нових підходів до забезпечення цифрової безпеки, зокрема через вдосконалення законодавства та формування етичних стандартів для використання OSINT. Окрему увагу приділено нормативно-правовим аспектам використання OSINT в Україні. Аналізуються основні законодавчі акти, що регулюють збір та обробку персональних даних, а також етичні принципи, які повинні дотримуватися під час проведення OSINT-досліджень. Розглядаються приклади порушень прав на конфіденційність та правові наслідки таких дій. Стаття також висвітлює практичні аспекти використання OSINT у контексті війни в Україні. Показано, як технології OSINT використовуються для виявлення та аналізу діяльності зловмисників, відстеження пересування та планів ворога. Представлено приклади успішного використання OSINT для ідентифікації російських військових злочинців та розслідування воєнних злочинів. Мета цієї статті полягає в дослідженні можливостей OSINT як інструменту деанонімізації в інтернет-просторі, аналізі потенційних ризиків для приватності та розробці рекомендацій для покращення цифрової безпеки. Результатом дослідження стало визначення стратегій та рекомендацій, які можуть сприяти балансу між національною безпекою та правами людини в цифровому просторі.

Ключові слова: OSINT; деанонімізація; конфіденційність; персональні дані; цифрова безпека; методологія пошуку; OSINT-дослідження.

ВСТУП

У сучасному світі, де інформаційні технології прискорено розвиваються, з'являються нові методи збору та аналізу даних, які створюють багато можливостей для отримання знань. Одним з таких методів є OSINT (Open Source Intelligence), який використовує відкриті джерела для збору інформації. Хоча OSINT може служити корисним інструментом для досліджень і безпеки, він також представляє нову загрозу конфіденційності, дозволяючи деанонімізувати осіб в інтернет-просторі. Завдяки легкому доступу до величезної кількості інформації в інтернеті, індивіди та організації можуть використовувати OSINT для виявлення особистої інформації про людей без їхньої згоди і відому.

Такий збір інформації може мати серйозні наслідки для приватності, оскільки дозволяє виявляти не тільки базові особисті дані, але й зібрати детальну інформацію про особисте життя людей, їхні зв'язки, переваги та звички. Це відкриває широкі можливості для зловмисників, які можуть використовувати цю інформацію для шахрайства, маніпуляцій або навіть прямого шантажу.

Крім того, використання OSINT утруднює захист особистих даних, оскільки багато інформації публікуються самими користувачами в соціальних мережах, форумах та інших платформах. Це створює проблему для розробників систем безпеки, які намагаються знайти баланс між захистом приватності та свободою інформації.

У зв'язку з цим, визначення меж між необмеженим доступом до інформації та захистом приватності стає ключовим викликом для суспільства, законодавців, і технологічних компаній. Основна дилема полягає в тому, як забезпечити безпечний простір в інтернеті, де права осіб на конфіденційність будуть поважатися та захищатися, не обмежуючи при цьому свободу слова та доступ до відкритої інформації, яка може сприяти розвитку знань та інновацій.

В цьому контексті виникає необхідність розробки комплексних методологій та інструментарію, що дозволять ідентифікувати та мінімізувати ризики, пов'язані з використанням OSINT, а також розробки ефективних стратегій захисту даних. Це передбачає не лише вдосконалення технічних засобів захисту інформації, але й формування правової бази, що враховує сучасні виклики цифрової епохи, та зміцнення цифрової грамотності серед користувачів інтернету.

Постановка проблеми. В контексті стрімкого зростання кількості доступної інформації в інтернеті та посилення здатності інструментів OSINT до деанонімізації, виникає актуальна проблема захисту персональних даних особи. Питання конфіденційності та безпеки стають дедалі більш нагальними, а зростання випадків використання OSINT з метою деанонімізації вимагає розробки нових підходів та технологій для захисту особистої інформації.

Аналіз останніх досліджень і публікацій. Вже понад п'ятнадцять років в Україні відомий метод OSINT, який є засобом розвідки, використовуваним у всьому світі. Основу корисних даних, які збираються, часто складають відкриті джерела — до 90%. «Раніше основними відкритими джерелами слугували газети, радіо, телевізія та наукові публікації», — говорить Віталій Мороз, консультант у сфері цифрових технологій. Але з появою інтернету до цього переліку додалися соціальні мережі, форуми, онлайн-карти, вебсайти та обмін повідомленнями через месенджери. До відкритих джерел також

відносять державну та комерційну інформацію, включаючи урядові звіти, бюджети, фінансові аналізи та інше [1].

OSINT дозволяє збирати різноманітну інформацію про людей з загальнодоступних джерел, включаючи, але не обмежуючись, іменами, електронними адресами, домашніми адресами та геолокацією. Використання електронних пристроїв, таких як смартфони та фітнес-трекери, а також обмін особистою інформацією через соціальні мережі та інші онлайн-платформи роблять пошук особистої інформації в Інтернеті тривіальним завданням. Це може мати як позитивні, так і негативні наслідки в залежності від того, як така інформація використовується та в якому контексті вона ділиться. Більшість людей, ймовірно, будуть здивовані кількістю інформації про них, яку можна знайти в Інтернеті через загальнодоступні джерела. Важливість розуміння цих джерел, їх використання для суспільного блага і потенційні загрози для особистого життя стають очевидними в контексті OSINT [2].

До 2014 року в Україні OSINT використовувався переважно журналістами-розслідувачами. Російська збройна агресія значно поширила використання OSINT-технологій у світі та Україні, зокрема, сприяла заснуванню InformNapalm, «Миротворець» та популяризації Bellingcat після розслідування збиття MH17. Після 2014 року більшість українських журналістських розслідувань корупції активно застосовують OSINT, аналізуючи життя чиновників через соцмережі, відстежуючи приватні літаки та вивчаючи реєстри [3].

Важливо також перевіряти отриману інформацію і правильно аналізувати її, оскільки неперевірені дані можуть призвести до неправильних висновків та рішень. Особливо в контексті сучасних інформаційних воєн, де рефлексивний контроль використовується для маніпулювання перцепцією та діями супротивника, необхідно з великою обережністю підходити до аналізу інформації, отриманої з відкритих джерел. У цьому контексті, російсько-український конфлікт показав, що розвиток навичок критичного мислення і використання передових аналітичних інструментів може значно покращити якість аналізу відкритих даних і, відповідно, якість прийнятих на їх основі рішень [4].

Однак, ці зусилля стикаються з комплексною проблемою балансу між свободою інформації та правом на приватність. Публічні дебати та законодавчі ініціативи в різних країнах вказують на високий рівень суспільного інтересу до цього питання. «Різні агентства та компанії працюють відповідно до різних інструкцій, визначених їхніми керівними організаціями. Хоча ці правила можуть відрізнятися за формулюванням і нюансами, загальновизнано, що інформація, отримана з OSINT, повинна бути отримана таким чином, щоб не порушувати існуючі закони про конфіденційність, не повинна використовуватися в зловмисних цілях і повинна використовуватися лише за необхідності. означає досягнення мети», — попереджає Міністерство внутрішньої безпеки в документі відповідно до загальних принципів аналітиків [5].

У контексті цих викликів, майбутні дослідження у сфері OSINT та кібербезпеки повинні зосередитися на розробці етичних принципів використання відкритих даних, а також на створенні технологічних рішень, які можуть запобігти зловмисному використанню інформації без компрометації основних прав і свобод людини.

Мета статті — проаналізувати використання технологій Open Source Intelligence (OSINT) для деанонімізації осіб у цифровому середовищі та виявити основні ризики та загрози для конфіденційності, які цей процес може створити. Окрім цього, стаття має на меті визначити ефективні підходи та інструменти для захисту особистих даних, які можуть бути впроваджені для зменшення потенційних загроз, пов'язаних з використанням OSINT.

Основними завданнями статті є:

1. Аналіз потенційних ризиків для приватності, що виникають внаслідок використання OSINT.
2. Оцінка ефективності існуючих інструментів OSINT та методик їх використання.
3. Розробка рекомендацій для покращення цифрової безпеки користувачів.
4. Визначення потреби в нових підходах до забезпечення цифрової безпеки через вдосконалення законодавства та підвищення обізнаності громадян про цифрову грамотність.

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

Визначення OSINT та його місце серед інших джерел інформації.

OSINT (Open source intelligence) або іншими словами розвідка на основі відкритих джерел — це технологія, в основі якої лежить пошук, аналіз та використання політичної, військової, економічної та іншої інформації для прийняття рішень у сфері національної оборони та безпеки, розслідувань тощо [1].

Розвідка на основі відкритих джерел (OSINT) має довгу історію. Вона була задокументована ще в середині XIX століття в Сполучених Штатах Америки і на початку XX століття у Великій Британії [6]. Можна виділити декілька етапів:

1) кінець 1941 р. — створення у США Служби моніторингу іноземного мовлення (**Foreign Broadcast Monitoring Service — FBMS)** задля дослідження радіопрограм. Результатом роботи працівників цієї служби стало виявлення взаємозв'язку між вартістю апельсинів у Парижі та вдалим бомбардуванням залізничних мостів під час Другої світової війни;

2) 2005-2009 рр. — у США було створено центр із аналізу розвідувальних матеріалів з відкритих джерел. Відбулося це внаслідок зростання кількості інформації, що розміщувалась на просторах Інтернету;

3) 2009-2016 рр. — стрімкий розвиток Інтернету, його роль та вплив на людське життя;

4) 2016 р. – до тепер — введення концепції OSINT не лише в сферу оборони, але й в інші сфери життєдіяльності людини.

На рис. 1 коротко візуалізовано еволюцію розвитку OSINT.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023

ЕВОЛЮЦІЯ OSINT

Рис. 1. Еволюція OSINT

Сьогодні ж OSINT широко використовується у військовій сфері, для того щоб виявити потенційні загрози від ворогів, а також протидіяти терористичним організаціям.

У правоохоронних органах OSINT використовується для збору детальної інформації про порушників та їх злочинні діяння, що в більшій мірі пов'язані з Інтернетом. Особливо це легалізації коштів отриманих злочинним шляхом, боротьбі з розповсюдження наркотичних речовин, зброї тощо.

У сфері кібербезпеки, OSINT застосовується з метою виявлення таких кіберзагроз як фішингові атаки, розвідка і зломи, для пошуку та ідентифікації різного роду вразливостей та їх активній протидії.

Журналісти також користуються можливостями OSINT для дослідження та розкриття новинних історій, вивчення певного роду соціальних питань, дослідження громадської думки, виявлення корупції з використанням загальнодоступних декларацій про доходи, соціальних мереж тощо.

У бізнесі OSINT, безперечно, теж грає важливу роль. Адже він допомагає великим компаніям та організаціям проводити аналіз їхніх конкурентів та продуктів, знаходити нові можливості для розвитку їхнього бізнесу та слідкувати за новими тенденціями. Крім цього, застосування OSINT сприяє оптимізації маркетингових стратегій за рахунок глибшого розуміння цільової аудиторії та конкурентного середовища, що дозволяє знизити ризики прийняття невдалих рішень.

Будь-яка розвідувальна діяльність складається з розвідувального циклу, який відомий ще як механізм розвідувальної діяльності — це процес, що включає в себе п'ять складових [7]:

1. Планування і керування.
2. Життєвий цикл розвідки починається з оцінки потенційних загроз та визначення процесів, на яких вона буде зосереджена.
3. Збирання.

4. Після проведення попереднього оцінювання команда розвідки переходить до ідентифікації та збору відповідних даних. Ці дані включають в себе будь-які вільно доступні ресурси, такі як: новини, публікації в соціальних мережах і блоги тощо.
5. Обробка та експлуатація.
6. Перш ніж перейти до аналізу, групи розвідки перетворюють зібрані дані в єдину комплексну систему.
7. Аналіз.
8. Команда розвідки аналізує дані, отримуючи корисну інформацію для прийняття рішень та передбачення подальших подій.
9. Поширення та зворотній зв’язок.

Останнім кроком розвідувального циклу є представлення командою розвідки своїх висновків основним зацікавленим сторонам і надання рекомендації щодо вирішення проблем. Розглянувши висновки команди, зацікавлені сторони висловлюють власну думку та дають розгорнутий відгук щодо проробленої роботи. Обговорення триває доти, доки не буде прийнято рішення, яке влаштує всіх.

