COMPUTER SYSTEMS AND NETWORKS

Vol. 7, No. 1, 2025

DOI: https://doi.org/10.23939/csn2025.01.143

УДК 621.3

ДОСЛІДЖЕННЯ ІСНУЮЧИХ ЗАСОБІВ ТА ПІДХОДІВ ДО ПРОВЕДЕННЯ OSINT В КОНТЕКСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОСОБИ ТА ДЕРЖАВИ

В. С. Івкова, І. Р. Опірський

Національний університет "Львівська політехніка",
кафедра захисту інформації
E-mail: valeriia.s.ivkova@lpnu.ua, ivan.r.opirskyi@lpnu.ua

Досліджено сучасні засоби та підходи до проведення OSINT-аналізу відкритих джерел інформації. Ключова роль OSINT, разом з іншими методами розвідки, такими як HUMINT, IMINT, SIGINT, MASINT та GEOINT, полягає у створенні цілісного інформаційного поля, що поєднує відкриті, технічні, людські та геопросторові джерела. Постійний розвиток методологій та вдосконалення інструментів автоматизації дає змогу підвищити ефективність і точність аналізу отриманої інформації, що робить OSINT одним із найважливіших елементів сучасної розвідки.

Під час дослідження розглянуто основні джерела даних, такі як публічні реєстри, соціальні мережі, новинні ресурси, геопросторові дані та інші відкриті ресурси. Висвітлено ключові етапи збору, аналізу та обробки інформації, що є невід'ємною складовою OSINT-досліджень.

Особливу увагу приділено інструментам Geospatial Intelligence (геопросторової розвідки) із наведенням порівняльної характеристики найпоширеніших рішень. Досліджено їх функціональні можливості, переваги, обмеження та сфери застосування.

Проведено аналіз популярних інструментів OSINT, таких як "Maltego", "Shodan", і платформ для моніторингу соціальних медіа. Проаналізовано новітні підходи, зокрема використання штучного інтелекту, автоматизацію процесів аналізу та забезпечення прозорості даних.

Оцінено ступінь загрози персональним даним та конфіденційній інформації в розрізі проведення OSINT. Визначено, які саме дані потребують захисту, а також наведено відповідні заходи для мінімізації ризиків, які включатимуть проведення класифікації даних за рівнем конфіденційності.

Запропоновано ефективні стратегії протидії OSINT, зокрема щодо виявлення та нейтралізації інформаційних витоків, застосування адекватних засобів захисту даних, як-от шифрування, системи моніторингу та аудит доступу, окреслено перспективи розвитку в умовах сучасного інформаційного суспільства.

Ключові слова: аналіз даних, відкриті джерела інформації, інструменти OSINT, інформаційна безпека, конфіденційна інформація, класифікація конфіденційної інформації, OSINT.

Вступ

OSINT – технології в сучасному світі широко використовують представники правоохоронних органів, журналісти, громадські активісти, військові та спеціалісти інших галузей.

Водночас розвиток OSINT породжує нові виклики у сфері захисту персональних даних та конфіденційної інформації. Завдяки можливостям автоматизації та широкому доступу до технологій потенційно уразливими стають навіть ті дані, які раніше вважалися недоступними.

Значна кількість інформації, що обробляється в інформаційних системах державних і приватних установ, може бути використана для несанкціонованого доступу, маніпуляцій або інших деструктивних дій. Особливо це стосується персональних даних громадян, конфіденційної комерційної інформації, стратегічних або науково-технічних розробок тощо.

Отже, перед організаціями постає важливе завдання - визначити, які саме дані потребують захисту, а також впровадити відповідні заходи для мінімізації ризиків, які передбачатимуть проведення класифікації даних за рівнем конфіденційності та застосування адекватних засобів їх захисту, включаючи шифрування, системи моніторингу та аудит доступу.

Класифікація інформації за рівнем критичності наслідків від її витоку є важливим інструментом для управління ризиками та забезпечення інформаційної безпеки. Вона дає змогу чітко визначити, які дані потребують базового рівня захисту, а які - найвищого рівня безпеки.

Ефективна реалізація цієї класифікації сприяє впровадженню диференційованих заходів захисту, що відповідають рівню чутливості даних, та мінімізації ризиків в умовах сучасного інформаційного середовища. Застосування такого підходу є критично важливим для державних установ, бізнесу та інших організацій у цифрову епоху.

Наразі OSINT-інструменти дають змогу автоматично аналізувати великі обсяги інформації, проводити геолокаційний аналіз та верифікацію джерел, виявляти інформаційні аномалії та потенційні витоки даних. Аналіз функціоналу сучасних OSINT-інструментів дає змогу не лише оцінити ступінь загрози, а й сформулювати ефективні стратегії протидії, зокрема щодо виявлення та нейтралізації інформаційних витоків. Проте ці інструменти не є досконалими. Основним викликом залишається потреба у кваліфікованих спеціалістах, здатних правильно інтерпретувати отримані дані, а також ризик використання результатів досліджень для зловмисних цілей.

OSINT залишатиметься важливим інструментом в умовах глобалізації та інформаційної революції. Подальший розвиток технологій штучного інтелекту та машинного навчання значно підвищить ефективність цих інструментів. Однак необхідно знайти баланс між можливостями OSINT та захистом приватності, щоб уникнути зловживань і забезпечити етичне використання відкритих даних.

Огляд джерел літератури

Питання використання OSINT-технологій досліджують в останні роки науковці, спеціалісти з безпеки, журналісти та громадські активісти. Розробляються методології пошуку інформації, удосконалюються інструменти автоматизації отримання відомостей з відкритих джерел.

Генерал-лейтенант Самуель Уілсон, який очолював Розвідувальне управління Міністерства оборони США, зазначав, що 90 % всієї розвідувальної інформації отримується з відкритих джерел, тоді як лише 10 % припадає на агентурну діяльність [1].

Зокрема, існує шість основних способів для отримання розвідувальної інформації [2, с. 27]:

OSINT (Open source intelligence) – збір та аналіз публічно доступної інформації, доступ до якої не обмежено власником або розподільником такої інформації та не обмежено грифом таємності.

HUMINT (Human intelligence) - найдавніший метод отримання інформації, збір даних із людських джерел, шляхом спілкування. У сучасному інформаційному середовищі цей процес може бути пов’язаний із застосуванням методів “соціальної інженерії”.

IMINT (Imagery Intelligence) - відображення об'єктів, які відтворюються за допомогою електронних або оптичних засобів, на плівці, екранах електронних пристроїв чи інших носіях.

SIGINT (Signals intelligence) - перехоплення сигналів, чи то між людьми, між машинами або комбінацією обох.

MASINT (Measurement and signature intelligence) - це спеціалізована дисципліна в галузі збору розвідданих. Вона передбачає збір і аналіз даних, отриманих із специфічних технічних та наукових джерел. MASINT зосереджується на унікальних характеристиках об'єктів та явищ, надаючи розвіддані, які виходять за рамки того, що можна зібрати за допомогою традиційних методів розвідки.

GEOINT (Geospatial Intelligence) - зображення та геопросторові дані, створені за допомогою інтеграції зображень та географічної інформації.

До ключових етапів проведення OSINT-розвідки належить:

1. Постановка мети та планування – залежно від об'єкта пошуку (відомості, що підлягають встановленню та аналізу) здійснюється підбір ключових джерел та визначається набір інструментів для проведення дослідження з урахуванням етичних та правових норм використання та обробки інформації.

