МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет «Одеська юридична академія»

О. О. Торбас

OSINT ПРИ РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

Підручник

Видавництво
«Юридика»
2024

УДК 004.77:343.132(075.8)
Т59

Рецензенти:

Тетерятник Ганна Костянтинівна — докторка юридичних наук, професорка, завідувачка кафедри кримінального процесу та криміналістики Одеського державного університету внутрішніх справ;

Аркуша Лариса Ігорівна — докторка юридичних наук, професорка, завідувачка кафедри криміналістики, детективної та оперативно-розшукової діяльності Національного університету «Одеська юридична академія»

Рекомендовано до друку Вченою радою
Національного університету «Одеська юридична академія»
(протокол № 5 від 06.03.2024 р.)

Торбас О. О.

Т59 OSINT при розслідуванні кримінальних правопорушень : підручник / О. О. Торбас. — Одеса : Видавництво «Юридика», 2024. — 180 с.

ISBN 978-617-8182-13-7

Підручник «OSINT при розслідуванні кримінальних правопорушень» надає читачам необхідні та достатні знання щодо інструментів, методів та стратегій ефективного збору, аналізу та використання даних із відкритих джерел при розслідуванні кримінальних правопорушень. Підручник охоплює широкий спектр тем, включаючи особливості використання інтернет-джерел, соціальних мереж, публічних баз даних та інших ресурсів у процесі здійснення кримінальних проваджень. Наукове видання розраховане як на здобувачів закладів вищої освіти юридичного профілю, так і на практикуючих юристів — суддів, прокурорів, слідчих, дізнавачів, адвокатів та інших.

УДК 004.77:343.132(075.8)

ISBN 978-617-8182-13-7

ЗМІСТ

Тема 1

ПОНЯТТЯ ТА ЗАГАЛЬНІ ВИМОГИ ПРОВЕДЕННЯ OSINT РОЗСЛІДУВАНЬ

1.1 ПОНЯТТЯ OSINT. OSINT ТА СУМІЖНІ ДИСЦИПЛІНИ РОЗВІДКИ

«У листопаді 2017 р. компанія Strava, яка займається підтримкою мобільного додатку та сайту для відстеження спортивної активності через GPS, опублікувала теплову карту активності з усіма відкритими даними від користувачів. Як зазначив тоді один із фахівців Strava, карта показує у шість разів більше інформації, аніж початкова версія 2015 року, а саме — 10 терабайтів даних про активність близько 10 мільйонів людей: від бігу та катання на велосипеді до скелелазіння, серфінгу та йоги. Загалом було зібрано понад одного мільярда маршрутів, загальна довжина яких становить 27 мільярдів кілометрів.

Хоча карта була опублікована в листопаді минулого року, деякі цікаві речі, пов'язані з нею, користувачі почали помічати тільки у січні 2018 р. Студент Австралійського національного університету Натан Расер зауважив, що "освітлені" на тепловій карті регіони в районі Сирії та Сахари зазвичай не зайняті цивільними особами, що свідчить про присутність сил безпеки біля військових баз. "Точкою відліку" інформаційної епопеї з тепловою картою став твіт Расера — хлопець помітив, що фітнес-додаток розкриває місце розташування військових баз США.

“Як тільки ви зможете ідентифікувати людину, що використовувала додаток, дані стають дуже цінними,” — наголосив німецький аналітик з безпеки Тобіас Шнайдер. Фахівцю вдалося виявити імена 573 людей, які щоранку бігали навколо стоянки штаб-квартири британської розвідки. Ймовірно, що ці люди там же і працюють, тому ця інформація зацікавила б багатьох. Шнайдер стверджує, що можна легко знаходити когось, хто працює на секретному об’єкті та відстежувати його переміщення на інші точки.

А от Натаніель Раймонд, директор “Сигнальної програми з безпеки людини та техніки”, разом зі своєю командою визначили імена та маршрути щоденних “прогулянок” восьми іноземців, що працюють в агентствах з надання допомоги та ООН у Могадішо, столиці Сомалі, що є найнебезпечнішим містом у світі.

У свою чергу, журналіст Крістофер Міллер у своєму Твіттері відзначив, що дані теплової карти можуть бути корисними для оцінки військових сил на сході України. Він навів фрагмент аналізу, що показує рух російських військ поблизу Мар’їнки. Міллер також звернув увагу на те, що за допомогою карти можна проаналізувати бойові дії біля Донецького аеропорту, виявити ключові позиції та шляхи просування ворожих військ. З огляду на резонанс, викликаний оприлюдненням теплової карти активності, компанія Strava заявила, що вони прагнуть працювати з військовими та представниками влади для вирішення проблем. У компанії зазначили, що вони хочуть допомогти зрозуміти налаштування додатку, щоб користувачі змогли контролювати конфіденційність даних задля уникнення “незручних” ситуацій»[1].

Власне історія з фітнес-додатком демонструє силу, значення та інколи несподівані результати аналізу даних, які знаходяться у відкритому доступі. Сучасне суспільство все більше і більше залежить від інформаційних технологій, що проявляється у будь-яких сферах життя, в тому числі і злочинності. Тому правоохоронні органи не мають права

[1] Левков О. Шпигунська STRAVA : як фітнес-додаток розкриває таємниці військових баз. Інформаційно-консалтингова компанія «Defense Express» : вебсайт. URL: https://old.defence-ua.com/index.php/statti/4492-shpyhunska-strava-yak-fitnes-dodatok-rozkryvaye-tayemnytsi-viyskovykh-baz

ігнорувати відомості, які можуть бути отримані за допомогою OSINT розслідувань з будь-яких доступних джерел.

OSINT (open source intelligence — розвідка відкритих баз даних) в цілому можна визначити як розвідку інформації, отриманої із загальнодоступних джерел, яка не потребує таємних методів збору[1]. Необхідно зробити уточнення, що термін «OSINT» є відносно уніфікованим у міжнародній спільноті, який розуміється всіма однаково. У зв'язку з цим, а також через неможливість провести якісний дослівний переклад українською, необхідно більш детально розібрати дві ключові складові OSINT — «розвідка» (intelligence) та «відкриті бази даних» чи «відкриті джерела» (open source).

Коли ведуть мову про аналітику будь-яких даних, часто використовують поняття «інформація» (information), «розвідка» (intelligence) та «аналіз» (analysis).

Інформація:

– знання в «сирому» вигляді.