Отже, розвідувальний цикл об’єднує всі етапи розвідування інформації з метою її систематизації і подальшого використання.

На рис. 2 зображено діаграму розвідувального циклу [8].

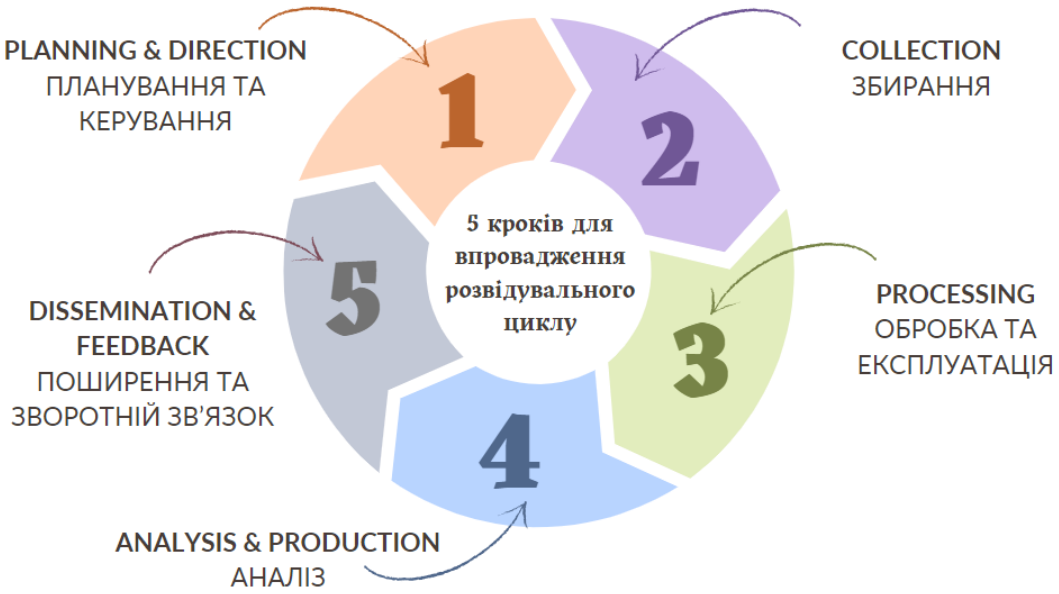

Рис. 2. Розвідувальний цикл

Розглянувши етапи розвідувального циклу, можна вбачити їх схожість з циклом Демінга, також відомим як PDCA (Plan-Do-Check-Act). Він базується на систематичному підході до управління, спрямованому на досягнення постійного вдосконалення процесів та результатів в організації.

У кінці 20-х рр. XX ст. Уолтер Ендрю Шухарт (англ. Walter Andrew Shewhart), усесвітньо відомий американський учений, консультант із теорії управління якістю, розробив концепцію статистичного управління процесами — СУП (SPC), яка ґрунтується на ідеї використання статистичних методів для скорочення варіацій навколо

цільового значення параметрів у процесі масового виробництва. Цю концепцію називають «цикл Шухарта».

Демінг Вільям Едвардс (Wílliam Édwards Déming) — американський учений, консультант із теорії управління якістю, трансформував «цикл Шухарта», додаючи до трьох етапів ще один — етап «перевіряй» (Check) або вивчай (Study), даючи більш загальні назви кожному з етапів. Саме тому цикл Шухарта-Демінга називають PDCA або PDSA [9].

До циклу PDCA входять 4 етапи, які зображено на рис. 3:

1. Планування (Plan). На цьому етапі визначаються мети та цілі, що мають бути досягнуті, розробляються конкретні стратегії, плани дій та методів, які будуть використовуватися для досягнення цих цілей.
2. Виконання (Do). Після розробки плану, наступний крок — це його виконання. Організація реалізує заплановані дії та ініціативи відповідно до визначених стратегій та планів.
3. Перевірка (Check). Після завершення виконання плану оцінюються отримані результати. Це включає перевірку того, чи були досягнуті поставлені цілі, і аналіз того, як ефективно були виконані заплановані дії.
4. Дія, Вплив, Управління (Act). На основі результатів оцінки приймаються рішення щодо подальших дій. Це може включати внесення коректив до планів, модифікацію стратегій або запуск нових ініціатив для покращення результатів.

Можна зробити висновок, що цикл Демінга — це, справді, безперервний процес, адже після завершення одного циклу вдосконалення, організація розпочинає наступний, використовуючи отримані результати для подальшого поліпшення.

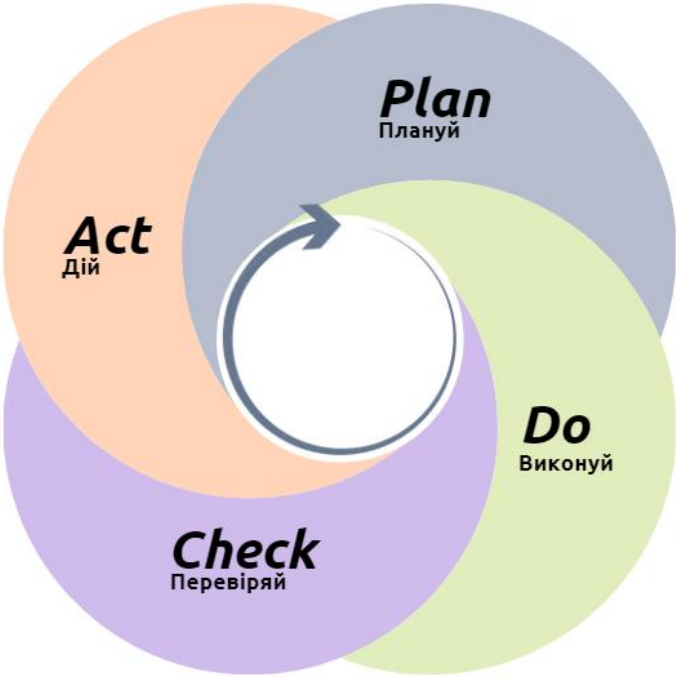

Рис. 3. Цикл Демінга

В табл. 1 наведено коротку порівняльну характеристику циклу Демінга та циклу розвідувальної діяльності.

Таблиця 1

Порівняння двох циклів

Характеристика	Цикл Демінга	Цикл розвідувальної діяльності
Мета	Постійне вдосконалення якості та ефективності продукції чи послуги.	Забезпечення національної безпеки, прийняття стратегічних рішень, шляхом збору та аналізу інформації.
Етапи	1. Планування (Plan): визначення цілей та стратегій; 2. 2. Виконання (Do): впровадження запланованих дій; 3. Перевірка (Check): оцінка результатів порівняно з цілями; 4. Дія за результатами перевірки (Act): корекція та поліпшення на основі отриманих результатів.	1. Планування і керування: визначення мети та цілі, що мають бути досягнуті, розроблення стратегії, плани дій та методів для досягнення цих цілей. 2. Збирання: ідентифікація та збір відповідних даних. 3. Обробка та експлуатація: перетворення зібраних даних в єдину комплексну систему. 4. Аналіз: аналіз даних для прийняття рішень та передбачення подальших подій. 5. Поширення та зворотній зв'язок: представлення висновків зацікавленим сторонам і надання рекомендації щодо вирішення проблем.
Застосування	У всіх сферах діяльності, де потрібне постійне поліпшення процесів та якості продукції чи послуг.	В розвідувальних агентствах, поліції, військовій сфері, дипломатичних службах для забезпечення національної безпеки та прийняття стратегічних рішень.
Процес	Цикл Демінга передбачає постійний ітеративний цикл вдосконалення, який застосовується для покращення якості продукції чи послуг шляхом систематичного аналізу та корекції.	Цикл розвідувальної діяльності передбачає систематичний процес збору, аналізу, інтерпретації та використання розвідувальної інформації для прийняття важливих рішень та забезпечення національної безпеки.

Розвідка з відкритих джерел (OSINT) має кілька переваг, які роблять її важливою у порівнянні з іншими методами збору розвідувальної інформації:

1) **Доступ до загальнодоступної інформації**: оскільки OSINT заснована на відкритих джерелах, які доступні для всіх. Тому будь-хто може отримати доступ до тієї чи іншої інформації без обмежень. Це означає, що організаціям не потрібно покладатися на засекречені або обмежені джерела інформації, отримання яких може бути дорогим і трудомістким.

2) **Різноманітні джерела**: дані, які можна знайти через OSINT, є різноманітними, оскільки їх можна зібрати з таких джерел як соціальні мережі, відкриті бази даних, новини, урядові звіти, наукові публікації тощо. Це дає можливість отримувати різноманітну та збалансовану інформацію з різних джерел.

3) **Швидкодія збору та аналізу інформації:** оскільки OSINT базується на загальнодоступній інформації, вона може бути зібрана швидко, в режимі реального часу, без необхідності складних процедур або довгих очікувань на дозвіл.

4) **Економічна вигода**: використання OSINT є економічно вигіднішим порівняно з іншими методами збору розвідувальної інформації, такими як використання людського інтелекту або спеціалізованих засобів розвідки. Це обумовлено тим, що OSINT

використовує доступні загальнодоступні джерела та не потребує великих витрат на дороге спеціалізоване обладнання.

5) **Прозорість:** концепція OSINT є прозорою з можливість легкої перевірки інформації. Організації можуть бути впевнені у точності та надійності цієї інформації, оскільки вони можуть самостійно перевірити її джерела походження і аналізувати достовірність отриманих даних.

Всі ці аспекти роблять OSINT надзвичайно цінним інструментом для широкого кола організацій, компаній та приватних осіб. Його економічна доступність, прозорість та можливість відносно легко перевірити інформацію дозволяють зробити обґрунтовані висновки на основі достовірних даних.

OSINT та інші напрямки розвідувальної діяльності

Спеціалісти з безпеки та аналітики виділяють шість основних способів для отримання розвідувальної інформації [10]:

- **Розвідка з відкритих джерел (OSINT)** — публічно доступна інформація, яка з'являється в джерелах, що не мають грифів таємності або обмежень доступу;
- **Агентурна розвідка (HUMINT)** — найстаріший спосіб збору інформації від її носіїв — інформація, зібрана з людських джерел;
- **Видова розвідка (IMINT)** — представлення об'єктів, що відтворюються в електронному або оптичному засобі на плівці, електронних дисплеях або інших носіях;
- **Радіоелектронна розвідка (SIGINT)** — перехоплення сигналів, чи то між людьми, між машинами або комбінацією обох;
- **Інструментальна розвідка (MASINT)** — розвідка фізичних полів, наукова і технічна розвідувальна інформація, що використовується для визначення, виявлення та опису специфічних ознак конкретних цілей;
- **Геопросторова розвідка (GEOINT)** — зображення та геопросторові дані, створені за допомогою інтеграції зображень та географічної інформації.

На рис. 4 зображено основні напрямки розвідувальної діяльності.

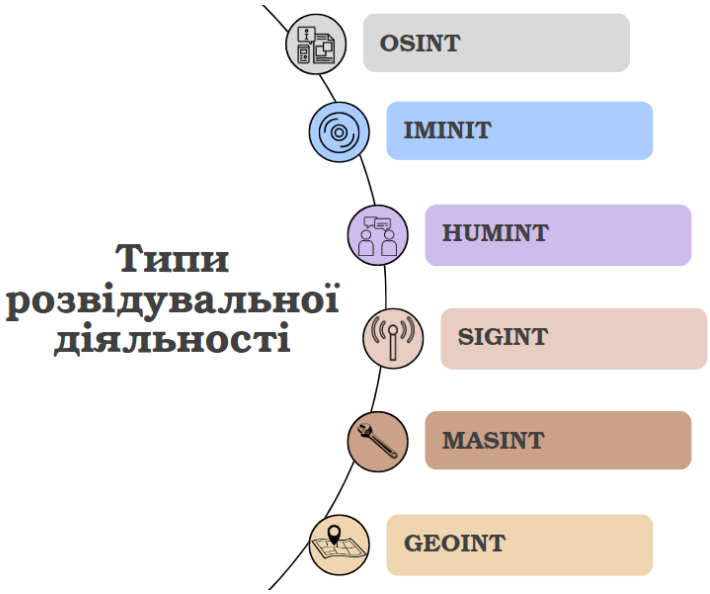

Рис. 4. Основні типи розвідувальної діяльності

В порівняльній характеристиці розвідувальних методів збору інформації, важливо розглянути їх переваги та недоліки для кращого розуміння їхнього потенціалу та обмежень у використанні. Кожен з цих методів має свої унікальні особливості, які роблять його важливим інструментом в сфері розвідувальної діяльності. .