2. Збір даних – процес формування масиву даних, що підлягають аналізу, зокрема сюди можна зарахувати: інтернет-ресурси (вебсайти, блоги, форуми, соціальні мережі); медіа (ЗМІ, новинні портали, відео, радіо та друковані видання); урядові та офіційні документи (звіти, бази даних, судові рішення тощо); технічні джерела (IP-адреси, доменні реєстрації, метадані файлів).

Інструменти, що використовуються на цьому етапі: пошукові системи, спеціалізовані OSINT-платформи (наприклад, Maltego, Shodan, Spiderfoot), аналіз соціальних мереж (LinkedIn, Facebook, Instagram) тощо.

3. Обробка та фільтрація інформації – здійснюється перевірка достовірності джерел і зібраних даних, виділення ключових фактів і відсіювання зайвої або хибної інформації, структурування даних для подальшого аналізу (створення таблиць, схем, діаграм).

4. Аналіз даних – за результатами отриманих даних аналітики шукають взаємозв'язки між зібраною інформацією, виявляють шаблони, тенденції або аномалії у поведінці суб'єктів дослідження. Використовують інструменти візуалізації для полегшення розуміння (наприклад, побудова графів зв'язків).

5. Інтерпретація та висновки – на цьому етапі формуються висновки на основі аналізу. Проводиться оцінка впливу отриманих даних на вирішення завдання, розробляються рекомендації або сценарії подальших дій.

6. Оформлення звіту - підготовка зрозумілого та структурованого звіту, що містить результати розвідки, графіки, таблиці та висновки, із зазначенням використаних джерел, з метою забезпечення прозорості та можливості верифікації даних.

7. Перевірка та оцінка результатів – здійснюється перевірка точності отриманих даних перед їх використанням, а також аналіз ефективності обраних методів збору та обробки інформації для покращення майбутніх досліджень.

Ключова роль OSINT, разом з іншими методами, такими як HUMINT, IMINT, SIGINT, MASINT та GEOINT, полягає у створенні цілісного інформаційного поля, що поєднує відкриті, технічні, людські та геопросторові джерела. Постійний розвиток методологій та вдосконалення інструментів автоматизації дає змогу підвищити ефективність і точність аналізу отриманої інформації, що робить OSINT одним із найважливіших елементів сучасної розвідки.

Однак використання таких технологій супроводжується викликами, зокрема щодо захисту конфіденційної інформації, дотримання етичних норм і забезпечення інформаційної безпеки. Це потребує створення чіткої нормативно-правової бази, а також підготовки висококваліфікованих фахівців, які здатні працювати з відкритими джерелами в умовах інформаційної війни та глобальної цифровізації.

Постановка задачі

Дослідження та аналіз функціоналу інструментів для проведення розвідки по відкритих джерелах надасть можливість визначити перелік даних, що потребують захисту, а також запровадити заходи протидії OSINT з метою мінімізації ризиків для персональних даних особи або конфіденційної інформації, що обробляється в інформаційних системах приватних та державних установ або організацій.

Мета дослідження полягає у вивченні особливостей OSINT-інструментів, аналізі їх функціоналу та розробці рекомендацій щодо зменшення ризиків, пов'язаних із обробкою персональних та конфіденційних даних. Робота спрямована на поглиблене розуміння вразливостей інформаційних систем та створення механізмів їх захисту, що є особливо актуальним у контексті зростання загроз інформаційній безпеці на національному та міжнародному рівнях.

Завдання дослідження:

1. Дослідити та проаналізувати функціонал OSINT-інструментів, визначити їх переваги та недоліки.

2. Встановити перелік даних, що потребують захисту, за результатами роботи OSINT-інструментів та запропонувати їх класифікацію.

3. Запропонувати методологію мінімізації ризиків для персональних даних особи або конфіденційної інформації, яка обробляється у відкритих джерелах інформації.

Дослідження надає можливість не лише виявити слабкі місця у захисті інформаційних систем, а й запропонувати заходи протидії OSINT-розвідці, які можуть бути інтегровані у політику інформаційної безпеки організацій.

Інструменти для проведення GEOINT (Geospatial Intelligence)

Цікавим прикладом використання поєднання декількох методів OSINT-технологій стало дослідження журналістів французького видання "Le Monde", оприлюднене у жовтні 2024 року.

Розслідування показує, що людей можна ідентифікувати через використання ними програми для відстеження спортивних змагань.

"Strava" - це застосунок, який використовують бігуни чи велосипедисти. Зокрема, у 2018 році у застосунку була мапа активності, яка відображає усі агреговані поїздки користувачів.

За даними "Le Monde", охоронці зі служб безпеки президентів Франції та Сполучених штатів Америки не захищали свою активність та оприлюднили її у вищевказаному застосунку. Тому "Strava" отримала доступ до даних, які можуть розкрити наявність військових баз в усьому світі або їхнє розташування та маршрути, які військові пройшли там або навколо. Журналісти ідентифікували 12 осіб зі служби охорони президента Франції, які користувалися застосунком "Strava", а в Секретній службі США – 26 осіб, а також маршрути їх пересування під час тренувань [3].

В цьому випадку журналісти використовували методики GEOINT з метою аналізу переміщення спортсменів та виокремлення певних осіб.

Геопросторова розвідка (GEOINT) є однією з ключових складових сучасної системи збору розвідувальних даних. Інтеграція географічної інформації та зображень забезпечує багатовимірний аналіз місцевості, який є незамінним для прийняття стратегічних рішень у військовій справі, плануванні інфраструктурних проєктів, управлінні ресурсами та реагуванні на надзвичайні ситуації.

GEOINT дає змогу ефективно відстежувати динаміку подій, аналізувати географічні особливості місцевості та оцінювати їхній вплив на операційні процеси. Використання супутникових знімків, зображень, зроблених за допомогою дронів, картографічних даних та інноваційних аналітичних інструментів сприяє підвищенню точності прогнозів і швидкості ухвалення рішень.

Зокрема, до основних інструментів, які використовуються при GEOINT, належить:

- **Soar** (https://soar.earth/) – платформа позиціонує себе, як онлайн-атлас, який дає змогу переглядати, завантажувати, відкривати та взаємодіяти з величезною бібліотекою високоякісних карт та зображень. Кожна карта, супутникове зображення та зображення з дронів, які коли-небудь існували або будуть існувати, зібрані в одному місці [4].

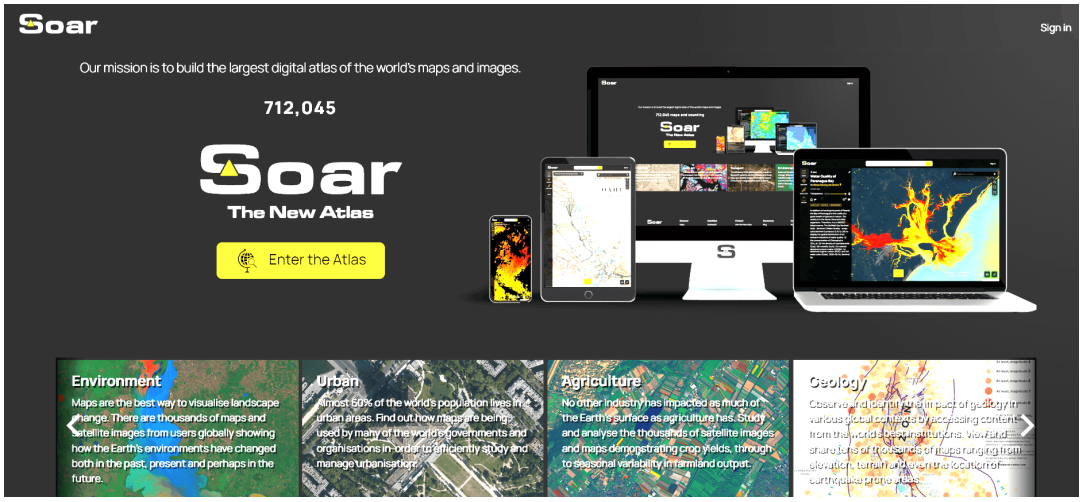

Рис. 1. Платформа для пошуку зображень місць Soar

- **Google Earth Engine** (https://earthengine.google.com/platform/) - платформа для обробки та аналізу геопросторових даних з використанням хмарних обчислень в інфраструктурі Google.