Розвідка:

– інформація, яку можна зрозуміти;
– інформація, яка була оцінена в контексті її джерела та надійності.

Аналіз:

– розділення інформації на складові частини;
– визначення цих частин;
– відстеження інформації до їхнього джерела, щоб виявити загальні принципи, що лежать в її основі;
– формулювання звіту за результатами процесу аналізу.

Важливо правильно розуміти різницю між цими термінами та те, як вони взаємодіють, однак навіть на цьому прикладі можна помітити принципові відмінності. Інформація — це просто необроблені дані, в той час як розвідка передбачає обробку даних, оцінку їхньої надійності (верифікація)[2].

---

1 Sampson, Fraser. Intelligent evidence : Using open source intelligence (OSINT) in criminal proceedings. The Police Journal. 2016. 90. P. 3.

2 Criminal Intelligence. Manual for Analysts. United Nations Office on Drugs and Crime. 2011. URL: https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf

Інформація + оцінка = розвідка

Переважно термін «розвідка» використовується в контексті національної безпеки. Класичним прикладом використання розвідки є військова сфера. Під час війни від лідерів постійно вимагається прийняття стратегічних і тактичних рішень у польових умовах, для чого необхідно отримувати інформацію про ворога. Найчастіше для цього використовували шпигунів.

Сьогодні шпигуни — це лише один з багатьох способів отримання цінних розвідданих, адже на даний момент вже розроблені цілі «дисципліни» зі збору інформації:

- людська розвідка (Human Intelligence — HUMINT) — це збір інформації з людських джерел. Збір може здійснюватися відкрито, наприклад, коли уповноважені особи опитують свідків або підозрюваних, або це може бути зроблено таємно (наприклад, шпигунами);
- розвідка сигналів (Signals Intelligence — SIGINT) передбачає збір відомостей електронних сигналів кораблями, літаками, наземними станціями або супутниками. Комунікаційна розвідка (COMINT) є різновидом SIGINT і стосується перехоплення комунікацій;
- розвідку зображень (Imagery Intelligence — IMINT) іноді також називають фоторозвідкою (PHOTINT). Одна з найперших форм IMINT була застосована під час Громадянської війни в США, коли солдатів відправляли на повітряних кулях для збору розвідданих. IMINT більшою мірою застосовувався під час Першої та Другої світових воєн, коли обидві сторони робили фотографії з літаків. Геопросторова розвідка (Geospatial Intelligence — GEOINT) є розвідувальною діяльністю, що полягає в дослідженні та аналізі зображень і геопросторових даних, в результаті яких описуються, оцінюються і візуалізуються фізичні характеристики та географічно локалізовані процеси на Земній кулі;
- розвідка сигнатур (Measurement and Signatures Intelligence — MASINT) є відносно маловідомою дисципліною збору відомостей, яка стосується можливостей зброї та промислової

діяльності. MASINT включає розширену обробку та використання даних, зібраних із систем збору даних IMINT і SIGINT. Телеметрична розвідка (Telemetry Intelligence — TELINT) іноді використовується для встановлення даних, які передаються зброєю під час випробувань, тоді як електронна розвідка (Electronic Intelligence — ELINT) використовується для визначення електронного випромінювання, що випромінює сучасна зброя та системи спостереження. І TELINT, і ELINT можуть бути типами SIGINT і сприяти MASINT;

– розвідка з відкритих джерел (Open-Source Intelligence — OSINT) відноситься до збору інформації з джерел, які є загальнодоступними, включаючи інформацію, отриману із засобів масової інформації (газети, радіо, телебачення тощо), професійні та академічні тексти (статті, тези конференції та ін.), а також публічні дані (урядові звіти, демографічні дані, різні виступи тощо)[1].

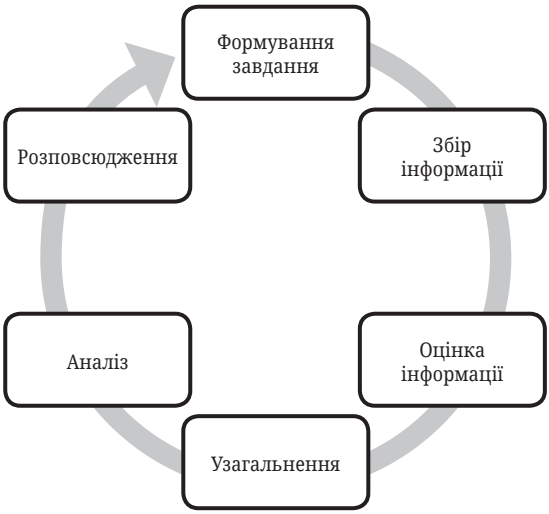
1.2 ЕТАПИ OSINT РОЗСЛІДУВАННЯ

Розвідку зазвичай поділяють на два види:

– стратегічна розвідка, яка фокусується на довгострокових цілях правоохоронних органів. У даному випадку, як правило, досліджуються поточні та нові тенденції у злочинному середовищі, загрози громадській безпеці, розробка програм протидії та ймовірні шляхи удосконалення державної політики чи законодавства;
– оперативна розвідка, яка зазвичай використовується слідчою групою щодо конкретних кримінальних правопорушень або окремих їхніх елементів. Вона включає гіпотези та висновки щодо конкретних злочинних мереж, осіб або груп осіб, залучених до незаконної діяльності, обговорення їхніх можливостей та намірів, які можуть бути використані для ефективних дій правоохоронних органів.

[1] Intelligence Studies : Types of Intelligence Collection. Learning Commons : website. URL : https://usnwc.libguides.com/c.php?g=494120&p=3381426

У літературі досить поширеним є наступний цикл проведення розвідки (мал. 1.1):



Мал. 1.1. Етапи (цикли) OSINT розслідування

1. Формування завдання

Результат розвідки насамперед має ґрунтуватися на потребах клієнтів, тобто споживачів «аналітичного продукту». Саме вони мають чітко визначити завдання, яке необхідно виконати. В той же час будь-яке OSINT розслідування має базуватися на принципі партнерства, тобто щоб і клієнт, і аналітик були відповідальними за спільну роботу, адже вимоги до кінцевого результату мають бути чітко визначені і зрозумілі всім сторонам.

Питання, які необхідно вирішити на цьому етапі:

– хто ставить завдання?
– яка кінцева мета завдання?
– які конкретно завдання необхідно виконати?