В табл. 2 наведено детальний опис переваг та недоліків основних методів розвідувальної діяльності, які використовуються для збору інформації.

Таблиця 2

Порівняння основних методів розвідувальної діяльності

Метод	Переваги	Недоліки
OSINT	Легкий доступ до інформації, широке охоплення різноманітних джерел, можливість швидкого аналізу великих обсягів даних.	Обмеженість доступу до секретної або обмеженої інформації, можливість неправильного розуміння або тлумачення даних.
HUMINT	Доступ до внутрішньої інформації, можливість отримання конфіденційних даних, можливість взаємодії з джерелами для додаткового запитання або уточнення інформації.	Залежність від довірливості та надійності джерел, складність в обробці інформації, можливість зіткнення з етичними проблемами.
IMINT	Отримання візуальної інформації про об’єкти та місцевість, можливість використання для картографування та планування операцій.	Залежність від погодних умов і часу доби, обмеженість в точності та роздільній здатності зображень.
SIGINT	Можливість перехоплення комунікаційної інформації на великій відстані, великий потенціал для виявлення ворожих збройних сил та розвідувальних дій.	Складність аналізу великих обсягів даних, можливість перехоплення шумових або неповних сигналів.
MASINT	Додаткові джерела інформації через вимірювання фізичних параметрів об’єктів, можливість виявлення та аналізу невидимих аспектів.	Технічна складність у вимірюванні та аналізі даних, обмеженість в просторовій та часовій роздільній здатності.
GEOINT	Інтеграція зображень та географічних даних для розуміння обстановки на місцевості, великий потенціал для використання в геополітичних аналітичних операціях.	Обмеженість точності та доступності даних в певних регіонах, складність в аналізі великих обсягів геопросторових даних.

Дані концепції можуть застосовуватися як по-одинці, так і комбінуватися та доповнювати одна одну в тій чи іншій ситуації.

Наприклад, уявімо, що розвідувальна організація має завдання відстежити підозрілу діяльність терористичної групи в певному регіоні. Вони вирішили поєднати різні методи розвідки для досягнення цієї мети, зокрема:

1) OSINT (Open Source Intelligence) було використано для:

- аналізу соціальних мереж, форумів та інших вебсайтів, що допоможе у виявленні публічної інформації про можливі дії терористичної групи та її членів.
- перегляду відео- та фотоматеріалів, опублікованих в Інтернеті, які можуть містити важливі відомості про здійснення певних дій або злочинні активності.

2) HUMINT (Human Intelligence) застосовано для таких завдань:

- встановлення контактів з місцевими жителями або іншими джерелами, які можуть надати конфіденційну інформацію про діяльність терористичної групи.
- використання агентурних мереж для отримання конфіденційної інформації про плани та рухи терористів.

3) SIGINT (Signals Intelligence) впроваджено для:

- моніторингу електронних комунікацій, таких як телефонні дзвінки, SMS, електронні листи, щоб виявити зв'язки між членами терористичної групи.
- аналізу радіосигналів або інших електронних сигналів задля виявлення комунікаційніих зв'язків між ними.

4) GEOINT (Geospatial Intelligence) використано з метою:

- виявлення геопросторових даних, що допоможуть відстежити рух терористичної групи та визначити її можливі місця перебування або маршрути переміщення.

Отож, можна дійти висновку, що поєднання різних напрямів розвідувальної діяльності дозволило створити повну картину дій терористичної групи, відкриваючи можливості для запобігання потенційним терактам або затримання їх членів.

Кожна концепція має свої переваги, недоліки та обмеження, але їх комбінування може створити синергію та забезпечити комплексний аналіз тієї чи іншої ситуації.

Категорії відкритих даних, доступних для аналізу

Впровадження технологій та розвиток інформаційного суспільства перетворили відкриті дані на цінний ресурс, що сприяє процвітанню різних сфер діяльності, включаючи наукові дослідження, розвідувальну діяльність, аналіз ринків та забезпечення громадської безпеки.

За допомогою відкритих даних, доступних для аналізу OSINT-дослідники, аналітики, та розвідники мають можливість отримати об'єктивну та актуальну інформацію для прийняття важливих рішень.

У цьому контексті варто розглянути поширені методи OSINT, які активно використовують для збору інформації із загальнодоступних джерел [11]:

- **Аналіз соціальних мереж**: Включає в себе вивчення профілів та діяльності осіб на популярних соціальних мережах, таких як Facebook, Twitter, LinkedIn, Instagram та інші. Дослідники можуть отримувати важливу інформацію про особисті дані, зв'язки та інтереси.
- **Моніторинг новин та медіа**: Полягає в стеженні за новинами та медійними джерелами для отримання актуальної інформації про події, організації та особи.
- **Аналіз геоданих**: Використовує інформацію про трафік, місцезнаходження та геодані для відстеження подорожей і місць, де знаходяться особи.
- **Пошук у відкритих базах даних**: Включає в себе пошук в публічних базах даних, таких як телефонні каталоги, реєстри компаній, бази даних нерухомості та інші ресурси.
- **Вебскрапінг і аналіз вебсторінок**: Використовує автоматизований аналіз вебсторінок та вилучення інформації з вебсайтів та форумів.
- **Аналіз відео та аудіо засобами**: Для виявлення відео- та аудіозаписів, аналізу мови, звукових слідів та інших аудіовізуальних даних.

- **Використання відкритих інформаційних джерел**: Включає в себе перегляд публічно доступних документів, статей, звітів, книг та інших джерел інформації.
- **Пошук в архівах та базах даних**: Використовується для пошуку історичної інформації та архівних документів.
- **Моніторинг інтернет-форумів та соціальних обговорень**: Дослідники можуть відстежувати обговорення на форумах, в соцмережах та в інших онлайн-спільнотах для отримання інсайтів та аналізу глосаріїв.
- **Аналіз заголовків та метаданих файлів**: Завдяки цьому можна аналізувати інформацію, яка міститься в заголовках файлів, включаючи метадані фотографій та документів.

Проаналізувавши основні методи, які використовуються для збору інформації в OSINT можна зробити висновок, що у світі OSINT доступні різноманітні категорії відкритих даних, які можуть бути використані для аналізу.

Серед них першою є особиста інформація, до якої можуть відноситися рік народження, місце проживання, сімейний статус, освіта та професійний досвід. Ці дані дозволяють створити докладний профіль особистості та розкрити різні аспекти її життя, включаючи інтереси, зв'язки та пріоритети.

Другою категорією є географічні дані, такі як геолокація, точні місця перебування, маршрути подорожей тощо. Ці дані можуть бути використані для відстеження руху особи, вивчення її звичок або навіть виявлення потенційно небезпечних областей.

Крім того, відкриті дані також можуть містити інформацію про фінанси, банківські транзакції та інші аспекти, що можуть розкрити економічний статус та поведінку особи. Ці дані можуть бути корисними для аналізу фінансової стійкості, інвестиційних звичок або навіть виявлення потенційних шахраїв.

Отже, усі ці категорії даних представляють великий інформаційний потенціал для дослідження та аналізу в рамках OSINT. Тому важливо пильно ставитися до розголошення особистої інформації в мережі та ретельно вивчати наслідки її публікування. Адже, розуміння того, як ваші дані можуть бути використані проти вас, допоможе вам уникнути потенційних загроз і зберегти вашу приватність і безпеку в Інтернеті.

Методологія пошуку особи за допомогою OSINT

Збір відкритої інформації про особу може бути складним процесом, який вимагає обережності, суворого дотримання вимог конфіденційності та дотримання правових норм, а також принципів етики при проведенні даних досліджень. Слід також мати на увазі, що згідно з деякими правовими стандартами, збір інформації, яка відноситься до особистої інформації, може бути обмежено або регулюватися законодавством про захист даних. Тому важливо пам'ятати про дотримання вимог згідно з встановленими законами.

Етап 1. Визначення джерел та інструментів для пошуку

Перший крок у методології збору відкритих даних — це пошук різних джерел інформації. Це може бути пошук в Інтернеті, соціальних мережах, новинах, звітах, сайтах правоохоронних органів, державних сайтах тощо. Зараз на ринку існує багато засобів, які можуть використовуватися для пошуку і збору відкритих даних. До цих засобів відносяться: Google інструменти для пошуку (Google News, Google Alerts і т. д.), соціальні мережі, бази даних публічних реєстрів (Україна має публічний реєстр фізичних осіб та підприємців) та ін.

Етап 2. Систематичний збір даних

Систематичний збір даних є критичним етапом у зборі інформації про особу. Коли ви обрали джерела інформації і встановили критерії пошуку, ви можете розпочати пошук. Зважаючи на масштаб дослідження, важливо робити це систематично і зі структурністю, а не випадково, тому що можливість пропустити важливу інформацію велика.

Важливо дотримуватися певного порядку, щоб не пропустити чогось важливого. Почніть з популярних джерел інформації, таких як соціальні мережі, новинні портали або сайти, з яких ви знаєте, що вони можуть містити відомості про особу. Звертайте увагу на деталі, адже часто вони є ключовими. Наприклад, це може бути ім'я людини, її місце роботи або навчання, фотографії, рецензії, коментарі, та інше. На фото можуть бути назви магазинів, вулиць чи будь-які інші вказівники. Погода та одяг людей також може вказувати на пору року та час в який було зроблено фото.

Наступним етапом може бути звернення до джерел, які можуть містити певну категорію даних, наприклад, фінансові інформації або юридичні документи. Для цього можна використовувати публічні реєстри, бази даних компаній, архіви судових рішень та інше.

Етап 3. Обробка та аналіз інформації

Після того, як ви зібрали інформацію з різних джерел, ви можете почати аналізувати її. Одним із ключових елементів аналізу інформації є встановлення її достовірності. Зверніть увагу на джерело інформації та на те, які дані воно містить, щоб визначити його надійність.

Важливо також враховувати контекст, у якому була отримана інформація. Наприклад, якщо інформація надходить з відомих та достовірних джерел, таких як офіційні джерела, то вона може бути довіреною. Але якщо ця інформація з'явилася на сайті, який спеціалізується на «сенсаційних» новинах, то її може бути важко підтвердити.

Також зверніть увагу на дату публікації інформації. Інформація, яка була опублікована більше року тому, може бути застарілою, і можуть бути зміни в особистому житті чи ситуації. Після оцінки інформації ви можете почати аналізувати її та виходити на висновки.

Етап 4. Створення звіту

На заключних етапах, після збору і аналізу даних, ви можете створити звіт або аналітичний звіт на основі зібраної інформації, що допоможе вам вирішити ваші завдання.

На рис. 5 зображено блок-схему послідовності етапів пошуку особи.