Earth Engine інтегрує великий каталог геопросторових даних із розподіленими обчисленнями, доступними через клієнтські бібліотеки. Користувачі можуть отримати доступ до широкого діапазону супутникових і екологічних даних, а також включати власні набори даних.

Платформа спрощує геопросторовий аналіз, автоматично обробляючи проекцію, масштабування та компонування даних на основі заданих користувачем параметрів. Його аналітичні функції працюють ефективно в різних масштабах, не вимагаючи чітких етапів підготовки даних або фрагментації. Завдяки внутрішньому керуванню складною обробкою даних і обчислювальним масштабуванням Earth Engine дає змогу користувачам зосередитися на аналізі, а не на технічних налаштуваннях.

Є кілька способів взаємодії з платформою. Редактор коду - це вебінтегроване середовище розробки для написання та виконання сценаріїв. Explorer - це легка вебпрограма для вивчення каталогу даних і виконання простих аналізів [5].

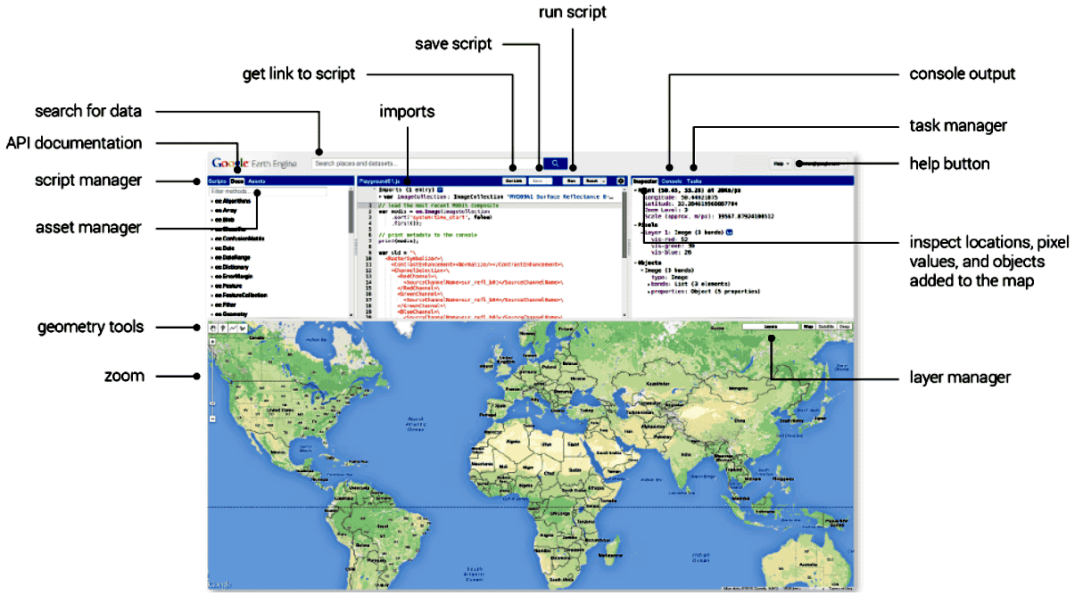

Рис. 2. Інфраструктура редактора коду Google Earth Engine

- **geOSINT** (https://github.com/coldfusion39/geOSINT) - скрипт, за допомогою якого здійснюється пошук фотографії з геотегами в соціальних мережах, зображення в подальшому відображаються на карті. Якщо зображення знайдено, на карті з'являється червоний маркер. Натиснувши на цей маркер, ви можете переглянути знайдене зображення. Скрипт використовує API "FourSquare", "Flickr" і "X" (Twitter) для пошуку фотографій, розміщених на певній відстані від наданої адреси. Потрібен принаймні один ключ API, щоб geOSINT міг повертати будь-які результати [6].

Рис. 3. Результат роботи скрипту ***geOSINT***

- **Newspaper Map** (https://newspapermap.com/) - це вебсервіс, який пропонує інтерактивну карту газет світу, за допомогою якої здійснюється пошук газети за країною, мовою, темою та датою публікації.

Недолік вказаного інструменту – це вибіркова інтеграція про видання, що обмежує можливості повноцінного аналізу ситуації в певній місцевості. Наприклад, у Львові, згідно з даними інструменту, наявне лише одне видання - Експрес (https://expres.online/).

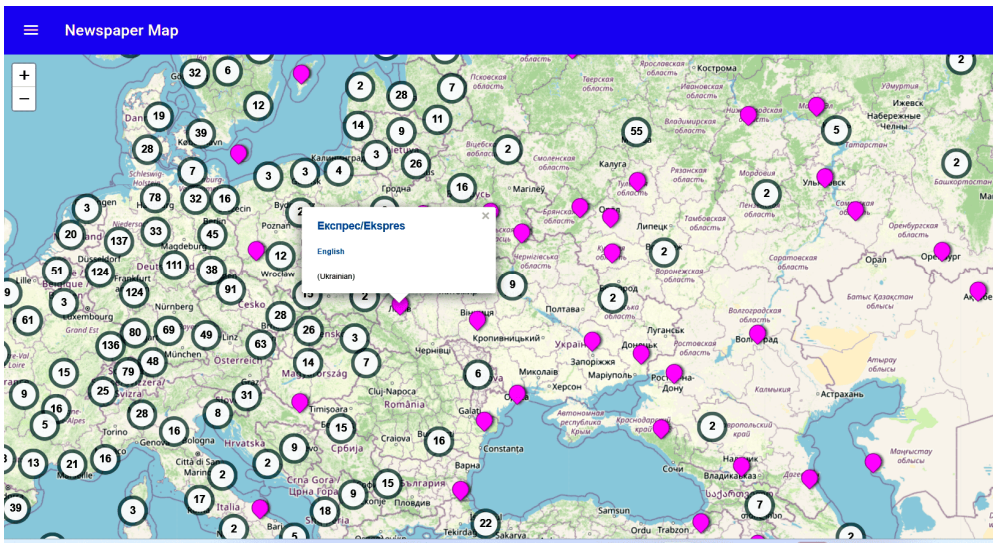

Рис. 4. Платформа ***Newspaper Map***

- **EOS Land Viewer / USGS Earth Explorer / NASA Earthdata** – сервіси для отримання доступу до різних колекцій супутникових даних та використовувати їх для наукових, дослідницьких, агрономічних та інших цілей.