Важливо, щоб була активна взаємодія між клієнтом та аналітиком, що забезпечить ефективність виконання завдання. Аналітик повинен

бути об'єктивним, не піддаватися будь-яким упередженням, але в той же час має бути готовим прийняти завдання без зауважень.

Постановка завдань може мати дві основні форми:

– клієнту потрібен аналітичний продукт щодо конкретного предмета, події, особи тощо;
– клієнт формулює загальні очікування для аналітика щодо певної сфери або загрози.

Після чіткого визначення завдання аналітичний підрозділ починає планування наступних фаз циклу.

2. Збір інформації

Процес розвідки спирається на здатність знаходити та використовувати дані. Однак перша проблема, яку потрібно вирішити, полягає у зборі та збереженні таких даних, які можуть мати безліч форм — від електронних до письмових.

На цій ранній стадії слід бути обережним, щоб уникнути перевантаження даними, що завжди є проблемою для будь-якого аналітика. В той же час ігнорування даних через їхню нерелевантність може стати причиною проблем у майбутньому.

Будь-який збір інформації має відбуватися відповідно до визначеного плану. Питання планування всіх дій у процесі розвідки є особливо важливим на етапі збору інформації. І в оперативному, і в стратегічному аналізі розвідданих теми та обсяг аналізу повинні бути чітко визначеними. План збору відомостей, в якому визначено необхідну інформацію та викладено засоби її отримання, є обов'язковим для забезпечення впорядкованого та точного збору інформації.

План збору повинен включати:

– категорії інформації, які є важливими для аналізу;
– конкретні дані, необхідні для проведення аналізу;
– можливі джерела інформації;
– план із зазначенням того, коли та хто отримував доступ до інформації.

Існує три основні типи джерел інформації: відкриті, закриті та таємні.

Відкриті джерела — інформація, яка є загальнодоступною. Одним із дуже важливих видів інформації з відкритих джерел є так звана «сіра

література». Вона може складатися з дослідницьких, технічних, економічних звітів, технічної документації, тез конференції, дисертацій, тематичних інформаційних бюлетенів тощо. Однією з головних труднощів у роботі з цим типом джерел є їхня оцінка, оскільки інформація, що знаходиться у відкритому доступі, часто може бути упередженою чи неточною.

Закриті джерела — це інформація з обмеженим для громадськості доступом. Інформація із закритих джерел часто відображається у формі структурованих баз даних. У контексті аналізу кримінальної розвідки ці бази даних в основному включатимуть персональні дані, зібрані в рамках поточних цільових операцій, або кримінальні записи, реєстраційні дані транспортних засобів, дозволи на зброю тощо.

Таємною є інформація, зібрана за допомогою спеціальних таємних засобів, включаючи використання людських і технічних ресурсів. Використання таємної інформації може значно підвищити якість аналітичного продукту, оскільки він, як правило, має високу точність. Однак це також може зробити аналітичний продукт значно менш ефективним через обмеження на його розповсюдження.

Аналітик повинен вміти аналізувати всі типи даних, обираючи джерела з огляду на їхню релевантність, а не на легкодоступність. Аналітик, який працює з усіма джерелами, повинен уникати упередження про те, що лише інформація з обмеженим доступом може бути достовірною та релевантною. Використання відкритих джерел часто створює додаткову довіру до кінцевого продукту або спонукає до збору подальшої закритої чи секретної інформації.

Вибір джерел також можна розглядати з точки зору економічної доцільності. Використання відкритих джерел замість джерел з обмеженим доступом може значно скоротити бюджет або дозволити отримати більше інформації в межах встановленого бюджету. Використання відкритих джерел також може допомогти захистити або зберегти джерела закритої та секретної інформації.

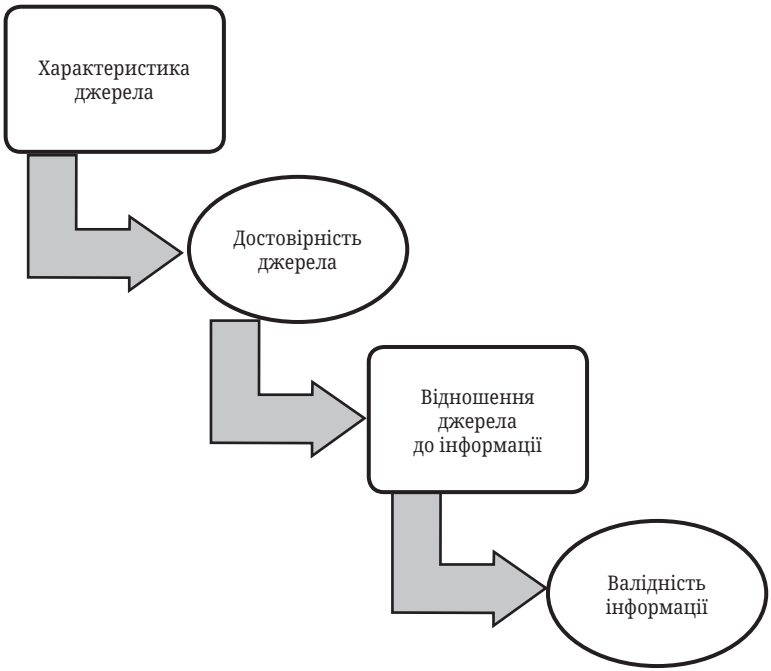
План збору розвідувальних даних може містити такі елементи:

– визначення проблеми — проблема розвідки повинна бути сформульована точно і чітко;
– мета проєкту — в ідеалі визначення вимоги до результатів розвідки одним реченням;

– «охоплення» проєкту — розширює визначення мети проєкту та встановлює дії, які очікуються від аналітика. Він також містить детальний опис обсягу та мети збору заходів і джерел.

3. Оцінка інформації

Достовірність висновку безпосередньо пов'язана з якістю даних, що були використані аналітиками. Таким чином, оцінка даних є ключовим елементом циклу розвідки. Її слід проводити одночасно з отриманням даних або відразу після цього, щоб переконатися, що оцінка відбувається нерозривно з контекстом, в якому інформація була отримана. Також вимагається окрема оцінка надійності джерела та достовірності і точності інформації (мал. 1.2).



Мал. 1.2. Етапи оцінки джерела та самої інформації

Джерело та фактична інформація повинні бути оцінені незалежно одна від одного, тому вкрай важливо, щоб особа, яка заповнює звіт, добре знала систему оцінювання. Дві найбільш популярні системи — це системи «4 x 4» і «6 x 6».