ISSN 2663 - 4023

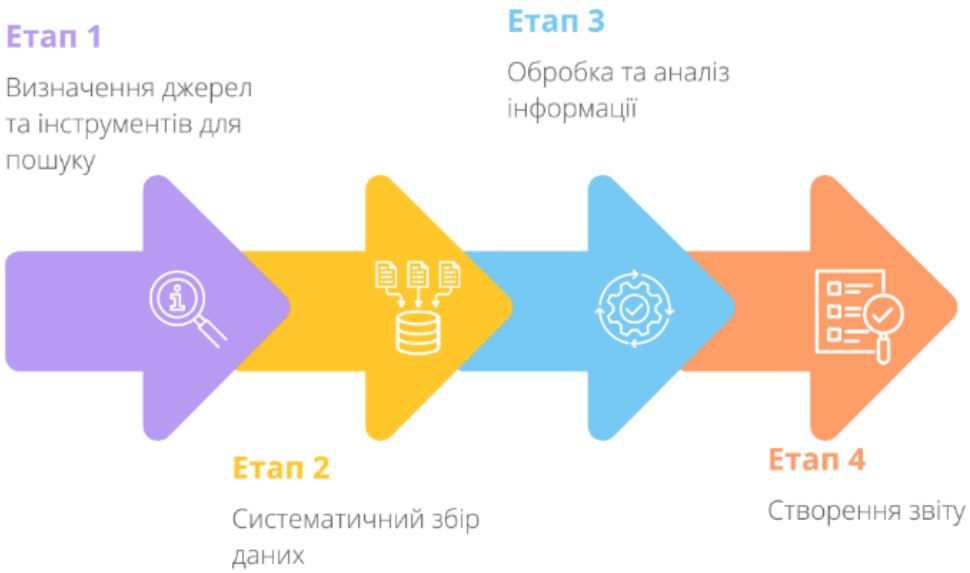

Рис. 5. Етапи пошуку особи

Ці етапи можна інтерпретувати як циклічний процес, оскільки на етапі збору відкритої інформації про особу можуть виникнути нові висновки або додаткові запитання, які вимагатимуть подальшого дослідження або перевірки. Наприклад, після аналізу попередньо зібраної інформації може з'явитися новий напрямок для пошуку, або може стати очевидним, що певні джерела потребують більш докладного дослідження.

Для збору інформації про особу доступно безліч інструментів і ресурсів. Деякі з них засновані на технологіях інтернету, таких як пошукові системи, соціальні мережі, а також спеціалізовані програми та платформи для збору та аналізу даних. Інші — це традиційні джерела інформації, такі як публічні записи, документи, звіти та архіви.

Пошукові системи: Google, Bing, Yahoo.

Соціальні мережі: Facebook, Twitter, LinkedIn, Instagram, TikTok тощо.

Спеціалізовані платформи та інструменти: Maltego, OSINT Framework, Hunchly, SpiderFoot тощо.

Публічні ресурси: Урядові сайти, сайти місцевих адміністрацій, законодавчі бази даних, сайти публічних реєстрів тощо.

Додатково, важливо враховувати правові обмеження, конфіденційність особистих даних та етичні питання. Необхідно дотримуватися законодавства про захист даних та зважати на вимоги конфіденційності та приватності при використанні таких інструментів.

Практичні аспекти використання OSINT

Пошук в соціальних мережах є ключовим елементом в OSINT (Open Source Intelligence) дослідженнях, який дозволяє збирати дані та інформацію з відкритих джерел для вирішення різноманітних задач, від приватних розслідувань до аналізу конкурентів у бізнесі.

Далі розглянемо, які засоби та методи можна використати у таких соціальних мережах: Instagram, Facebook, TikTok.

ISSN 2663 - 4023

Instagram

Instagram пропонує низку інструментів та функцій, які дозволяють користувачам публікувати контент, взаємодіяти з аудиторією та аналізувати ефективність своїх публікацій.

Розглянемо спочатку засоби графічного інтерфейсу Instagram.

У контексті OSINT, графічний інтерфейс Instagram надає користувачам можливість здійснювати глибокий аналіз профілів, публікацій, історій, та інших елементів контенту без використання додаткових інструментів. Далі буде наведено важливі аспекти та засоби графічного інтерфейсу Instagram.

Профіль користувача

Аналізуємо профіль. Це дозволяє отримати загальну інформацію про користувача, включаючи біографію, посилання, кількість підписників, підписок та публікацій. Аналізуючи профілі, можна ідентифікувати потенційні інтереси, зв'язки та діяльність особи в мережі.

Вивчаємо публікації та взаємодії. Вивчення публікацій користувача, коментарів, вподобань та взаємодії з іншими користувачами може надати цінну інформацію про соціальний круг, інтереси та поведінку.

Історії (Stories) та Reels

Stories — це тимчасовий контент, який зберігається 24 години, може містити показники активності, місцезнаходження, опитування та інші важливі дані.

Відео Reels на Instagram може бути дуже цінним джерелом для OSINT досліджень, оскільки вони містять багато різноманітної інформації.

Пошук

Функція пошуку дозволяє шукати конкретні хештеги, локації та користувачів, що може бути корисно для визначення даних та зв'язків.

Але інколи це не дає повної та вичерпної інформації. Саме тут на допомогу приходить «Переглянути джерело сторінки». За допомогою цього методу можна дізнатись точний час (до секунд) коли був опублікований пост, коментар та id користувача.

Отже, відкриваємо профіль «жертви» у браузері, обираємо пост (можна той, який найбільше цікавить чи будь-який) та клікаємо правою кнопкою миші на будь-яке пусте місце (це зображено на рис. 6) та обираємо пункт «Переглянути джерело сторінки».

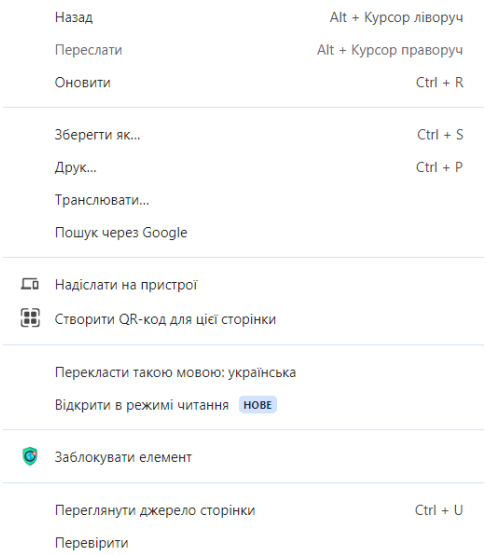

Рис. 6. Перегляд джерела сторінки

Ми побачимо сторінку з купою коду. Далі натискаємо cnrl+f (або ж command+f) і вводимо у строку пошуку слово owner. Серед заданих варіантів шукаємо той, який виглядатиме приблизно так "owner":{"pk". Число біля «pk» — це ідентифікатор користувача в інстаграмі.

Далі повертаємось до рядку пошуку і вводимо created_at. Довге число біля це Час Unix чи час POSIX. Це спосіб відстежувати час як загальну кількість секунд. Цей відлік починається в епоху Unix 1 січня 1970 року за UTC [12]. Щоб перевести цей час в звичний формат, заходимо на сайт https://www.unixtimestamp.com/ та вводимо число і отримуємо точний час та дату публікації поста. Те саме ми можемо отримати, якщо клікнемо правою кнопкою миші на коментарі.

Існують також сайти, які допомогають скачати зображення профілю, постів, сторіс. Наприклад, https://www.save-free.com/. Цей сайт допомагає скачати зображення профілю навіть приватного акаунту. Далі можна скористатись пошуком по фото. Також цей сервіс дозволяє скачати фото з поста, рілс та сторіс. Також є сервіси, які дозволяють переглянути чи зареєстрований користувач з таким нікнеймом в інших соц мережах. Наприклад, https://whatsmyname.app/.

Facebook

Якщо говорити у контексті такої соціальної мережі як Facebook, то варто зазначити, що ця мережа має досить «скандальне минуле». Загалом були такі випадки як, продаж даних стороннім компаніям і витік інформації через плагіни. У липні 2019 року, компанія Facebook отримала рекордний штраф у розмірі 5 мільярдів доларів від Федеральної торгової комісії США за витік особистих даних користувачів [13]. Марк Цукерберг був зобов'язаний особисто підтвердити, що компанія дотримується всіх вимог щодо захисту даних, загрожуючи адміністративною або кримінальною відповідальністю у випадку недостовірної інформації. У листопаді 2019 року, Facebook визнала новий витік даних, коли близько 100 розробників додатків отримали доступ до приватної інформації користувачів, попри заборону, і запросила розробників видалити зібрані дані. Протягом 2020–2021 років, дані 533 мільйонів користувачів Facebook, зібрані зловмисниками у 2019 році, з'явилися спочатку на форумах для продажу, а потім у відкритому доступі, через використання вразливості, яка дозволяла збирати особисті дані користувачів.

Через проблеми з безпекою найбільше цінних методів пошуку у цій соціальній мережі зникли у 2019 році. Проте багато користувачів самі викладають достатньо інформації у своїх профілях. Зокрема, ось основні категорії інформації, які можна знайти:

- Особисті дані: Ім'я, вік, стать, дата народження, мови, якими володіє користувач, стосунки (сімейний стан), релігійні та політичні переконання, освіта та місце роботи.
- Контактна інформація: Електронна пошта, номер телефону, адреса проживання (якщо вказано).
- Інтереси та вподобання: Музика, фільми, книги, телевізійні шоу, групи, заходи, які користувач вподобав або підписався.
- Друзі та зв'язки: Список друзів, їхні фотографії, відносини та спільні інтереси, запрошення в друзі, які були відправлені чи отримані.
- Публікації та активність: Статуси, фотографії, відео, місця, які відвідував та ін.

Важливо зауважити, що доступ до багатьох з цих даних обмежений налаштуваннями приватності користувача. Користувачі можуть контролювати, хто

бачить їхні публікації, особисті дані, список друзів, тощо. Facebook також пропонує інструменти для перегляду та управління даними, які він збирає про користувачів.

Важливо також зазначити, що пошукова стрічка Facebook надає користувачам потужний інструмент для пошуку різноманітної інформації та контенту всередині соціальної мережі. Ось деякі з основних можливостей пошукової стрічки:

- Пошук людей. Можна шукати користувачів за їхнім ім'ям, прізвищем, електронною поштою або іншими ідентифікаторами. Це дозволяє швидко знайти профілі друзів, колег або знайомих.
- Групи. Можливість знаходити групи за інтересами, тематиками або ключовими словами. Це включає закриті та секретні групи, до яких можна подати запит на вступ.
- Події. Можна шукати події за назвою, датою, місцезнаходженням або організатором. Можна виявити заходи, які відбуватимуться навколо вас, або знайти заходи, які відповідають вашим інтересам.
- Стрічки новин. Пошук новинних статей, публікацій та іншого контенту, який поділяється у Facebook, за ключовими словами або фразами.
- Фотографії та відео. Відшукання фотографій та відеоматеріалів, опублікованих користувачами або сторінками, за ключовими словами, темами або мітками.
- Бізнес-сторінки та місцеві підприємства. Пошук сторінок компаній, місцевих підприємств, ресторанів, магазинів тощо за назвою або категорією.
- Хештеги. Можливість шукати публікації за хештегами, що дозволяє знаходити контент на певні теми або тенденції.
- Розширений пошук. Використання розширених фільтрів для звуження результатів пошуку за датою публікації, типом контенту, географічним положенням тощо.
- У цій соціальній мережі також можна дізнатись id профілю користувача. Для цього відкриваємо профіль користувача у браузері, клікаємо правою кнопкою миші на будь-яке пусте місце та обираємо пункт «Переглянути джерело сторінки».

Ми побачимо сторінку з купою коду. Далі натискаємо cnrl+f (або ж command+f) і вводимо у строку пошуку слово profile_id. Шукаємо той, який виглядатиме приблизно так "owing_profile_id":. Також ідентифікатор користувача можна дізнатись за допомогою сервісу https://lookup-id.com/.

У період з квітня по грудень 2009 року Facebook змінив формат ідентифікаторів користувачів з 32-розрядних чисел на 64-розрядні, починаючи з числа 100 000. Якщо номер вашого облікового запису менший за 100000000000000, ймовірно, він був створений до квітня 2009 року. Облікові записи з 15-значним ідентифікатором були, мабуть, створені після грудня 2009 року. Ці оцінки можуть бути використані як загальні орієнтири для визначення часу створення облікового запису [14].

2006: Число менше 600400000
2007: 600400000–1000000000
2008: 1000000000–1140000000
2009: 1140000000–100000628000000
2010: 100000629000000–100001610000000
2011: 100001611000000–100003302000000
2012: 100003303000000–100004977000000
2013: 100004978000000–100007376000000

2014: 100007377000000–100008760000000
2015: 100008761000000–100010925000000
2016: 100010926000000–100014946000000
2017: 100014947000000–100023810000000
2018: 100023811000000–…

TikTok

TikTok, подібно до Instagram, пропонує багато інструментів та функцій, які дозволяють користувачам публікувати контент, взаємодіяти з аудиторією та аналізувати ефективність своїх публікацій. Розглянемо засоби графічного інтерфейсу TikTok у контексті OSINT (Open Source Intelligence), який надає можливість здійснювати глибокий аналіз профілів, відео, взаємодій між користувачами, та інших елементів контенту без використання додаткових інструментів.