Таблиця 1

Порівняльна таблиця функціоналу вищевказаних інструментів

Назва інструменту	Тип інформації, що обробляється	Переваги інструменту	Недоліки інструменту	Рівень загрози
Soar	Фотозображення місцевості. Фото з камер БПЛА. Мапи різних типів. Знімки з супутників	Безкоштовний доступ. Можливість додавати власний контент	Можливість отримання недостовірної інформації, фото об'єктів може завантажувати будь-який з користувачів проєкту	Середній (на фото з супутників можуть бути зафіксовані об'єкти критичної інфраструктури, військові об'єкти тощо)
Google Earth Engine	Зображення зі супутників. Екологічні дані	Безкоштовний інструмент. Можливість створювати та інтегрувати власні бібліотеки	Необхідність знань з Python і JavaScript	Помірний
geOSINT	Зображення в соціальних мережах. Геотегі	Безкоштовний інструмент. Можливість отримати зображення за певною адресою та навколо неї	Консольна інсталяція програми	Помірний
Newspaper Map	Аналіз геолокації видавництв	Безкоштовний інструмент. Доступ до газет за територіальною ознакою	Інтегровано незначну кількість видань	Низький
EOS Land Viewer	Супутникові зображення. Геопросторові дані	Безкоштовний інструмент	Неповнота інформації, обмеження згідно з рухом супутників	Низький
USGS Earth Explorer	Супутникові зображення. Геопросторові дані	Безкоштовний інструмент	Неповнота інформації, обмеження згідно з рухом супутників	Низький
NASA Earthdata	Супутникові зображення. Геопросторові дані	Безкоштовний інструмент	Неповнота інформації, обмеження згідно з рухом супутників	Низький

Отже, ефективність GEOINT залежить від доступу до якісних геопросторових даних, їх актуальності та точності. GEOINT посідає важливе місце у структурі сучасної розвідки завдяки своїй здатності інтегрувати геопросторові аспекти в загальний процес збору даних. Його використання сприяє оптимізації роботи в багатьох сферах, зокрема обороні, логістиці, екології та урбанізації, роблячи його потужним інструментом для вирішення складних завдань у різних контекстах.

Інструменти для проведення OSINT
з використанням соціальних мережах

За даними платформи “DataReportal” станом на січень 2024 року в Україні було зареєстровано 24,30 мільйона користувачів соціальних мереж, що дорівнювало 64,9 % загального населення. Зокрема, Facebook мав 13,85 млн користувачів в Україні, що становить приблизно 37 % від загальної чисельності населення. Месенджер від Meta охопив 8,6 млн користувачів, а 12,4 млн українців на початок 2024 року були користувачами Instagram. Одночасно YouTube - мав 24,3 млн користувачів, а це 64,9 % від загальної чисельності населення, TikTok - 16,47 млн користувачів віком від 18 років і старше, LinkedIn - 5,1 млн користувачів, X - 4,55 млн користувачів в Україні [7].

Одним з дієвих інструментів для аналізу профілів в соціальних мережа є продукт української компанії “**Artellence**”, яка розробила інтегровану платформу для аналізу облікових записів в соціальних мережах. Вказаний проєкт працює на основі штучного інтелекту.

Згідно з даними, зазначеними на сайті проєкту, станом на січень 2025 року база даних, за допомогою якої здійснюється пошук інформації, налічує понад 3 млрд проаналізованих профілів користувачів різних соціальних мереж та понад 5 млрд розпізнаних облич.

Зокрема, підпроєкт “**BigDataPeople**” для оборонних структур, державного сектора та служб безпеки великого бізнесу допомагає правоохоронним вирішувати задачі аналізу цифрових слідів у відкритих джерелах інформації. Рішення цієї компанії, зокрема, допомагають виявляти людей, які схильні до сепаратизму [8].

Підпроєкт “**BigDataAnalytics**” адаптований під консалтингові задачі із проведення досліджень та створення потужних аналітичних продуктів для політичної та державної сфер.

Підпроєкт “**BigDataCredit**” - продукт для банків та МФО. Вирішує задачі аналізу недобросовісних позичальників та уникнення ризиків шахрайства.

Рис. 5. Платформа ***Artellence***

Ще одним з ефективних інструментів для обробки і аналізу інформації в соціальних мережах є платформа **Lampyre**.io. Принцип роботи Lampyre.io є досить простим. Платформа використовує API різних сервісів та баз даних, щоб надати доступ до інформації без необхідності реєструватися в кожному окремо.

Проєкт представлено у двох видах доступу web-сайту для швидкого відпрацювання інформації з таких ідентифікаторів: номер телефону, електронна адреса, IP-адреса та домен і програмне забезпечення для персонального комп’ютера, яке має більший пошуковий функціонал, який здійснюється за різними типами пошукових запитів. Вивід знайденої інформації здійснюється у вигляді схеми з таблицею відомостей з посиланнями на джерела [9].

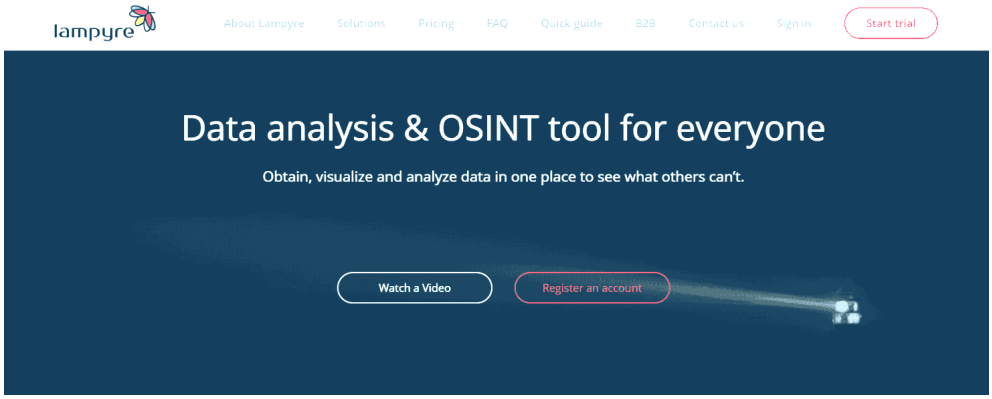

Рис. 6. Платформа Lampyre

Платформа **WhatsMyName** (https://whatsmyname.app/) – це простий OSINT-інструмент для пошуку інформації про реєстрацію особи на форумах, в соціальних мережах та інших сервісах за нікнеймом (username), інструмент дає змогу виявляти присутність особи в різних застосунках.

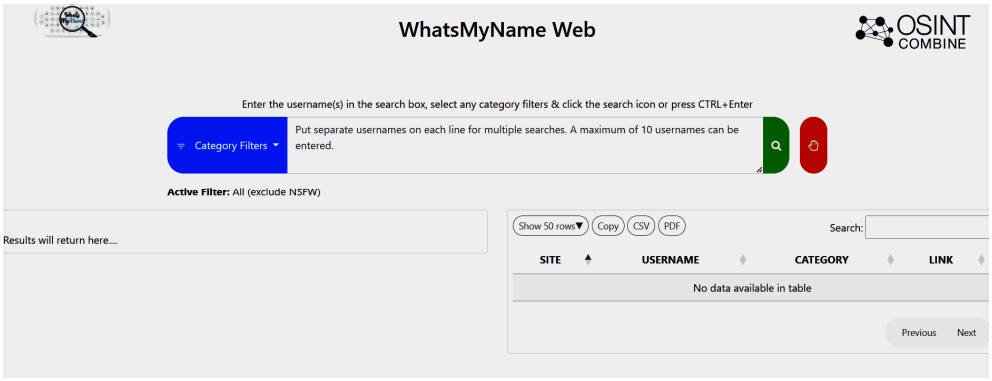

Рис. 7. Платформа WhatsMyName

Один із дієвих інструментів OSINT - це **X-Ray Contact** (https://x-ray.contact/), який дає змогу аналітикам оперативно знаходити потрібну інформацію та встановлювати зв'язки між різними суб'єктами. Інструмент з інтеграцією штучного інтелекту дає змогу здійснювати пошук даних за електронною поштою, номером телефону, фотографією, ім'ям або юзернеймом. X-Ray Contact використовує широкий спектр джерел для збору інформації, а його головна мета полягає в агрегуванні різноманітних відомостей про конкретну особу.