При оцінці застосовуються три фундаментальні принципи:

1. Оцінка має бути об'єктивною, на оцінку не повинні впливати суб'єктивні судження будь-кого.

2. Оцінка джерела має відбуватися окремо від оцінки інформації.

3. При цьому оцінка має проводитись максимально наближено до джерела.

Система оцінки 4 x 4

Оцінка джерела

A	– жодних сумнівів щодо автентичності, достовірності, правдивості джерела; – попередні приклади повної надійності
B	– джерело, з якого була отримана інформація, в більшості випадків було надійним
C	– джерело, з якого була отримана інформація, в більшості випадків було ненадійним
X	– надійність джерела оцінити неможливо

Оцінка інформації

1	– немає сумнівів у точності інформації
2	– інформація особисто відома джерелу, з якого вона отримується, але не відома аналітику, який її отримує; – логічна сама по собі; – узгоджується з іншою наявною інформацією
3	– інформація особисто джерелу невідома, але підтверджується іншою інформацією
4	– інформація особисто джерелу не відома та не може бути незалежно підтверджена

Система оцінки 6 х 6

Надійність джерела

A Повністю надійне	– жодних сумнівів щодо автентичності, достовірності, правдивості джерела; – попередні приклади повної надійності
B Зазвичай надійне	– певні сумніви щодо автентичності, достовірності, правдивості чи компетентності джерела (одне з перелічених); – попередні приклади відносної надійності
C Відносно надійне	– сумніви щодо автентичності, достовірності, правдивості чи компетентності джерела (два і більше перелічених); – попередні приклади періодичної надійності
D Зазвичай ненадійне	– явні сумніви щодо автентичності, достовірності, правдивості чи компетентності джерела; – попередні прикладі нерегулярної надійності
E Ненадійне	– впевненість у відсутності автентичності, достовірності, правдивості чи компетентності джерела; – приклади ненадійності
F	– неможливо оцінити

Оцінка інформації

1 Підтверджено	– підтверджено іншими незалежними джерелами; – логічна сама по собі; – узгоджується з іншою інформацією
2 Вірогідно правда	– не була підтверджена незалежними джерелами; – логічна сама по собі; – узгоджується з іншою інформацією
3 Ймовірно правда	– не була підтверджена; – логічна сама по собі; – дещо узгоджується з іншою інформацією
4 Сумнівно правда	– не була підтверджена; – нелогічна; – сумнівна на момент отримання, хоча потенційно може бути правдивою
5 Неправдоподібно	– підтверджується протилежна інформація; – нелогічна сама по собі; – суперечить іншій інформації
6	– неможливо оцінити

Таким чином, аналізуючи джерело та інформацію, аналітики присвоюють їм відповідні оцінки, а не описують власні роздуми щодо достовірності джерела чи правдивості інформації. Наприклад, оцінка А2 за системою «6 х 6» вказує на те, що така інформація фактично без застережень може використовуватися в розслідуванні, в той же час оцінка С3 за системою «4 х 4» вимагає вкрай критичного ставлення до такої інформації

4. Узагальнення

Узагальнення — це передача зібраної інформації до системи, де ця інформація має зберігатися (картотека, комп'ютерна база даних тощо) у структурованому (індексованому, з перехресними посиланнями) форматі, який забезпечує швидкий та повний доступ до такої інформації. Узагальнення не означає збереження всієї інформації, яка була отримана, на цьому етапі частина інформації повинна відсіюватися (нерелевантна, непідтверджена тощо).

5. Аналіз

Цей етап є ключовим. Аналіз можна описати як поглиблене дослідження значення та суттєвих характеристик наявної інформації. Аналіз допомагає визначити прогалини, сильні та слабкі сторони розслідування, сформувати подальшу стратегію розслідування.

Обсяг аналізу та його загальна достовірність залежать від рівня та точності отриманої інформації в поєднанні з необхідними навичками аналітика. Аналіз — це циклічний процес, який можна використовувати для вирішення всіх типів завдань у правоохоронній діяльності.

Інтеграція даних є першою фазою аналітичного процесу. Вона передбачає поєднання інформації з різних джерел для підготовки до формулювання висновків. Для відображення цієї інформації можна використовувати різні методи, найпоширенішим з яких є використання методу створення діаграм:

- діаграма зав'язків — щоб показати зв'язки між об'єктами, які фігурують у розслідуванні;
- діаграма подій — для відображення хронологічних зав'язків між об'єктами або послідовністю подій;
- графіки потоків товарів та речей — щоб досліджувати рух грошей, наркотиків, викрадених або інших товарів;

– діаграма активності — для встановлення дій, що пов'язані із певною злочинною операцією;
– фінансове профілювання — для виявлення прихованих доходів фізичних або юридичних осіб та виявлення ознак економічної злочинності;
– діаграми частот — для організації, узагальнення та інтерпретації кількісної інформації;
– кореляція даних — для ілюстрації зв'язків між різними даними.

Наступним кроком в аналітичному процесі є інтерпретація інформації, яка вимагає «виходу за межі доступних фактів». Дисциплінований підхід до аналізу вимагає оцінки максимальної кількості інформації під час інтеграції, щоб визначити її релевантність. Виключення інформації на початку даного процесу може призвести до того, що буде пропущена важлива інформація. Це може призвести до неправильного аналізу, що зрештою може поставити під загрозу результати самого розслідування.

Інтеграція даних не є самоціллю, адже створення будь-яких діаграм є лише інструментом, який використовується аналітиками для отримання необхідного результату. Першим по-справжньому аналітичним продуктом у даному процесі є *висновок*. Висновок має виходити з умов, а не навпаки. Поширеною є помилка, коли висновок роблять інтуїтивно, а далі шукають умови, які б цей висновок підтвердили. Тому постійно необхідно повторювати собі твердження «умови, які дозволили мені зробити цей висновок, були...», а не «умови, які підтверджують мій висновок, були...» (однак при представленні результатів відправною точкою є саме висновок — загальна ідея — за якою слідують умови, з яких вона була сформульована).

«Умови» використовуються для ідентифікації фактів або фрагментів інформації, які у поєднанні дають змогу зробити певний висновок. Умови є першим і ключовим етапом справжнього процесу аналізу даних, на відміну від їхнього опису чи узагальнення. Розуміння сутності процесу ідентифікації умов є ключовим для формування висновків.