Профіль користувача

Аналіз профілю на TikTok може виявити важливу інформацію про користувача, включно з біографією, посиланнями, кількістю підписників, підписок, лайків та відеопублікацій. Це дозволяє ідентифікувати потенційні інтереси, соціальні зв'язки та діяльність особи в мережі.

Відеопублікації та взаємодії

Вивчення відеопублікацій користувача, коментарів, лайків, та взаємодії з іншими користувачами на TikTok може надати цінну інформацію про соціальний круг, інтереси, та поведінку. Користувачі також можуть поширювати відео, і завдяки цим пошиерння, можна дізнатись багато цікаво про інтереси та життя людини.

Пошук

Функція пошуку на TikTok дозволяє шукати конкретні хештеги, відео, користувачів та звукові доріжки, що може бути корисно для визначення даних та зв'язків.

Додаткові інструменти

Аналіз тенденцій. TikTok відомий своїми трендовими челенджами та звуками, аналіз яких може надати інформацію про популярність певних тем або інтересів серед широкої аудиторії.

Duets і Зшивання. Ці функції дозволяють користувачам взаємодіяти з іншими відео, створюючи спільний контент, що може вказувати на зв'язки між користувачами.

Зовнішні інструменти

Завантаження відео. Існують вебсайти та програми, які дозволяють завантажувати відео з TikTok, що може бути корисним для детального аналізу або архівування контенту.

Точний час публікації. Існують сервіси, які допомагають визначити точний час публікації відео з точністю до секунд. Наприклад, https://bellingcat.github.io/tiktok-timestamp/

Перевірка наявності користувача в інших соцмережах. Інструменти, подібні до https://whatsmyname.app/, можуть допомогти перевірити, чи зареєстрований користувач TikTok під таким же або схожим нікнеймом в інших соціальних мережах.

https://mavekite.com/ допомагає збирати дані про лайки, коментарі, описи відео і т. д. Створює своєрідний звіт про профіль.

Візуалізація процесу пошуку: від ідентифікації цілі до аналізу отриманої інформації

Для візуалізації процесу використання OSINT (Open Source Intelligence) можна створити блок-схему, яка демонструватиме послідовність кроків для збору відкритих даних про особу, організацію чи подію. Процес можна порівняти з розв'язанням детективної головоломки, де кожен крок веде нас ближче до розкриття «таємниці».

Алгоритм використання OSINT

1. Визначення цілі:

Початок розслідування схожий на встановлення маяка у тумані, що допоможе нам зорієнтуватися у величезному океані інформації.

2. Планування:

Цей крок можна порівняти з кресленням карти, яка допоможе нам знайти найкоротший шлях до маяка, враховуючи всі можливі перепони та об'єкти, що цікавлять.

3. Збір даних:

Тут ми вирушаємо в подорож, використовуючи різні засоби і транспорт (пошукові системи, соціальні мережі, спеціалізовані бази даних), щоб зібрати необхідні відомості.

4. Аналіз даних:

На цьому етапі ми стаємо як археологи, що намагаються відтворити історію з зібраних фрагментів, виявляючи зв'язки та встановлюючи факти.

5. Верифікація і валідація:

Схоже на перевірку якості виробу перед тим, як представити його світові, щоб переконатися, що вся інформація точна та надійна.

6. Звітування:

Останній крок — це мистецтво розповіді, де ми передаємо наші відкриття аудиторії, забезпечуючи чіткі та зрозумілі відповіді на поставлені запитання.

Давайте тепер перейдемо до створення блок-схеми, щоб візуально представити цей алгоритм.

На рис. 7, власне, представлена блок-схема алгоритму використання OSINT.

Дотримання етичних принципів та правил у OSINT-дослідженнях

При використанні відкритих даних у контексті розвідки OSINT важливо дотримуватися ряду правил та принципів. Це включає збір, обробку та аналіз інформації, дотримання законодавчих обмежень і етичних норм. Крім того, слід звертати увагу на перевірку достовірності інформації та використання її лише там, де це справді необхідно. Додатково, потрібно враховувати особливості та обмеження різних джерел інформації, щоб забезпечити якість та точність отриманих даних.

Основним принципом використання OSINT-методик для організацій, компаній чи фізичних осіб є збір інформації з дотриманням законів та правових норм. Важливо усвідомлювати, що незаконний збір інформації є недопустимим і може призвести до кримінальної відповідальності. Тому рекомендується керуватися нормативно-правовими актами, що регулюють процеси збору/обробки персональних даних, а також права на інтелектуальну власність.

Достовірність інформації є ще одним ключовим аспектом будь-якої розвідувальної діяльності, особливо в контексті OSINT. Під час збору інформації вкрай важливо мати впевненість у її точності та надійності, оскільки від цього залежить правильність висновків та прийнятих рішень. Необхідно переконатися в авторитетності джерел, вміти порівнювати та перевіряти інформацію з різних джерел, а також виділяти найважливіше.

ISSN 2663 - 4023

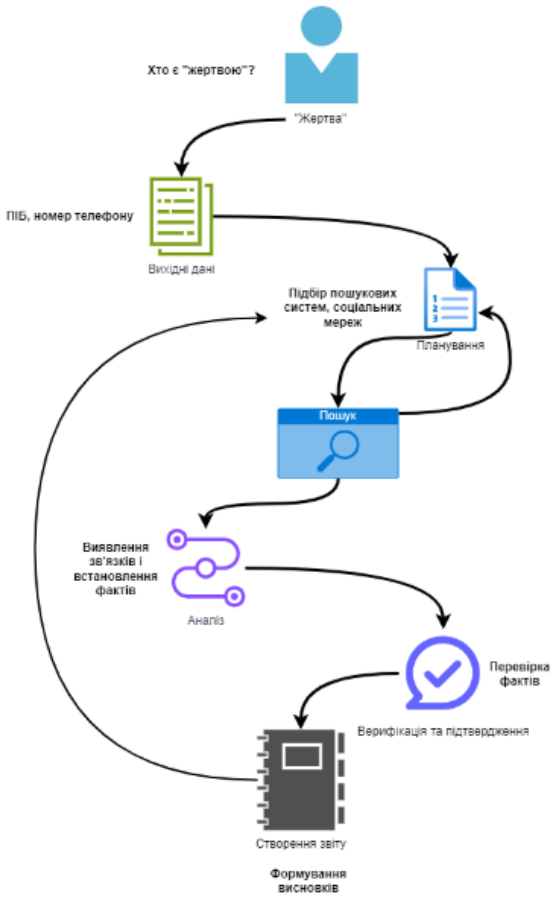

Рис. 7. Блок-схема алгоритму використання OSINT

Забезпечення ефективного та відповідального використання OSINT-методик починається з компетентних осіб, які володіють необхідними знаннями та навичками. Важливо, щоб ці особи розуміли контекст та потреби дослідження. Вони повинні керуватися етичним підходом до збору та використання інформації, а також дотримуватися законодавства та правил конфіденційності даних.

Отже, успішне використання OSINT-методик є багатоаспектним процесом, який потребує постійного вдосконалення знань та навичок, а також врахування етичних міркувань та відповідних правил.

Нормативно-правові аспекти використання OSINT в Україні

Використання відкритих джерел інформації (OSINT) у сучасному світі стає все більш важливим і розповсюдженим. Збір та аналіз інформації з відкритих джерел може використовуватися для різноманітних цілей, включаючи розвідувальну діяльність, безпеку мережі, дослідження кіберзлочинів, аналіз ринку та інше. Проте важливо пам’ятати, що ця діяльність повинна відбуватися в рамках нормативно-правового поля країни, дотримуючись встановлених правил і законів.

В Україні використання відкритих джерел інформації (OSINT) регулюється низкою нормативно-правовиз актів. Серед них основними є Конституція України, Закон України «Про захист персональних даних», Кодекс України про адміністративні правопорушення, Кримінальний кодекс України та Цивільний кодекс України.

Відповідно до Конституції України, кожна особа має право на захист своєї гідності, честі, приватного життя, інтимної та сімейної таємниці. Це означає, що збір, обробка та

використання персональних даних без згоди їх власника є незаконними та можуть порушувати права людини. Саме тому, організації зобов'язані гарантувати безпеку особистих даних, збирати їх лише з визначеною метою, зберігати обмежений проміжок часу та надавати особам можливість відмовитися від збору їхніх особистих даних.

Якщо не дотримуватися етичних міркувань у OSINT-дослідженнях, наприклад таких як виявлення поваги до приватного життя інших людей, дотримання відповідних законів і правил, а також забезпечення того, щоб отримана інформація використовувалася виключно в законних цілях, то можуть бути порушені такі статті Конституції України [15]:

- Стаття 31: Кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції.
- Стаття 32: Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.
- Стаття 34: Кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань.

У Кримінальному кодексі України теж містяться статті, що передбачають відповідальність за розголошення та збір інформації, що є державною або службовою таємницею. Крім того, відповідно до цього кодексу, неправомірне збирання та обробка персональних даних, які порушують вимоги законодавства, можуть бути кваліфіковані як порушення прав людини.

Нижче наведено приклади статей Кримінального кодексу України, які можуть бути порушені при невідповідному застосуванні OSINT-методик [16]:

- Стаття 182: Порушення недоторканності приватного життя. Дана стаття передбачає відповідальність за незаконне збирання, використання та поширення конфіденційної інформації, в тому числі шляхом їх отримання з використанням концепцій OSINT.
- Стаття 361: Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Незаконний доступ до комп'ютерних матеріалів, що зберігаються у комп'ютерних системах або мережах, зокрема з використанням методів OSINT також може бути кваліфіковано як злочин.

Ще один з аспектів використання OSINT, на який необхідно звернути увагу, це авторське право. При зборі, аналізі чи використанні даних з відкритих джерел, до яких належать інтернет-ресурси, соціальні мережі чи публічні бази даних, важливо дотримуватися авторських прав на ці дані. Не дозволено копіювати та використовувати ці дані у власних інтересах та без згоди їх власників.

Отже, найкращим підходом до використання OSINT-методик є дотримання правових норм та етичних принципів. Важливо збирати лише ту інформацію, яка є відкритою та доступною для загального використання; необхідно дотримуватися правил збору та обробки персональних даних. А також пам'ятати про те, що збір та використання інформації з метою нанесення шкоди іншим особам може бути кваліфіковано як злочин і мати серйозні наслідки.

OSINT та війна в Україні

В епоху загострених конфліктів та інформаційної війни технологія OSINT виявилася неоціненною зброєю, що розкриває образи беззаконня та порушень прав людини.

Війна, яку розв'язала росія проти України, додала новий аспект в розумінні можливостей OSINT. Якщо раніше розвідка з відкритих джерел використовувалась для вирішення цивільних питань і мирних цілей (корпоративної безпеки, бізнесових досліджень), то зараз OSINT — важливий інстрмент у ході війни [17].

Завдяки методам OSINT, українські військові можуть відстежувати пересування, плани та операції рашистів. Супутникові знімки надають інформацію про райони, атаковані російськими військами. Незашифровані радіохвилі та мобільні телефони дозволяють ЗСУ прослуховувати російські повідомлення. Повідомлення в соціальних мережах як від російських солдатів, так і від громадян України показали, як виглядає війна на місцях, давши українським офіційним особам інформацію про те, де і як діють російські збройні сили. Ці переваги, що дає OSINT, дозволили Україні кинути серйозний виклик росії [18].

На допомогу Україні у боротьбі проти ворога, прийшло багато OSINT-спільнот, зокрема до них належать:

● Аґенція Molfar, яка надає послуги приватної розвідки у більше ніж 39 країнах світу ще з 2019 року. Вона займається ідентифікацією російських воєнних злочинців, воєнними розслідуваннями та воєнною аналітикою.

Одне з важливих завдань Molfar — робота з західною аудиторією. Масштаби та бюджети, які виділяє російська федерація на закордонну пропаганду — гігантські. Саме тому кожне розслідування Molfar намагаються запропонувати західним журналістам.