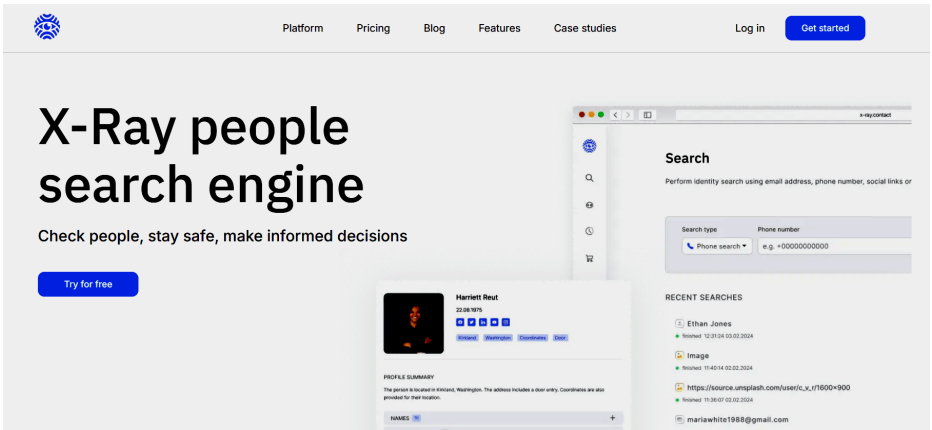

Рис. 8. Платформа X-Ray Contact

Таблиця 2

Порівняльна таблиця функціоналу вищевказаних інструментів

Назва інструменту	Тип інформації, що обробляється	Переваги інструменту	Недоліки інструменту	Рівень загрози
Artellence	Відкриті дані профілів соціальних мереж. Контактна інформація (номер телефону). Зв'язки осіб. Інформація з маркетплейсів. Фотографії	Швидкість. Наявність модулів ШІ. Можливість отримання контактної інформації. Можливість аналітичного звіту по публікаціям користувача	Обмеження переліку користувачів	Середній (інструмент надає контактну інформацію, номер мобільного телефону)
Lampyre	Відкриті дані профілів соціальних мереж. Контактна інформація (номер телефону). Зв'язки осіб. Фотографії	Вивід інформації у вигляді схем-зв'язків. Швидкість. Обробка великого масиву даних. Наявна демо-версія	Необхідність придбання ліцензії	Середній (інструмент надає контактну інформацію, номер мобільного телефону, email)
WhatsMyName	Соціальні мережі. Форуми та додатки	Безкоштовний інструмент. Наявність пошуку по нікнейму. Вивід посилань на профілі користувача	Обмежений пошук по 624 джерелам	Низький (обробляється загальнодоступна інформація)
X-Ray Contact	Відкриті дані профілів соціальних мереж. Контактна інформація (номер телефону). Зв'язки осіб. Інформація з відкритих реєстрів. Фотографії	Швидкість. Наявність модулів ШІ. Можливість отримання контактної інформації. Можливість отримання інформації про досвід і місця роботи об'єкта. Наявна демо-версія	Необхідність придбання ліцензії	Середній (інструмент надає контактну інформацію, номер мобільного телефону)

Соціальні мережі є потужним джерелом відкритої інформації, що дає змогу отримувати цінні дані для аналізу в рамках OSINT. Інструменти для роботи із соціальними платформами значно спрощують і прискорюють процес збору, обробки та інтерпретації інформації. Вони дають змогу аналітикам ефективно ідентифікувати взаємозв'язки між користувачами, досліджувати активність у мережах, збирати дані за профілями, геолокаціями, фотографіями та іншими відкритими джерелами.

Серед ключових можливостей таких інструментів:

1. **Пошук за іменем, нікнейм (username), email чи номером телефону**, що дає змогу швидко знаходити профілі користувачів.
2. **Аналіз взаємозв'язків та мережевої активності**, що сприяє розумінню соціального контексту та ідентифікації ключових осіб чи груп.
3. **Моніторинг публічної активності та змін у профілях**, який забезпечує актуальність зібраної інформації.

Однак ефективне використання таких інструментів потребує обізнаності щодо правових і етичних аспектів. Забезпечення конфіденційності та дотримання законодавства про захист персональних даних є важливими складовими роботи з соціальними мережами в OSINT.

Інші категорії OSINT-інструментів

Програмне забезпечення **Maltego** дає змогу шукати інформацію у профілях соціальних мереж, за адресами електронної пошти, за номерами телефонів тощо. Maltego шукає у відкритих джерелах інформацію, все знайдене поєднує у схеми та вибудовує логічні взаємозв'язки. У роботі для цього використовується три елементи: Entities (об'єкт), Transforms (процес) та Links (зв'язки).

Однією з основних функцій програми є збір інформації серед джерел Maltego Transform Hub. Вивід даних здійснюється у вигляді схеми, за обраним макетом, наприклад, блоковий, ієрархічний, круговий, органічний. На потужних графіках можна виявляти закономірності. Графік можна анотувати та експортувати для подальшого використання.

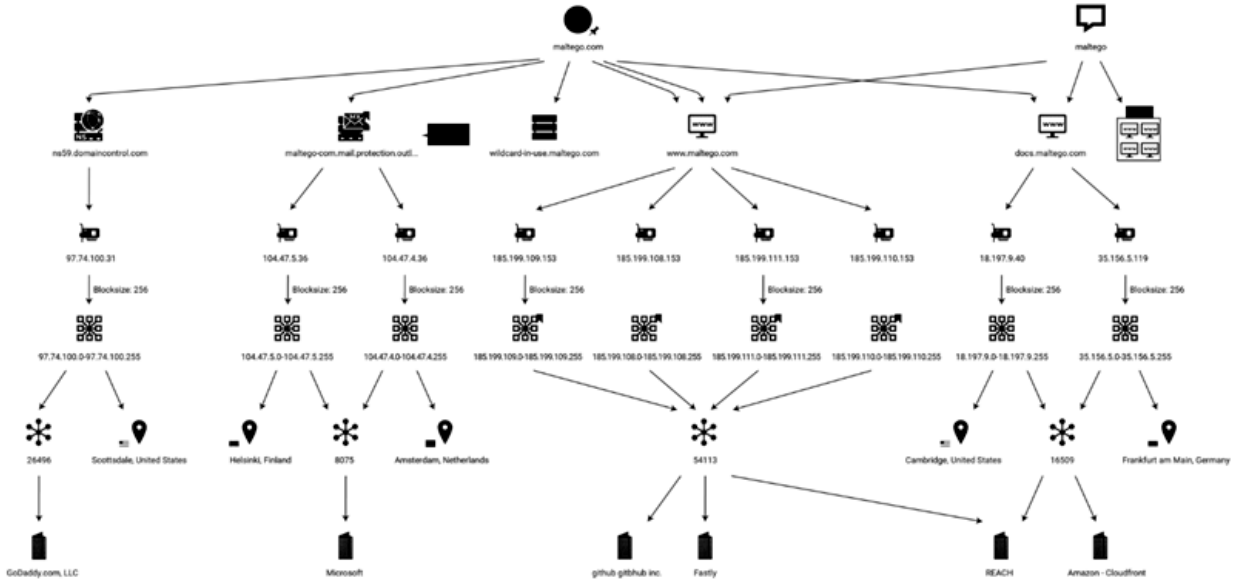

Рис. 9. Результат пошуку за запитом "домен maltego.com"

Intelligence X – чеський проєкт, який позиціонується, як пошукова система та архів даних. Згідно з інформацією на сайті, станом на січень 2025 року, проєкт нараховує понад 207,3 млрд записів. Основний функціонал системи:

1. Пошук здійснюється за допомогою селекторів, тобто конкретних пошукових термінів, таких як адреси електронної пошти, домени, URL-адреси, IP-адреси, CIDR, адреси Bitcoin, хеші IPFS тощо.
2. Інтегрована платформа збирає інформацію в таких місцях, як DarkNet, платформи для обміну документами, дані Whois, публічні витоки даних тощо.
3. Проєкт зберігає архів історичних даних із результатами, подібно до того, як Wayback Machine з archive.org зберігає історичні копії вебсайтів.