Існує чотири типи висновків:

– гіпотеза — попереднє твердження, теорія, яка потребує додаткової інформації для підтвердження або спростування;

– передбачення — висновок про те, що станеться в майбутньому;
– розрахунок — висновок, зроблений про ціле на основі окремих частин;
– кінцевий висновок — добре підтверджене пояснення.

Слід зазначити, що всі висновки вимагають певної перевірки перш ніж їх можна буде прийняти як факт.

6. Розповсюдження

Аналітик несе відповідальність за розповсюдження аналітичних матеріалів цільовій аудиторії. Значна частина розповсюдження може здійснюватися за допомогою коротких нотаток. Але аналітики повинні мати можливість проводити усні брифінги щодо більш масштабних розслідувань і писати структуровані звіти з детальним описом наявної на даний момент інформації.

Розповсюдження може здійснюватися в різних формах, наприклад:
– структуровані формалізовані звіти;
– структуровані та формальні усні доповіді з супровідною документацією;
– щотижневі огляди у формі бюлетенів;
– спеціальні брифінги для працівників правоохоронних органів.

Фаза розповсюдження завершує початковий цикл процесу розвідки.

Повторна оцінка

Повторна оцінка передбачає безперервний перегляд усього циклу розвідки, щоб визначити способи, за допомогою яких можна покращити будь-який етап. Повторна оцінка має відбуватися протягом усього процесу, а не просто виступати в якості останнього етапу. Повторна оцінка може проводитись відносно:
– процесу;
– аналітичного продукту;
– використання аналітичного продукту;
– ефективність звітності тощо[1].

[1] Criminal Intelligence. Manual for Analysts. United Nations Office on Drugs and Crime. 2011. URL: https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf

1.3 ПОНЯТТЯ ТА ВИДИ ВІДКРИТИХ ДЖЕРЕЛ

Щоб визначити сутність інформації з відкритих джерел, спочатку необхідно встановити, чим являються самі відкриті джерела. Інформація з відкритих джерел не є тотожною персональним даним, але може містити чи складатися з таких відомостей. Традиційно персональні та неперсональні дані розрізняються за можливістю ідентифікації фізичної особи. Персональні дані дозволяють «встановити» людину. Той факт, чи є персональні дані відкритими, в даному випадку не має значення. Відомості з відкритих джерел, у свою чергу, можуть бути персональними та неперсональними.

Дані з відкритих джерел (відкриті дані) не мають офіційного визначення в будь-якому правовому документі. У багатьох документах цей термін використовується без визначення, але в цілому можна зробити висновок, що така інформація характеризується як *загальнодоступна*. «Відкриті джерела» можна визначити як інформацію, надану будь-якою особою чи групою осіб «без очікування на конфіденційність»[1]. Іншими словами, це «інформація, яка не захищена від публічного розголошення»[2]. Те, що інформація є загальнодоступною, не обов'язково означає, що вона безкоштовна або легкодоступна. Існує кілька загальнодоступних інформаційних платформ, які вимагають реєстрації, автентифікації або оплати (наприклад, пошукова система перевірки особистості pipl). Інтелектуальні дані, надані цими комерційними платформами та постачальниками послуг, вважаються відкритими, оскільки «відкритий» означає відсутність бар'єрів при користуванні, а не відсутність оплати чи реєстрації[3].

Концепція відкритих даних як така не є новою, в той же час бум соціальних мереж та інших джерел в інтернеті надав новий поштовх для оцінки даного поняття. Проте це не означає, що дані з відкритих

---

1 Staniforth, A., 2016. Police Use of Open Source Intelligence: The Longer Arm of Law, in: Akhgar, B., Bayerl, P.S., Sampson, F. (Eds.), Open Source Intelligence Investigation : From Strategy to Implementation, Advanced Sciences and Technologies for Security Applications. Springer International Publishing, Cham, pp. 21–31.

2 Ibid.

3 Gibson, H., 2016. Acquisition and Preparation of Data for OSINT Investigations, in: Akhgar, B., Bayerl, P.S., Sampson, F. (Eds.), Open Source Intelligence Investigation: From Strategy to Implementation, Advanced Sciences and Technologies for Security Applications. Springer International Publishing, Cham, pp. 69–93.

джерел обов'язково мають бути цифровими. Навіть якщо більшість даних з відкритих джерел сьогодні знаходиться в цифровій формі, фотографії чи будь-які паперові публікації можуть так само бути відкритими та загальнодоступними[1].

Конвенція Ради Європи про кіберзлочинність використовує термін «дані з відкритих джерел», але лише опосередковано посилається на них як на загальнодоступні дані, не даючи визначення. Управління ООН з наркотиків і злочинності (UNODC) описує дані з відкритих джерел як інформацію, яка є загальнодоступною, і додає, що однією з головних труднощів у роботі з цим типом джерел є їхня оцінка, оскільки інформація у відкритому доступі часто може бути упередженою або неточною. У своєму Посібнику з відкритих розвідувальних даних НАТО вперше відокремлює розвідувальні дані з відкритих джерел від академічних досліджень, журналістських та бізнес-розслідувань. Інформація з відкритих джерел, відповідно до позиції НАТО, є інформацією, яка розповсюджується серед широкого загалу і включає газети, книги, радіопередачі, щоденні звіти тощо.

У Протоколі Берклі зазначається, що інформація у відкритому доступі включає загальнодоступну інформацію, яку будь-який представник громадськості може спостерігати, купувати чи запитувати, не вимагаючи особливого правового статусу чи несанкціонованого доступу. Інформація із закритих джерел — це інформація з обмеженим доступом або доступом, що охороняється законом, але яка може бути отримана на законних засадах через приватні канали, такі як судові процеси, або запропонована добровільно.

Дані з відкритих джерел можуть бути створені будь-якою особою. В одних випадках автор такої інформації лишається невідомим, а надійність або точність такої інформації неможливо перевірити (наприклад, підроблені профілі в соціальних мережах). В інших випадках, наприклад у журналістських розслідуваннях, автор відомий, а інформація має високий ступінь достовірності та точності. Проте це все одно вважається даними з відкритих джерел. Тому для опису даних з відкритим джерелом не має значення, чи була перевірена їхня надійність і точність.