Серед інших засобів боротьби з ворожими інформаційними вкидами — збір реєстру закордонних пропагандистів. Так само як і реєстрів українських зрадників та ворогів — спільнота збирає та документує докази. На рис. 8 зображено вкладку «Вороги України» з вебсайту Molfar.

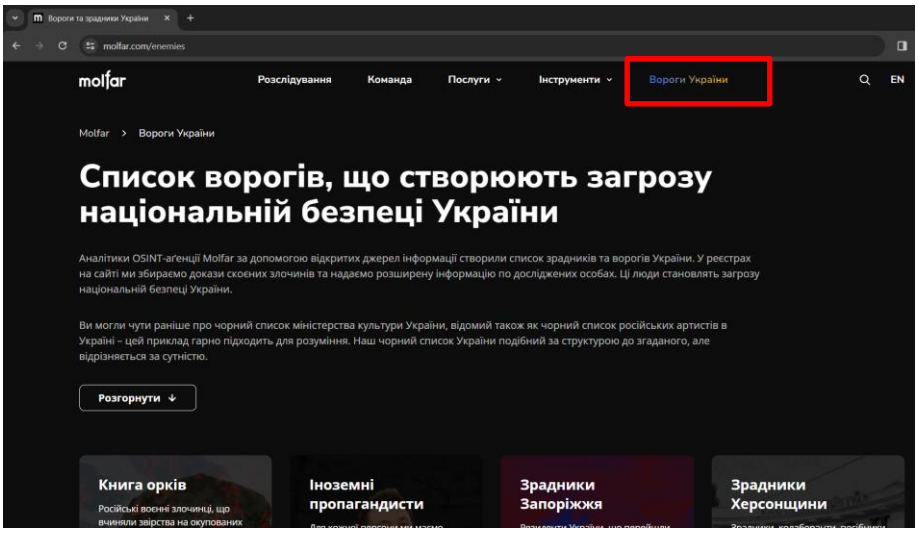

Рис. 8. Список ворогів України за дослідженнями агенції Molfar

Крім досліджень, спеціалісти Molfar навчають військовій OSINT-аналітиці фахівців Національної академії СБУ, Держприкордонслужби, Міністерства оборони України і представників громадських організацій [19].

ISSN 2663 - 4023

● Bellingcat — незалежний міжнародний колектив дослідників, слідчих і громадянських журналістів, які використовують відкриті джерела та соціальні мережі для розслідування різноманітних тем — від злочинів проти людства, до відстеження використання хімічної зброї та конфліктів у всьому світі [20].

У контексті війни в Україні міжнародна група незалежних журналістів Bellingcat на основі відкритих даних (фото, відео, записів перемовин) виявили можливих причетних до збиття рейсу МН-17 «Малазійських авіаліній» у липні 2014 року [1].

Також з 24 лютого 2022 року Bellingcat збирає дані про випадки пошкоджень і руйнувань цивільної території та інфраструктури, а також загибель мирного населення. Всю цю інформацію розміщено на інтерактивній карті, вигляд якої можна побачити на рис. 9 [21]. Кожен може досліджувати інциденти за датою та місцем розташування.

● Волонтерський проєкт — InformNapalm виник у відповідь на російську агресію в Україні ще у березні 2014 року.

Від початку війни дана організація займається підготовкою ґрунтовних досліджень російської збройної агресії проти України. Зокрема, ідентифікує російських військовослужбовців, які беруть участь у гібридних війнах, розв'язаних росією в інших країнах, включно з їхніми військовими званнями та частинами, до яких вони належать; викриває факти незаконного експорту росією зброї та військової техніки; збирає докази, що підтверджують участь російських урядовців і громадських діячів у плануванні підривних операцій і веденні воєн на території інших держав; аналізує та прогнозує військово-політичної ситуації в Центральній, Східній Європі та на Близькому Сході; розвінчує брехню російської пропаганди [22].

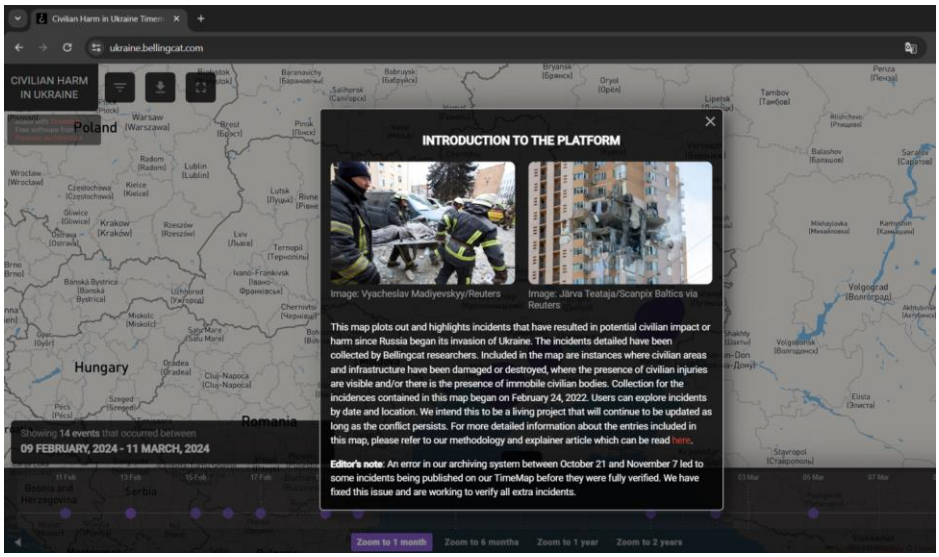

Рис. 9. Інтерактивна карта для дослідження випадків пов'язаних з війною в Україні

Отож, OSINT в Україні відіграє важливу роль у підтримці фронту під час війни. Це включає такі основні аспекти, як [23]:

1) Виявлення рухів ворожих військ. Збір інформації про рух ворожих військ, їхню кількість та розташування допомагає військовим командирам приймати обґрунтовані рішення та своєчасно реагувати на загрози.

2) Аналіз тактики і стратегії ворога. OSINT допомагає виявити тактику та стратегію ворога, що дає можливість українським військовим адаптувати свої дії для ефективного протистояння.

3) Збір інформації про зброю і техніку. Аналіз відкритих джерел дозволяє виявляти та відстежувати рух військової техніки та зброї ворога, а також визначати нові типи зброї, які вони можуть використовувати.

Цифровий слід та OSINT

Кожен користувач Інтернету залишає після себе відбиток, відомий як цифровий слід. Це може включати відвідування вебсайтів, пошукові запити, коментарі в соціальних мережах та інше.

В контексті OSINT, цифровий слід можна активно використовувати для збору і аналізу інформації про користувачів з відкритих джерел, таких як публічні профілі в соціальних мережах, публічні форуми та блоги. Цей аналіз допоможе зрозуміти поведінку користувача, його вподобання та інтереси, що може бути важливим для різних цілей, включаючи забезпечення кібербезпеки, виявлення та розслідування злочинів, оцінку громадської думки, проведення маркетингових досліджень тощо.

Також варто розрізняти цифровий слід, адже він буває активним та пасивним [24].

Активний цифровий слід базується на взаємодії між браузером користувача та вебресурсом. Тобто користувач залишає активний цифровий слід, коли навмисне ділиться інформацією про себе: робить публікації в соціальних мережах, залишає повідомлення на сайтах чи онлайн-форумах. Активні цифрові сліди часто можна знайти за реальним іменем людини. Їх поширення залежить не тільки від автора листа, допису або коментаря, але й від реакції інших користувачів, які виражають вподобання, репости або просто згадують особу у своїх матеріалах.

Щодо пасивного цифрового сліду, то він складається з даних, які автоматично збираються пристроями, без відома користувачів. Зокрема це файли-cookie, записи IP-адрес та історія відвідувань вебсайтів. Якщо історія відвідувань просто дозволяє дізнатися, які сайти було переглянуто раніше, то файли-cookie надають різноманітну аналітичну інформацію та полегшують взаємодію користувачів із вебсайтами. Використання файлів-cookie регулюється налаштуваннями вебоглядача.

На рис. 10 проілюстровано приклади активного та пасивного цифрового сліду.

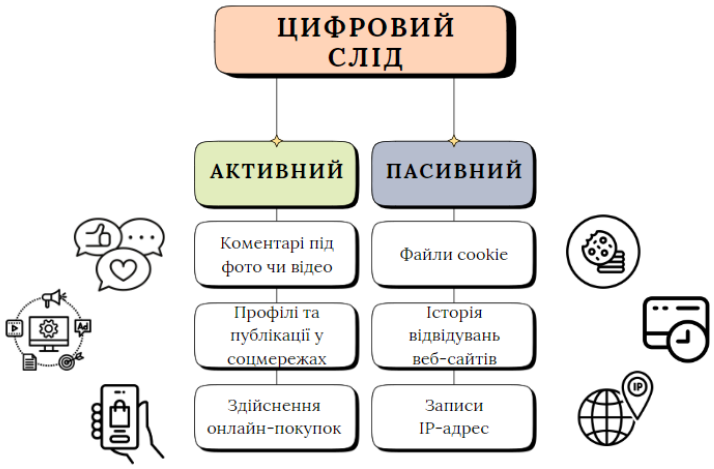

Рис. 10. Активний та пасивний цифровий слід

Крім вище згаданого, цифровий слід має декілька складових [25]:

1) По-перше, це візуальна інформація. Сюди входять будь-які відео, фото зроблені на смартфон, сигнали з камер спостереження і т. д. Один раз опублікована

фотографія залишиться там назавжди, навіть якщо ви спробуєте її видалити. Архіви сайтів, кеш пошукових систем та копії баз даних щосекунди оновлюються, тому не дадуть зникнути жодній фотографії. Звичайні камери спостереження записують всі пересування людей і є чудовим для того, хто хоче обчислити маршрут чи розпорядок дня потрібної їм людини. Саме на візуальні документи і доводиться максимальний обсяг даних, які зберігають інформацію про кожного з нас.

2) По-друге, це тексти, які ми залишаємо після себе в Інтернеті. Наприклад, електронні листи, реферати, документи, листування, опубліковані статі чи пости в соцмережах. Все листування у Viber, Facebook, Instagram зберігається там надовго і, отримавши доступ лише до архів активного листування, зловмисники можуть дізнатися про людину практично все.

Щодо менш очевидних текстових складових цифрового сліду, то варто згадати логіни та нікнейми, що ми використовуємо для різних сервісів. Ми часто не підозрюємо, що цей набір символів, може дозволити зловмиснику дізнатися про нас багато інформації.

3) По-третє, це голосова інформація. Сюди входить будь-що, що ми говоримо під час телефонних дзвінків або через месенджери. Всі мобільні оператори ведуть повний запис наших розмов, навіть якщо стверджують, що це не так. Згідно багатьох розслідувань, смартфон і без дзвінка може записувати та розшифровувати все те, що ми промовляємо біля нього.

4) Часова інформація — це четверта складова цифрового сліду. Наприклад логи, іншими слова, записи всіх дій людини, що ведуться як провайдерами, так і системами аналітики на сайтах. Це дуже докладна інформація, яка може навіть включати карту рухів курсором миші на сторінці або набраний, але згодом видалений текст у формах вводу. Дана інформація може сягати десятки гігабайт на день лише на одному сайті, проте зазвичай такі логи довго не зберігаються. Складні системи, такі як штучний інтелект чи нейромережі, аналізують логи, дістають з них суттєві дані, які в свою чергу і створюють наш цифровий слід.

Сукупність усі вище перерахованих даних називають ще цифровим відбитком.

Зацікавлені сторони можуть без невеликих зусиль зібрати потрібні дані про користувача за допомогою простих пошукових систем та відкритих сервісів, що власне і лежить в основі OSINT.

Системи стеження за цифровим відбитком працюють у кожному браузері. Вони фіксують всі наші дії та переміщення між сайтами. Кожна велика компанія, як от Google, Apple, Microsoft, Facebook та інші, створює у себе цифрову копію кожного користувача.

Методи захисту особистої інформації в інтернеті.

Оскільки OSINT покладається на наш цифровий слід для збору розвідувальних даних, найкращий спосіб захистити себе — звести його до мінімуму. Адже все, що ми публікуємо в Інтернеті, може бути використано під час OSINT-розслідувань.