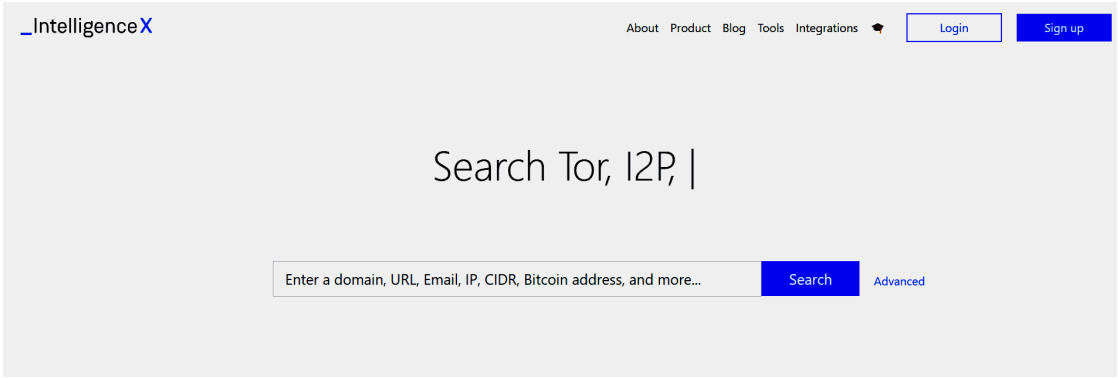

Рис. 10. Проєкт Intelligence X

Shodan – пошукова система, яка дає змогу аналізувати відкриті порти, запущені служби та виявляти під'єднані до мережі "Інтернет" пристрої за IP-адресою або запитом конфігурації пристрою. Крім того, платформа висвітлює вразливості пристроїв та надає їх опис. З її допомогою можна професійно досліджувати комп'ютерні мережі та інформаційні системи, аналізувати структуру інтернету, тенденції і статистику захищеності інтернет-ресурсів по усьому світі [10].

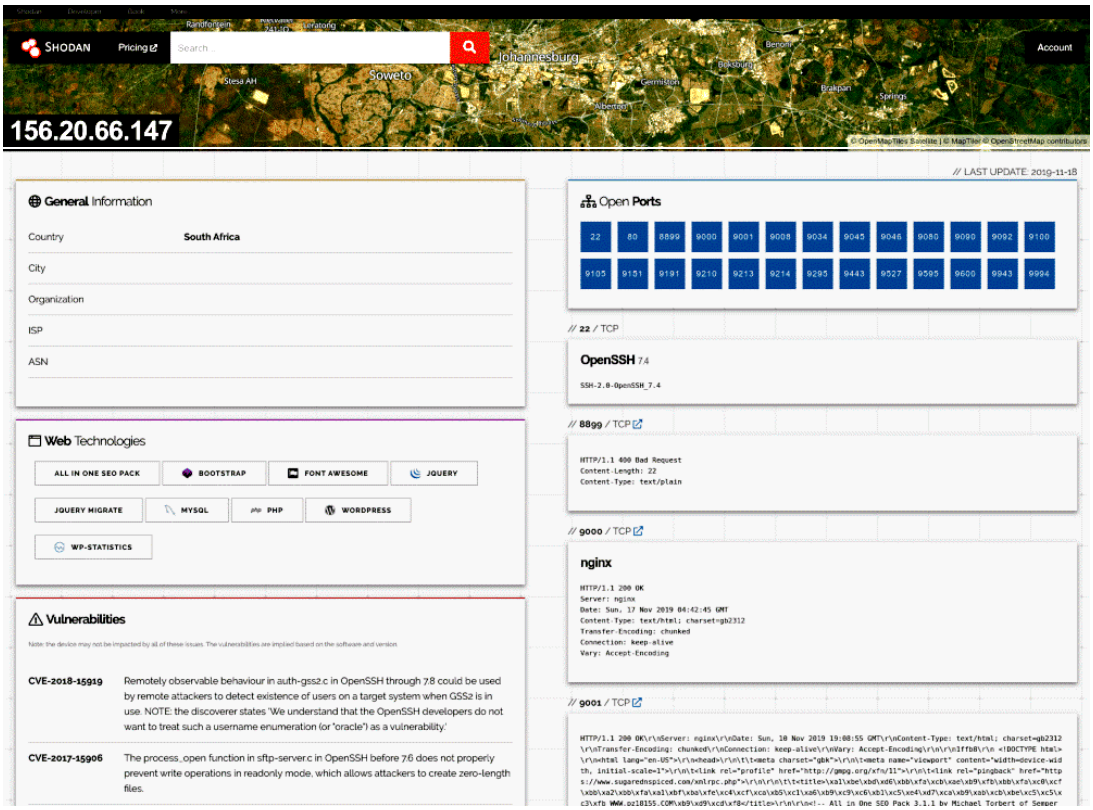

Рис. 11. Приклад відображення даних пошукової системи Shodan

Платформа для відстежування завантажень torrent-файлів https://iknowwhatyoudownload.com/ дає змогу отримувати інформацію про користувачів конкретної IP-адреси або генерувати різні типи статистики за результатами обміну файлами в torrent-системах.

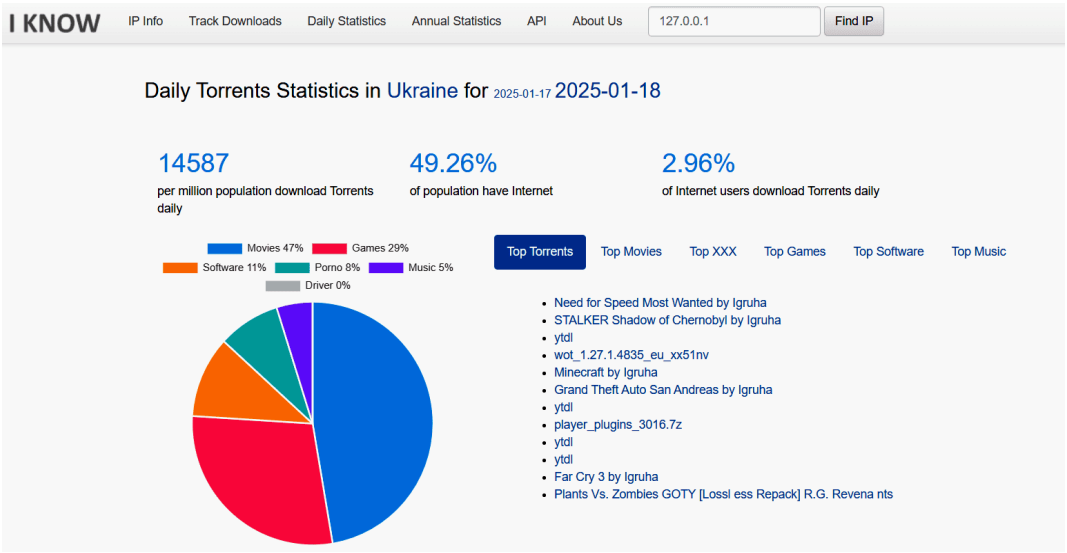

Рис. 12. Статистика використання torrent-систем за добу (17- 18.01.2025)

Одним із найпростіших і найкорисніших методів для OSINT-аналітика є вилучення метаданих із зображень. Метадані – це дані, які часто додаються до зображення, як, наприклад, час зйомки, тип камери, яка використовувалася, і, якщо пощастить, GPS-координати [11, с. 37]. Для аналізу метаданих використовують спеціалізовані сервіси, наприклад **Metadata2Go.com** - це безкоштовний онлайн-інструмент, який дає змогу отримати доступ до прихованих файлів exif та метадані файлів. Також дослідники використовують **fotoforensics.com**, тому що додатково до звичайних метаданих ресурс надає аналіз рівня помилок (ELA). ELA дає змогу бачити, коли змінюється ступінь стиснення зображення.