---

[1] EHE, Ricardo. The role of Open Source Intelligence in the Fight against Transnational Organized Crime — A European Perspective. Diplomová práce, vedoucí Butler, Eamonn. Praha : Univerzita Karlova, Fakulta sociálních věd, Katedra bezpečnostních studií, 2020.

Було б нереалістично обмежити визначення відкритих джерел даними, які є повністю безкоштовними, оскільки технічно потрібно враховувати вартість підключення до інтернету, навіть якщо газети чи соціальні медіа не знімають плату за доступ до своїх сайтів. Однак дані з відкритих джерел також можуть існувати в офлайновому світі. Наприклад, книга чи доповідь можуть бути загальнодоступними, але через свою ціну вони обмежені в доступності. З цієї причини фактор вартості не слід включати у визначення даних з відкритих джерел, швидше мова йде про доступність інформації для широкого загалу. Власне, обмежена кількість людей, які можуть переглядати інформацію, і викликає низку питань. Наприклад, власник закритого облікового запису в Facebook робить пост, які можуть бачити лише його підписники. Така інформація не вважається інформацією з відкритого джерела. Проте якщо у такого користувача 5000 друзів, то чи можна стверджувати, що мова все ще йде про закрите джерело? Крім того, кожен із цих друзів може ділитися інформацією зі своїми друзями, створюючи ефект снігової кулі. Те саме стосується газети, яка має тисячі передплатників, які можуть поширювати інформацію. Таким чином, можна дійти висновку, що різниця між відкритим та закритим джерелом полягає у можливості розповсюджувати інформацію. Проте такий висновок призводить до того, що будь-яка інформація, яка публікується в Facebook і якою можуть поділитися друзі чи підписники, автоматично має бути визначена як інформація з відкритих джерел. Це не означає, що будь-хто може робити будь-що з такою інформацією. По-перше, той факт, що такі дані є відкритими, не означає, що вони надійні. По-друге, дані з відкритих джерел можуть містити персональні дані. Якщо це так, то на них поширюються обмеження, які стосуються захисту персональних даних. Таким чином, науковці роблять висновок, що даними з відкритих джерел є будь-яка інформація, яка не обмежена доступністю лише певній групі людей та не обов'язково має бути надійною чи точною[1].

Поряд із доступністю відкритих джерел в інтернеті важливим аспектом є достовірність такої інформації та джерел. Якщо вести мову

[1] De Busser, Els. (2014). Open Source Data and Criminal Investigations: Anything You Publish Can and Will Be Used Against You. Groningen Journal of International Law. 2. 90.

про автентичність, то можуть виникнути проблеми, якщо достовірність інформації з відкритих джерел перевіряється за допомогою інформації, також отриманої з відкритих неперевірених джерел[1]. Крім того, наявність декількох джерел, які містять однакову інформацію, ще не означає, що така інформація була підтверджена. Тут важливо пам'ятати про надійність самого джерела. OSINT розслідування лише виграє в якості, якщо будуть використовуватися надійні і перевірені джерела. У сучасному світі, в якому панують соціальні мережі, забезпечення такої надійності є надзвичайно складним завданням. Тим не менш, численні приклади демонструють, що використання оперативно отриманої, але неперевіреної інформації з відкритих джерел може спричинити серйозні проблеми в майбутньому[2]. Зважаючи на інформацію, отриману з OSINT-джерел, також можна зіткнутися з фейковими новинами, неправдивими повідомленнями і дезінформацією. З домінуванням цифрових соціальних медіа та швидким розповсюдженням новин, які генеруються окремими людьми, вплив таких джерел стає все сильнішим. Без перевірки ця інформація може швидко почати сприйматися як надійна. Величезна кількість інформації на соціальних платформах та інших онлайн-медіа фактично унеможливлює для користувачів можливість відфільтрувати фейкові новини, що створює серйозну проблему навіть для організацій, що спеціалізуються на зборі, аналізі та оцінці інформації.

Власне, феномен фейкових нових є вкрай складним, оскільки тісно пов'язаний з людською поведінкою[3]. Оцінка достовірності новин та інформації надзвичайно складна і в багатьох випадках навіть неможлива. Проте це не означає, що кінцевий користувач не повинен намагатися самостійно виявити фейкові новини. Так, представники Міністерства з питань реінтеграції тимчасово окупованих територій України пропонують такі поради, які допоможуть розпізнати спотворення фактів:

---

1 Szabó, K. (2019): Az OSINT — Gondolatok a tevékenységről és az alkalmazás közegéről, Nemzetbiztonsági Szemle 2019/2

2 Dobák, Imre. (2023). OPEN SOURCE INTELLIGENCE AND THE RELIABILITY OF DATA. Conference: 1st BİLSEL INTERNATIONAL EFES SCIENTIFIC RESEARCHES AND INNOVATION CONGRESS 22-23 JULY 2023At: İZMİR/TURKEY

3 Langin, K. (2018): Fake news spreads faster than true news on Twitter — thanks to people, not bots, Social Science, doi:10.1126/science.aat5350

«1. Звертайте увагу на заголовки. Фейкові новини супроводжують гучні заголовки для привернення уваги. Часто вони можуть не відповідати змісту самого матеріалу.

2. Придивіться до адреси URL. Для розповсюдження фейків часто використовують копії відомих сторінок або сайтів. Від оригіналів вони можуть відрізнятися кількома літерами у вебадресі.

3. Намагайтеся встановити першоджерело повідомлення. Відсутність джерел інформації або посилання на анонімні витоки також є ознакою фейку.

4. Придивляйтеся до фото- та відеоконтенту. Фейкові новини можуть супроводжуватися невідповідними фотографіями та відео. Вони можуть бути вирваними з контексту — застарілими або зробленими в іншому місці.

5. Ретельно аналізуйте зміст інформації. Якщо матеріал базується на конспірологічних теоріях, емоційних накручуваннях або його думка подається як безапеляційний факт, то перед вами — спотворена інформація.

6. Звертайте увагу на баланс позицій. Висвітлення тільки однієї точки зору — ознака фейку. У достовірних виданнях зазвичай використовують кілька джерел новини»[1].

Серед західних медіа часто фігурують такі вісім порад:

1. Зверніть увагу на джерело — вивчіть сам сайт, його завдання, контактну інформацію тощо.

2. Читайте між рядками — заголовки можуть бути обурливими тільки для того, щоб людина «клікнула» на новину. А чи є там сама новина, про яку йдеться мова в заголовку?