Тому, аби не стати жертвою кіберзлочинців, важливо дотримуватися простих порад [26]:

1) Не розголошуйте свої особисті дані нікому та ні за яких обставин. У мережі Інтернет часто зустрічаються спроби шахрайства, такі як лотерейні афери, повідомлення про виграш чи акції, де вам пропонують надати свій номер телефону або інші особисті дані. Не піддавайтеся на такі спроби, адже більшість з них, а той усі є оманою. На рис. 11 зображено подібну шахрайську аферу.

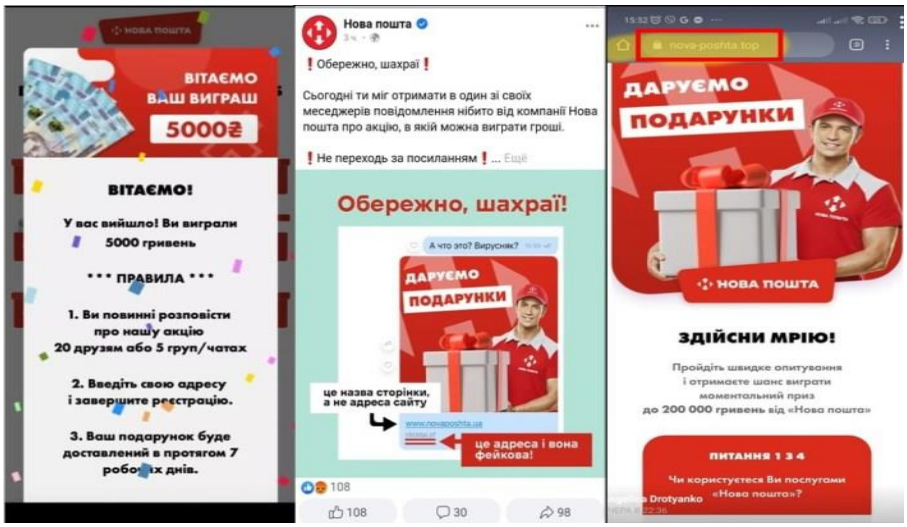

Рис. 11. Афера, що замаскована під виграш призу від Нової пошти

2) Використовуйте ліцензійне програмне забезпечення скрізь, зокрема на телефонах і планшетах, робочих та домашніх комп'ютерах, а також регулярно стежте за оновленнями.

3) Не довіряйте загальнодоступному Wi-Fi. Багато хто любить безкоштовний Wi-Fi, але в більшості таких загальнодоступних мереж дуже мало заходів безпеки, а це означає, що інші користувачі тієї самої мережі можуть легко отримати доступ до ваших дій і даних, а потім легко вкрасти гроші з вашої банківської картки. Тому краще надайте перевагу інтернету від мобільного оператора.

4) Використовуйте технології VPN (Virtual Private Network — віртуальна приватна мережа) при підключенні до публічного Wi-Fi. VPN — це тунель від вашого ПК до іншого комп'ютера, а потім до мережі Інтернет.

5) Створюйте надійні паролі та оновлюйте їх кожні 2–3 місяці. Надійний пароль — це, перш за все, унікальний пароль, який містить комбінації малих і великих літер, цифр і спеціальних символів, і в жодному разі не персональну інформацію, таку як дату дня народження, ім'я тощо. Адже більшість кібератак здійснюються завдяки безглуздим паролям, таким як admin, olena1978 або 123456780.

Також потрібно створювати індивідуальні паролі, на кожен з ваших акаунтів. Якщо виникають складнощі з тим, щоб придумати пароль, в цьому можуть допомогти сервіси-генераторів паролів, наприклад такі як:

- **ESET** — https://www.eset.com/ua/home/generator-paroley/

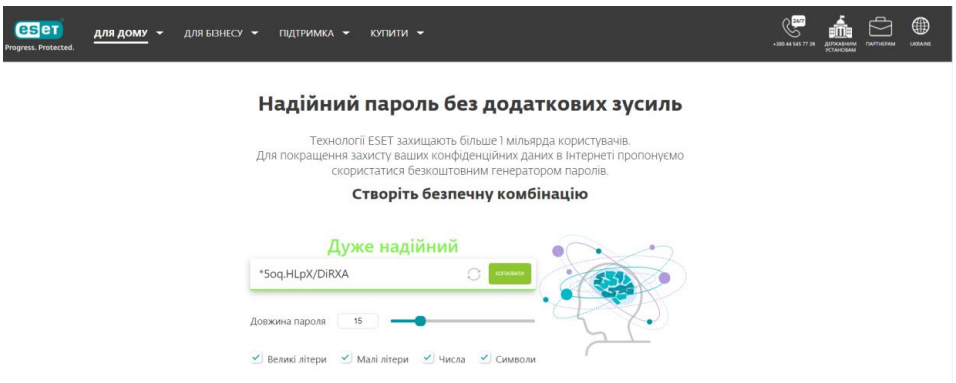

Рис. 12. Онлайн-сервіс від компанії ESET для генерації паролів

ISSN 2663 - 4023

- **DASHLANE** — https://www.dashlane.com/

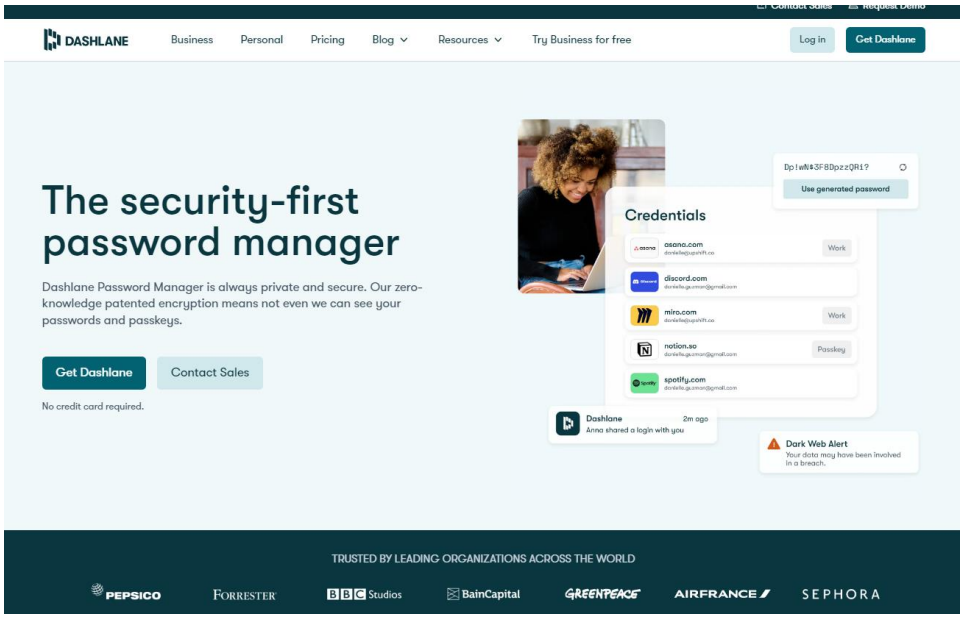

Рис. 13. Онлайн-сервіс від компанії DASHLANE для генерації паролів

6) Використовуйте двохфакторну автентифікацію. Двофакторна автентифікація — це використання одразу двох різних способів підтвердження особи. Вона дає можливість значно підсилити рівень вашого захисту та убезпечити персональні дані від кіберзловмисників. Якщо хтось намагатиметься увійти до вашого акаунту з незнайомого пристрою — наштовхнеться на додаткову перепону, а ви отримаєте сповіщення про таку спробу входу.

7) Робіть резервні копії важливих файлів, документів у хмарних сховищах. Це забезпечує доступність даних з будь-якого вашого пристрою з підключенням до Інтернету і захистить їх у випадку втрати чи пошкодження фізичних носіїв, таких як комп'ютери або зовнішні жорсткі диски.

8) Звертайте увагу на посилання, які приходять в особисті повідомлення або на електронну пошту, навіть якщо вони надіслані від друзів. Ніколи не переходьте на сайти і не завантажуйте програми, які здаються Вам підозрілими.

9) Завантажуйте програми та додатки лише з офіційних джерел.
Оскільки, офіційні веб-сайти розробників, офіційні магазини додатків (наприклад, Google Play Store для Android або App Store для iOS), зазвичай перевіряють та валідують програми, що ними розміщуються.

10) Не публікуйте онлайн фотографії ваших документів, квитків і платіжних чеків. Адже це створює ризик крадіжки особистої інформації і збільшення ймовірності фінансового шахрайства.

11) Контролюйте доступ до вашого номеру телефону та фотографій у месенджерах та соціальних мережах. Налаштуйте приватність вашого профілю таким чином, щоб номер телефону чи фотографія профілю були видимими лише для ваших друзів або контактів, яким ви довіряєте. Це допоможе попередити небажаний зв'язок з незнайомцями, шахраями та зберегти вашу приватність.

12) Не користуйтеся програмами, які можуть потенційно порушити вашу приватність, однією з таких є GetContact. Дана програма збирає та акумулює ваші дані.

Не тільки номер телефону, а e-mail, IP-адресу, геолокації, фото, вік, стать та ін. Ця інформація може передаватися третім особам з вашої згоди при реєстрації. Якщо ви вже встановили GetContact, можливо, варто подумати про його видалення. Так, це не збереже дані, які вже були передані, але щонайменше перестане дозволяти шахраям отримувати їх оновлення.

13) Реєструйтеся на сайтах за допомогою іншого номера телефону. Цей метод сприяє підвищенню рівня вашої безпеки, оскільки зменшується ризик викриття основного номера телефону перед шахраями та зловмисниками, які можуть намагатися скористатися цією інформацією для незаконних цілей. Такий підхід дозволяє зберегти приватність та захистити особисті дані від можливих загроз онлайн.

14) Користуйтеся корпоративною поштою, адже це має ряд переваг з точки зору безпеки та приватності. Користувачі можуть використовувати адресу електронної пошти, що належить їхній компанії, яка часто має більшу захищеність і застосовує додаткові заходи безпеки, такі як шифрування та механізми аутентифікації. Це дозволяє знизити ризик отримання спаму та небажаних повідомлень на основну особисту поштову скриньку. Крім того, використання корпоративної пошти може сприяти легкому керуванню обліковими записами та забезпечити більшу прозорість і контроль над активністю на вебсайтах, пов'язаних з роботою або професійними зобов'язаннями.

15) Будьте обізнаними у сфері безпеки в Інтернеті, постійно ознайомлюйтеся зі новими порадами та рекомендаціями щодо захисту вашої онлайн-активності, а також проходьте різноманітні курси та тренінги в цій галузі.

Отож, неможливо повністю захистити свої дані в Інтернеті від потенційних загроз чи досліджень, проте використання правильних заходів безпеки може значно зменшити ризики і зберегти вашу приватність.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Вивчення використання технології OSINT як інструменту деанонімізації особи в інтернет-просторі відкриває значний потенціал для збору даних про осіб, одночасно породжуючи глибокі питання щодо приватності та безпеки. Це дослідження підтверджує, що попри корисність OSINT у багатьох сферах, від журналістики до розвідки, його здатність до деанонімізації становить реальний ризик для особистої конфіденційності осіб. Зростаюче використання цифрових технологій та легкий доступ до об'ємних даних в інтернеті лише посилюють потребу в захисті особистих даних.

Перспективи розвитку інструментарію OSINT є вражаючими завдяки постійному прогресу в технологіях обробки та аналізу даних. Це відкриває нові можливості для поглиблення досліджень і збільшення ефективності використання відкритих джерел. Водночас, необхідність захисту особистих даних ніколи не була більш актуальною. Розробка ефективних механізмів захисту, освіта користувачів щодо основ цифрової безпеки, а також вдосконалення правового регулювання в цій сфері мають стати пріоритетами для забезпечення балансу між використанням можливостей OSINT та захистом прав на приватність.

Особлива увага в дослідженні приділяється розгляду етичних та правових аспектів використання OSINT. Публічні дебати та законодавчі ініціативи у різних країнах висвітлюють складність знаходження балансу між свободою інформації та захистом особистої конфіденційності. Це підкреслює важливість розробки міжнародних

стандартів та національного законодавства, яке б регулювало використання OSINT, враховуючи швидкі зміни в технологіях та способах збору даних.