Таблиця 3

Порівняльна таблиця функціоналу вищевказаних інструментів

Назва інструменту	Тип інформації, що обробляється	Переваги інструменту	Недоліки інструменту	Рівень загрози
Maltego	Інформація з відкритих джерел. Перелік залежить від підключених модулів	Вивід інформації у вигляді схеми. Обробка великого масиву даних	Необхідність придбання ліцензії. Необхідність підключення модулів пошуку	Середній
Intelligence X	Витоки інформації. Номери телефонів, логіни, паролі, банківська інформація	Наявний обмежений безкоштовний доступ. Можливість завантаження баз	Необхідність придбання ліцензії	Високий (інструмент працює з персональними даними)
Shodan	IP-адреси. Запущені служби. Вразливості. Недоліки системи безпеки (іноді показує пароль/логін до пристрою)	Надання інформації з поясненнями. Можливість пошуку по useragent	Обмежений пошук, необхідність придбання ліцензії	Високий (інструмент надає інформацію стосовно вразливостей, які можуть бути експлуатовані, а також дані для авторизації на деяких типах пристроїв)
iknowwhatyoudownload.com	Завантаження torrent-файлів	Безкоштовний	Аналізує лише torrent-трекери	Низький
Metadata2Go.com	Метадані exif-файли	Безкоштовний. Не зберігає файли користувача	Аналізує лише файли, немає модулів для аналізу файлу, розміщеного в інтернет-мережі	Низький
Fotoforensics.com	Метадані	Безкоштовний. Не зберігає файли користувача. Можливість завантаження файлу та аналізу по URL-посиланню	Не має	Низький

Результати дослідження

OSINT є одним із найважливіших інструментів сучасної розвідки. Його застосування сприяє отриманню високоякісних даних із мінімальними витратами ресурсів, що робить його незамінним у сучасному інформаційному просторі.

Перелік проаналізованих інструментів не є вичерпним і сформований на власному досвіді авторів, проте його достатньо для виокремлення основних закономірностей пошуку інформації з відкритих джерел.

Так, найбільш запитуваними є персональні дані особи, зокрема прізвище, ім'я, по-батькові, дата народження, місце проживання, а також ідентифікуюча інформація – номер мобільного телефону, адреси електронної поштової скриньки, нікнейми (username), акаунти в соціальних мережах, зв'язки, рід діяльності або захоплення тощо.

Крім того, велика кількість інструментів пов'язана з дослідженням технічної інфраструктури доступу до мережі "Інтернет". Зокрема, за допомогою сервісів Shodan, Maltego та ін. можна досліджувати запущені служби через відкриті порти в мережі, виявляти вразливості тощо. Захист вищевказаної інформації має забезпечуватися через комплексний та системний підхід, що виражається у сталій побудові політик безпеки та комплексу системи захисту інформації.

Не менш важливим є потреба в класифікації інформації, яка може бути отримана за результатами OSINT-дослідження. Зокрема, Х. П. Ярмакі, С. С. Музика пропонують класифікувати конфіденційну інформацію за такими критеріями [12, с. 98]:

1) за правом власності: а) державна; б) приватна;

2) за правом доступу: а) під час виконання посадовими особами службових повноважень; б) власника та осіб, яким надано це право;

3) за галуззю застосування: а) комерційна; б) банківська; в) податкова; г) адвокатська; д) судова та ін.

З точки зору кібербезпеки наведені варіанти класифікації конфіденційної інформації не є інформативними та не визначають рівень критичності відомостей в разі їх потенційного витоку.

Так, пропонується класифікувати інформацію за рівнем критичності наслідків від її витоку (табл. 4).

Таблиця 4

Класифікація інформації за рівнем критичності наслідків від її витоку

Рівень критичності інформації	Приклад інформації	Наслідки витоку
1	2	3
І рівень Висококритична інформація (стратегічні та секретні дані)	· Деталі стратегічних військових операцій. · Секретні розробки у сфері науки чи технологій. · Фінансові або банківські дані високого рівня чутливості. · Державна таємниця	1. Загроза національній безпеці. 2. Фізична небезпека для осіб. 3. Масштабні економічні або соціальні наслідки. 4. Необхідність серйозного відновлення репутації чи правової відповідальності
ІІ рівень Критична інформація (конфіденційні дані)	· Персональні дані (ПІБ, паспортні дані, банківські реквізити). · Комерційна таємниця (контракти, бізнес-плани, інформація про клієнтів). · Відомості про партнерів чи постачальників, які є частиною договірних відносин	1. Значні фінансові втрати. 2. Репутаційні збитки. 3. Потенційні судові позови чи штрафи за недотримання законодавства

Продовження табл. 4

1	2	3
III рівень Помірно критична інформація (внутрішні дані)	· Внутрішня документація, що не містить конфіденційної інформації. · Робочі розклади співробітників. · Звичайна внутрішня комунікація (без комерційної або стратегічної важливості)	1. Незначні репутаційний вплив. 2. Тимчасові незручності в роботі
IV рівень Некритична інформація (публічні дані)	· Загальнодоступна інформація на вебсайтах організацій (контакти, публічні звіти, розклади подій). · Відкриті дані з державних реєстрів або статистичних звітів. · Матеріали, що вже перебувають у публічному просторі (наприклад, рекламні матеріали)	Відсутні або мінімальні

1. **Некритична та помірно критична інформація** містить публічні дані, витік яких не створює жодних загроз для організацій чи осіб. Ці дані, як-от контактна інформація, публічні звіти або матеріали з вебсайтів, вже доступні для широкого загалу. Помірно критична інформація, наприклад внутрішня документація або звичайна робоча комунікація, має низький ризик, але її витік може спричинити незначні репутаційні чи організаційні втрати.

2. **Критична інформація** - дані, що мають конфіденційний характер і витік яких може завдати значної шкоди. Сюди належать персональні дані, комерційна таємниця, інформація про клієнтів та партнерів. Витік такої інформації може призвести до фінансових збитків, втрати довіри клієнтів, судових позовів чи штрафів за порушення законодавства щодо захисту даних.

3. **Висококритична інформація:** інформація містить стратегічні або секретні дані, витік яких може мати катастрофічні наслідки. Це державна таємниця, військові стратегії, секретні технологічні розробки чи високочутливі фінансові дані. Наслідки витоку можуть включати загрози національній безпеці, фізичну небезпеку для осіб, а також серйозні економічні або соціальні потрясіння. Захист таких даних потребує найвищого рівня заходів безпеки.