3. Перевірте автора — виконайте швидкий пошук за ім'ям. Чи заслуговує він на довіру?

4. «Додаткові джерела?» — якщо в новині є посилання на додаткові джерела, то перевірте їх. Визначте, чи справді вони підтверджують те, що написано в новині.

5. Перевірте дані — повторне розміщення старих новин не означає, що вони мають відношення до поточних подій.

---

[1] Як розпізнати фейк? Міністерство з питань реінтеграції тимчасово окупованих територій України: офіційний вебсайт. URL: https://minre.gov.ua/2023/08/27/yak-rozpiznaty-fejk/

6. Можливо це жарт? Якщо новина є занадто фантастичною, це може бути сатира. Дослідіть сайт і автора, щоб переконатися.

7. Дослідіть власні упередження — подумайте, чи можуть ваші власні переконання вплинути на ваше судження.

8. Запитайте в експертів. Зверніться за допомогою до того, хто вважається експертом в даній сфері[1].

Також виділяють такі поради щодо оцінки фейкових новин:

1. Велике «ні-ні» для будь-яких фейкових новин, якщо ВСЕ НАПИСАНО ВЕЛИКИМИ ЛІТЕРАМИ або використовуються явно відфотошоплені зображення.

2. Дуже багато спливаючих вікон і рекламних банерів? Це ознака того, що новина створена як клікбейт.

3. Перевірте домен сайту, на якому читаєте новини. Наприклад, фейкові сайти часто додають «.co» до назви, щоб видати себе за відомі сайти (наприклад, «abcnews.com.co»).

4. Якщо Ви натрапили на невідомий сайт, то перевірте сторінку «Про нас», де має надаватися інформація про цей сайт. Також введіть в пошуковий запит Google назву цього сайту та допишіть «фейк» та почитайте результати, які знайдете.

5. Якщо в новині є додаткові посилання, то пройдіть за ними («сміття веде до ще більшого сміття»). Немає жодного посилання на першоджерело чи автора? Це також поганий знак.

6. Перевірте новину, знайшовши аналогічну новину, але на авторитетному джерелі.

7. Перевірте дату. У соціальних мережах часто можна натрапити на застарілі новини.

8. Читайте не лише заголовки. Часто інформація, яка подається в новині, не співпадає з заголовком.

9. Фотографії можуть вводити в оману. Використовуйте зворотній пошук за зображенням, щоб знайти оригінал фото та за яких умов його було зроблено.

10. Довіряйте своїм почуттям. Якщо новина вас дратує, то з великою долею вірогідності вона спеціально для цього була сформована.

---

[1] How to spot fake news. Cornel University Library : website. URL: https://guides.library.cornell.edu/evaluate_news/infographic

11. Якщо ви не впевнені в новині, то не поширюйте її![1]

Власне, необхідно зазначити, що на даний момент існує безліч відкритих джерел, якими можуть користуватися аналітики при проведенні OSINT розслідувань. До найбільш популярних відносять наступні:

1. Новини та ЗМІ.

Сюди включаються публікації в ЗМІ, радіо, телебачення, газети та інші види друкованих чи інших ЗМІ. Новини та медіа дані публікуються як в оплатній, так і в безоплатній формі та поширюються на міжнародному, національному, регіональному та місцевому рівнях. Навіть місцеві новини можуть мати ключове значення, надаючи аналітикам детальну інформацію про події, що відбуваються в безпосередній близькості від джерела, яке їх цікавить.

Потенційні виклики при роботі з новинами та ЗМІ: з мільйонами одиниць контенту, які щодня публікуються багатьма мовами, новини та ЗМІ перебувають у стані постійного оновлення. Зрозуміти цей рух і відрізнити надійні новини від «фейкових» чи інших неавторитетних ЗМІ легше, коли аналітики правильно розуміють походження цих джерел.

2. «Сіра» література.

«Сіра» література включає в себе будь-яку загальнодоступну немедійну інформацію про політику в приватному та державному секторах. Сюди включаються документи та звіти благодійних та неурядових організацій, міжурядових установ і аналітичних центрів, а також статистику злочинності, дані перепису та інформацію, що міститься в академічних базах даних, журналах і звітах. До «сірої» літератури також відносяться відомості, які стали відомі завдяки різним витокам інформації.

Потенційні виклики при роботі з «сірою» літературою: ця інформація зазвичай є платною або вимагає певного рівня авторизації. Наприклад, близько 42 % всіх досліджень, які стосуються охорони здоров'я, є платними для ознайомлення. Це пов'язано з тим, що «сіра» література в основному існує в так званій глибокій мережі (Deep Web) — частині інтернету, яку неможливо знайти через стандартні пошукові системи.

---

[1] BREAKING NEWS CONSUMER'S HANDBOOK. FAKE NEWS EDITION (accessible version). By On the Media. URL: https://media.wnyc.org/media/resources/2021/Nov/22/BNCH_FAKE_NEWS_EDITION_o.pdf

Багато інструментів OSINT пропонують розширення для браузерів, які дозволяють аналітикам виявляти результати, які неможливо виявити за допомогою стандартних веббраузерів. Крім того, система зберігання та розповсюдження «сірої» літератури погано структурована, що ускладнює процес пошуку та виявлення взаємозв'язків.

3. Соціальні мережі.

Соціальні мережі можуть охоплювати весь спектр довгострокового контенту (наприклад, дописи Reddit, дописи в соціальних мережах, відповіді Quora), а також короткотривалий контент (твіти, оновлення LinkedIn, підписи в Instagram), фотографії, теги тощо.

Метадані, пов'язані з вмістом соціальних мереж, є ключовими для OSINT аналітиків, допомагаючи у візуалізації зв'язків та розумінні хронології подій.

Поряд з цим необхідно нагадати, що більше половини населення світу зараз використовує ті чи інші соціальні мережі, і, як наслідок, вони мають величезне охоплення, що робить їхнє дослідження надзвичайно трудомістким. Значна частина найкориснішої інформації в соціальних мережах не проіндексована і зберігається в «глибокій мережі», що робить стандартні вебпереглядачі неспроможними її виявити. Крім того, збереження анонімності має вирішальне значення для будь-якого аналітика, тому розслідування окремих осіб в соціальних мережах не повинно привертати до себе увагу.

4. Темна мережа (Dark Web).