У контексті визначених загроз і перспектив, це дослідження підкреслює важливість розуміння і впровадження комплексного підходу до використання OSINT. Важливо, щоб усі зацікавлені сторони — від урядових органів до приватних осіб — розробляли та застосовували відповідні стратегії захисту, щоб мінімізувати ризики і використовувати потенціал OSINT з користю для суспільства, при цьому забезпечуючи непорушність приватного життя та захист особистих даних.

Таким чином, дослідження технології OSINT як інструменту деанонімізації особи в інтернет-просторі не лише виявляє його потенціал та можливості, але й наголошує на необхідності розвитку комплексних підходів до захисту конфіденційності. У майбутньому, успіх використання OSINT залежатиме від здатності суспільства адаптуватися до нових викликів, забезпечуючи захист особистих даних у складному та динамічному цифровому середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Що таке OSINT?* (n. d.). https://explainer.ua/shho-take-osint-i-yak-vin-dopomig-vikriti-vbivstva-u-buchi/
2. Dincelli, E., Van Slyke, C., Yayla, A. (2023). Ethical Hacking for a Good Cause: Finding Missing People using Crowdsourcing and Open-Source Intelligence (OSINT) Tools. *Communications of the Association for Information Systems, 53(1),* 1052–1071. https://doi.org/10.17705/1cais.05345
3. *Інструменти інформаційної боротьби: OSINT, ІПСО та протидія дезінформації.* (n. d.). https://infolight.in.ua/wpcontent/uploads/2023/02/brochure-2.pdf
4. Varzhanskyi, I. (2023). Reflexive Control as a Risk Factor for Using OSINT: Insights from the Russia–Ukraine Conflict. *International Journal of Intelligence and CounterIntelligence,* 1–31. https://doi.org/10.1080/08850607.2023.2228489
5. *The Rise of OSINT: Few Rules, Many Opportunities.* (n. d.). https://www.afcea.org/signal-media/intelligence/rise-osint-few-rules-many-opportunities
6. *Розвідка з відкритих джерел (Open-source intelligence - OSINT).* (n. d.). https://www.maxzosim.com/rozvidka-z-vidkritikh-dzherel-osint/
7. *Що таке розвідка загроз?* (n. d.). https://nordvpn.com/uk/features/threat-protection/threat-intelligence/
8. *How To Use The Threat Intelligence Cycle To Secure Your Brand?* (n. d.). https://www.groupsense.io/resources/how-to-use-the-intelligence-cycle-to-secure-your-brand
9. Сидоренко, В. В. (2020). Цикл Шухарта-Демінга (Pdca) Для Організації Безперервного Професійного Розвитку Фахівців. *VI-а Міжнародна науково-практична конференція «НЕПЕРЕРВНА ОСВІТА НОВОГО СТОРІЧЧЯ: ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ».*
10. Юдіна, Д. (2020). *Основні напрями розвідувальної діяльності. Систематизація способів отримання інформації. Оцінка розвідувальної інформації.*
11. *Що таке OSINT (Open Source Intelligence, розвідка на основі відкритих джерел)?* (n. d.). https://thetransmitted.com/adlucem/shho-take-osint-open-source-intelligence-rozvidka-na-osnovi-vidkrytyh-dzherel/
12. *The Current Epoch Unix Timestamp*. (n. d.). https://www.unixtimestamp.com/
13. *Facebook у США оштрафували на п'ять мільярдів доларів.* (n. d.). http://surl.li/rqqjp
14. Bazzell, M. (2019). *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information.* Independently published.
15. *Конституція України — Розділ II. Права, свободи та обов'язки людини і громадянина.* (n. d.). https://www.president.gov.ua/ua/documents/constitution/konstituciya-ukrayini-rozdil-ii
16. *Кримінальний кодекс України.* (n. d.). https://zakon.rada.gov.ua/laws/show/2341-14#Text
17. *Онлайн-безпека: Як використати OSINT на користь Україні.* (n. d.). https://itarena.ua/ua/onlajn-bezpeka-yak-vykorystaty-osint-na-koryst-ukrayini/
18. *Як OSINT впливає на війну в Україні?* (n. d.). https://itedu.center/ua/blog/articles/osint/

19. *OSINT в Україні: хто і як допомагає фронту під час війни?* (n. d.). https://www.pravda.com.ua/columns/2023/01/23/7386112/
20. *Беллінгкет українською мовою.* (n. d.). https://uk.bellingcat.com/
21. *Civilian Harm in Ukraine Timemap-Bellingcat.* (n. d.). https://ukraine.bellingcat.com/
22. *InformNapalm.International Volunteer Community.* (n. d.). https://informnapalm.rocks/
23. *OSINT в Україні: як допомагає фронту під час війни?* (n. d.). https://the-news.com.ua/single/osint-v-ukrayini-iak-dopomagaie-frontu-pid-chas-viini
24. Wikipedia. (n. d.). *Цифровий слід.* https://uk.wikipedia.org/wiki/%D0%A6%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B8%D0%B9_%D1%81%D0%BB%D1%96%D0%B4
25. *OSINT, цифровий слід і як його зменшити?* (n. d.). https://www.youtube.com/watch?v=QJkLa5L9i8I
26. *21 правило цифрової безпеки.* (n. d.). https://euprostir.org.ua/practices/133410

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023

Anastasiia Hlavatska
Cybersecurity Department Student
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0009-0001-2975-8689
anastasiia.hlavatska.kb.2021@lpnu.ua

Oksana Anhelska
Cybersecurity Department Student
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0009-0004-4836-3772
oksana.anhelska.kb.2021@lpnu.ua

Ivan Opirskyy
Doctor of Science, Professor, Head of Information Protection Department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-8461-8996
ivan.r.opirskyi@lpnu.ua

INVESTIGATION OF THE USE OF OSINT TECHNOLOGY AS A NEW THREAT OF DE-ANONYMIZED PERSONS ON THE INTERNET SPACE

Abstract. This article undertakes a thorough investigation of Open Source Intelligence (OSINT) technology, which plays a significant role in modern information society by offering new methods for data collection and analysis. Special attention is given to analyzing the threats associated with the de-anonymization of individuals through the use of open information sources on the Internet. The use of OSINT allows the collection of vast amounts of data from various sources, such as social networks, forums, news sites, and other public resources, which can infringe on users' privacy. The methods of collecting information from open sources that can be used for de-anonymization of individuals are examined in detail. The potential privacy risks arising from access to large amounts of personal data are analyzed. Various aspects of the threats, including possibilities for fraud, manipulation, and even blackmail that may arise from the collection and analysis of open data, are discussed. It also considers how personal information published by users on the Internet can be used by malicious actors to carry out various types of attacks. The effectiveness of existing OSINT tools is assessed, and methods and practical examples of their use are presented. The article includes recommendations for improving digital security for users, including the enhancement of technical means of information protection and raising citizens' awareness of digital literacy. The possibilities of developing new approaches to ensuring digital security, particularly through legislative improvements and the formation of ethical standards for the use of OSINT, are discussed. Particular attention is paid to the regulatory and legal aspects of OSINT usage in Ukraine. The main legislative acts regulating the collection and processing of personal data, as well as the ethical principles that must be adhered to during OSINT investigations, are analyzed. Examples of violations of privacy rights and the legal consequences of such actions are considered. The article also highlights the practical aspects of using OSINT in the context of the war in Ukraine. It shows how OSINT technologies are used to detect and analyze the activities of malicious actors, track the movements and plans of the enemy. Examples of successful use of OSINT for identifying Russian war criminals and investigating war crimes are presented. The purpose of this article is to explore the capabilities of OSINT as a de-anonymization tool in the Internet space, analyze the potential risks to privacy, and develop recommendations for improving digital security. The result of the research is the identification of strategies and recommendations that can contribute to balancing national security and human rights in the digital space.

Keywords: OSINT; deanonymization; privacy; personal data; digital security; search methodology; OSINT research.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. *What is OSINT?* (n. d.). https://zakon.rada.gov.ua/laws/show/2341-14#Text
2. Dincelli, E., Van Slyke, C., Yayla, A. (2023). Ethical Hacking for a Good Cause: Finding Missing People using Crowdsourcing and Open-Source Intelligence (OSINT) Tools. *Communications of the Association for Information Systems, 53(1),* 1052–1071. https://doi.org/10.17705/1cais.05345
3. *Tools information struggle: OSINT, IPSO and opposition misinformation.* (n. d.). https://infolight.in.ua/wp-content/uploads/2023/02/brochure-2.pdf
4. Varzhanskyi, I. (2023). Reflexive Control as a Risk Factor for Using OSINT: Insights from the Russia–Ukraine Conflict. *International Journal of Intelligence and CounterIntelligence,* 1–31. https://doi.org/10.1080/08850607.2023.2228489
5. *The Rise of OSINT: Few Rules, Many Opportunities*. (n. d.). https://www.afcea.org/signal-media/intelligence/rise-osint-few-rules-many-opportunities
6. *Intelligence from open sources (Open-source intelligence - OSINT).* (n. d.). https://www.maxzosim.com/rozvidka-z-vidkritikh-dzherel-osint/
7. *What is threat intelligence?* (n. d.). https://nordvpn.com/uk/features/threat-protection/threat-intelligence/
8. *How To Use The Threat Intelligence Cycle To Secure Your Brand?* (n. d.). https://www.groupsense.io/resources/how-to-use-the-intelligence-cycle-to-secure-your-brand
9. Sidorenko, V. V. (2020). The Schuchart-Deming Cycle (Pdca) for the Organization of Continuing Professional Development of Specialists. *VI International Scientific and Practical Conference "CONTINUOUS EDUCATION OF THE NEW CENTURY: ACHIEVEMENTS AND PROSPECTS".*
10. Yudina, D. (2020). *The main directions of intelligence activities. Systematization of methods of obtaining information. Assessment of intelligence information.*
11. *What is OSINT (Open Source Intelligence)?* (n. d.). https://thetransmitted.com/adlucem/shho-take-osint-open-source-intelligence-rozvidka-na-osnovi-vidkrytyh-dzherel/
12. *The Current Epoch Unix Timestamp*. (n. d.). https://www.unixtimestamp.com/
13. *Facebook was fined five billion dollars in the US.* (n. d.). http://surl.li/rqqjp
14. Bazzell, M. (2019). *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information.* Independently published.
15. *Constitution of Ukraine - Chapter II. Rights, Freedoms and Obligations of A Man And A Citizen.* (n. d.). https://www.president.gov.ua/ua/documents/constitution/konstituciya-ukrayini-rozdil-ii
16. *Criminal Codex Of Ukraine*. (n. d.). https://zakon.rada.gov.ua/laws/show/2341-14#Text
17. *How To Use Osint For The Benefit Of Ukraine.* (n. d.). https://itarena.ua/how-to-use-osint-for-the-benefit-of-ukraine/
18. *How does OSINT affect the war in Ukraine?* (n. d.). https://itedu.center/ua/blog/articles/osint/
19. *OSINT in Ukraine: who and how helps the front during the war?* (n. d.). https://www.pravda.com.ua/columns/2023/01/23/7386112/
20. *Bellingket in Ukrainian.* (n. d.). https://uk.bellingcat.com/
21. *Civilian Harm in Ukraine Timemap-Bellingcat.* (n. d.). https://ukraine.bellingcat.com/
22. *InformNapalm.International Volunteer Community.* (n. d.). https://informnapalm.rocks/
23. *OSINT in Ukraine: how does it help the front during the war?* (n. d.). https://the-news.com.ua/single/osint-v-ukrayini-iak-dopomagaie-frontu-pid-chas-viini
24. Wikipedia. (n. d.). *Digital footprint.* https://uk.wikipedia.org/wiki/%D0%A6%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B8%D0%B9_%D1%81%D0%BB%D1%96%D0%B4
25. *OSINT, digital footprint and how to reduce it?* (n. d.). https://www.youtube.com/watch?v=QJkLa5L9i8I
26. *21 rules of digital security.* (n. d.). https://euprostir.org.ua/practices/133410