Одночасно з цим користувачам мережі “Інтернет” з метою запобігання несанкціонованому збору інформації про них необхідно дотримуватися таких рекомендацій:

1. **Мінімізація публікації особистої інформації в мережі “Інтернет”, зокрема соціальних мережах:** не розголошуйте конфіденційну інформацію, таку як паспортні дані, адреси, дати народження чи фінансові дані, у публічному доступі. Також необхідно здійснювати контроль за обсягом інформації, яка публікується у соціальних мережах, зокрема про місцезнаходження, рід діяльності чи особисті контакти.

Крім того, доцільно встановити налаштування конфіденційності у своїх облікових записах, обмеживши доступ до особистої інформації тільки для друзів чи знайомих.

2. **Використання складних паролів та їх оновлення, не рідше ніж 1 раз на місяць, враховуючи, що для кожного ресурсу має бути власний унікальний пароль.** Паролі мають складатися не менш як з 8 символів, містити літери верхнього та нижнього регістру, символи та цифри. Водночас збереження паролів в облікових записах є небезпечним у разі його компрометації, більш надійним з точки зору кібербезпеки є так звані Key-менеджери.

3. **Використання двофакторної автентифікації**. Входячи у свої облікові записи, більшість людей використовують лише один спосіб підтвердження особи. Зазвичай це – введення логіна і пароля. Проте це недостатньо надійно, особливо якщо як пароль ви використовуєте просте слово чи комбінацію, які хакерам легко зламати. Двофакторна автентифікація – це використання одразу двох різних способів підтвердження. Вона дає можливість значно підсилити рівень вашого захисту та убезпечити персональні дані від кіберзловмисників.

4. **Використання додаткових засобів для реєстрації на сервісах та ресурсах в мережі "Інтернет"**. Використовуйте окрему поштову скриньку або номер мобільного телефону для реєстрації на вебсайтах чи підписки на розсилки.

5. **Моніторинг цифрової безпеки.** Використовуйте інструменти для перевірки витоків особистих даних (наприклад, сервіси на кшталт "Have I Been Pwned"). Регулярно перевіряйте, чи немає ваших даних у загальнодоступних джерелах.

6. **Резервне копіювання даних**. Регулярно створюйте резервні копії важливої інформації та зберігайте їх у захищених місцях. Використовуйте хмарні сервіси із функціями безпеки для зберігання копій файлів.

Висновки

OSINT-інструменти є потужними засобами для аналізу відкритих джерел. Їх основними перевагами є автоматизація процесів збору та обробки даних, широкі можливості для візуалізації інформації та високий рівень деталізації. Однак виявлено й недоліки, зокрема ризик помилкових результатів через неправильну інтерпретацію даних, необхідність спеціальних навичок для роботи з інструментами та можливість зловживання отриманою інформацією.

На основі результатів роботи OSINT-інструментів встановлено, що дані, які підлягають захисту, можуть бути класифіковані за рівнем критичності наслідків їх витоку. Визначено чотири рівні: некритична інформація, помірно критична інформація, критична інформація та висококритична інформація. Такий підхід дає змогу чітко розставити пріоритети в захисті інформації та організувати ефективну систему безпеки.

Також запропоновано методологію мінімізації ризиків для персональних даних та конфіденційної інформації.

Список літератури

1. *Ghioni R., Taddeo M., Floridi L. Open source intelligence and AI: a systematic review of the GELSI literature. AI & Soc. 2024. Vol. 39. 1827–1842. Doi: https://doi.org/10.1007/s00146-023-01628-x.*

2. *Главацька, А., Ангельська О., Опірський І. Дослідження технології використання Osint як нової загрози з деанонімізації особи в інтернет просторі. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка". 2024. 1(25). 19–50. Doi: https://doi.org/10.28925/2663-4023.2024.25.1950.*

3. *Фітнес-додаток Strava розкриває конфіденційну інформацію про своїх користувачів. Судово-юридична газета. 2024. URL: https://sud.ua/uk/news/obshchestvo/315235-fitnes-prilozhenie-strava-raskryvaet-konfidentsialnuyu-informatsiyu-o-svoikh-polzovatelyakh.*

4. *Soar. URL: https://soar.earth/.*

5. *Yang L., Driscol J., Sarigai S., Wu Q., Chen H., Lippitt C. D. Google Earth Engine and Artificial Intelligence (AI): A Comprehensive Review. Remote Sens. 2022. 14. 3253. Doi: https://doi.org/10.3390/rs14143253.*

6. *coldfusion39. geOSINT. coldfusion39. 2016. URL: https://github.com/coldfusion39/geOSINT.*

7. *Simon K. Digital 2024: Ukraine. 2024. URL: https://datareportal.com/reports/digital-2024-ukraine.*

8. *ТОВ "АРТЕЛЛЕНС УКРАЇНА". Artellence. URL: https://artellence.com.*

9. *Lampyre.io Quick Start Guide 2022. URL: https://lampyre.io/assets/documents/Lampyre_Quick_Start_Guide.pdf.*

10. *Ercolani V. J., Patton M. W., Chen H. Shodan visualized. 2016 IEEE Conference on Intelligence and Security Informatics (ISI). Tucson, AZ, USA, 2016. Pp. 193- 195. Doi: https://doi.org/10.1109/ISI.2016.7745467.*

11. *Пашнєв Д. В., Шматков Д. І., Коломійцев С. О. та ін. Інструменти та методи AI та OSINT для розшуку дітей, які зникли безвісти, депортовані або примусово переміщені. Використання розвідданих на основі відкритих джерел, їх аналізу та новітніх технологій, включаючи розпізнавання облич : методичні рекомендації / МВС України, Харків. нац. ун-т внутр. справ. Харків : ХНУВС, 2024. 80 с.*

12. *Ярмакі Х. П., Музика С. С. Класифікація конфіденційної інформації. Південноукраїнський правничий часопис. 2021. № 1. С. 94–98. Doi: https://doi.org/10.32850/sulj.2021.1.16.*

RESEARCH OF EXISTING OSINT TOOLS AND APPROACHES IN THE CONTEXT OF PERSONAL AND STATE INFORMATION SECURITY

V. S. Ivkova, I. R. Opirskyy

Lviv Polytechnic National University,
Department of Information Protection

The article examines modern tools and approaches to conducting OSINT — the analysis of open sources of information. The key role of OSINT, along with other intelligence methods such as HUMINT, IMINT, SIGINT, MASINT and GEOINT, lies in creating a holistic information field that combines open, technical, human and geospatial sources. The constant development of methodologies and improvement of automation tools allows to increase the efficiency and accuracy of the analysis of the received information, which makes OSINT one of the most important elements of modern intelligence.

The study examined the main data sources, such as public registers, social networks, news resources, geospatial data and other open resources. The key stages of collecting, analyzing and processing information, which is an integral part of OSINT research, are highlighted.

Special attention is paid to Geospatial Intelligence tools with a comparative description of the most common solutions. Their functional capabilities, advantages, limitations and areas of application are investigated.

An analysis of popular OSINT tools, such as "Maltego", "Shodan", and platforms for monitoring social media was conducted. The latest approaches were analyzed, including the use of artificial intelligence, automation of analysis processes and ensuring data transparency.

The article assessed the degree of threat to personal data and confidential information in the context of OSINT. It was determined which data requires protection, and appropriate measures were provided to minimize risks, which will include classifying data by confidentiality level.

Effective strategies for countering OSINT were proposed, in particular in terms of detecting and neutralizing information leaks, using adequate data protection tools, including encryption, monitoring systems and access auditing, and development prospects in the conditions of a modern information society were outlined.

Keywords: data analysis, open sources of information, OSINT tools, information security, confidential information, classification of confidential information, OSINT.