Термін «темна мережа» використовується для позначення вебсторінок, які не проіндексовані та потребують спеціального програмного забезпечення для отримання доступу. У «темній мережі» користувачів і операторів не можна відстежити, і, як наслідок, це дуже зручне місця для вчинення злочинів.

Dark Web — це унікальний носій даних, який не індексується стандартними пошуковими системами. Аналітики повинні проявляти обережність, щоб не розкривати власну особу та не розкрити своє розслідування, а також не наближатися до шкідливого програмного забезпечення чи впливу незаконних ЗМІ. Крім того, аналітики також повинні використовувати OSINT-інструменти, щоб уникнути непотрібного

контакту з потенційно травматичним матеріалом під час перегляду темної мережі[1].

1.4 ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ТА OSINT

Питання захисту персональних даних при проведенні OSINT розслідувань є вкрай важливим, адже на даний час на міжнародному та національному рівнях розроблена нормативна база, яка забезпечує невтручання у приватне життя та обмежує збирання, обробку та використання персональних даних. Так, Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108 РЄ), прийнята 28 січня 1981 р., — це перший міжнародний правовий документ, спрямований безпосередньо і винятково на врегулювання питань захисту персональних даних. Поява Конвенції 108 РЄ пов'язана із стрімким розвитком інформаційних технологій у другій половині XX століття і виникненням потреби в розробленні більш детальних правил забезпечення захисту осіб через охорону їхніх (персональних) даних.

Конвенція 108 РЄ визначає основоположні, або так звані «рамкові», засади, зокрема щодо:

- прав особи, пов'язаних з обробленням персональних даних, та можливих обмежень цих прав;
- принципів і вимог до процесу обробки персональних даних;
- обов'язків осіб, які збирають, опрацьовують, використовують персональні дані, зокрема у зв'язку з передачею персональних даних на міждержавному рівні (транскордонного обміну);
- особливих випадків звільнення від зобов'язань, визначених Конвенцією, зумовлених іншими правами людини;
- особливих винятків, пов'язаних із специфічними потребами діяльності із забезпечення безпеки суспільства і держави в демократичному суспільстві;
- державного контролю у сфері захисту персональних даних.

[1] OSINT Sources: What Are The Different Types of Open Source Data? Blackdot Solutions: website. URL: https://blackdotsolutions.com/blog/osint-sources/

Наразі сторонами Конвенції 108 РЄ є країни європейського регіону і не тільки. Першою неєвропейською країною, яка у серпні 2013 року приєдналася до Конвенції 108 РЄ, став Уругвай. Україна ратифікувала Конвенцію 108 РЄ у 2010 році, результатом імплементації її положень в українське законодавство став ЗУ «Про захист персональних даних»[1].

У подальшому приймалися і інші нормативно-правові акти на рівні Ради Європи та Європейського Союзу, проте, напевне, найбільше значення для проведення OSINT розслідувань має Загальний регламент про захист даних (GDPR). Регламент GDPR покликаний надати громадянам та резидентам ЄС контроль за їхніми персональними даними та спростити регуляторне середовище для ведення міжнародного бізнесу, що досягається шляхом уніфікації регулювання в межах ЄС.

Відповідно до принципів опрацювання персональних даних, які передбачені ст. 5 Регламенту, персональні дані слід:

- опрацьовувати у законний, правомірний і прозорий спосіб щодо суб'єкта даних («законність, правомірність і прозорість»);
- збирати для визначених, чітких і законних цілей і в подальшому не опрацьовувати у спосіб, що є несумісним з такими цілями; подальше опрацювання для досягнення цілей архівування у суспільних інтересах, цілей наукового чи історичного дослідження або статистичних цілей не можна вважати, згідно зі статтею 89 (1), несумісним з первинними цілями («цільове обмеження»);
- вважати достатніми і відповідними та обмежити їх мірою необхідності в них з огляду на цілі опрацювання («мінімізація даних»);
- вважати точними і, за необхідності, оновлювати; необхідно вживати усіх відповідних заходів для того, щоб забезпечити, що неточні персональні дані, зважаючи на цілі їхнього опрацювання, було стерто чи виправлено без затримки («точність»);
- зберігати в формі, що дозволяє ідентифікацію суб'єктів даних не довше, ніж це є необхідним для цілей їхнього опрацювання;

[1] Європейські правові стандарти захисту ПД. Захист персональних даних : вебсайт. URL: http://zpd.inf.ua/index.html

персональні дані можна зберігати протягом більш тривалих періодів, доки їх опрацьовують винятково для досягнення цілей суспільних інтересів, цілей наукового чи історичного дослідження або статистичних цілей відповідно до статті 89 (1) за умов вжиття відповідних технічних і організаційних заходів, передбачених цим Регламентом для гарантування прав і свобод суб'єкта даних («обмеження зберігання»);

– опрацьовувати в спосіб, що забезпечує належну безпеку персональних даних, у тому числі захист проти несанкціонованого чи незаконного опрацювання та проти ненавмисної втрати, знищення чи завдання шкоди, із застосуванням відповідних технічних і організаційних інструментів («цілісність і конфіденційність»).

Оцінюючи дані засади з точки зору OSINT розслідувань, аналітики сформували наступні поради:

1. Законність, правомірність і прозорість.

Законність складається з двох частин. Спочатку необхідно оцінити правову основу для обробки персональних даних. Відповідно, методи збору даних також мають бути законними — «не взламуйте, не крадіть і не брешіть», щоб отримати дані. Знову ж таки тягар доведення буде лежати на аналітику, тому потрібно задокументувати джерела та методи, використані для отримання даних, що професійний OSINT аналітик у будь-якому випадку зробив би.

Правомірність пов'язана з пропорційністю. Чи методи, які використовує аналітик для отримання даних, пропорційні тяжкості справи, яку він розслідуєте? І чи тип і кількість персональних даних, які він збирає про суб'єкта даних, також пропорційні в цьому відношенні? Необхідно бути готовим відповісти на ці питання в будь-якому OSINT розслідуванні.

Прозорість частково покривається підзвітністю; аналітик повинен бути прозорим щодо мети та типу даних, що обробляє. Прозорість також є принципом обов'язку повідомляти про те, що було ним знайдено.

2. Мінімізація даних.

Регламент вимагає від аналітика мінімізувати обсяг персональних даних, що обробляються, до того, який справді необхідний

для досягнення мети розслідування. «Стільки, скільки потрібно, але чим менше, тим краще». Отже, коли аналітик збирає гігабайти даних, він має зберігати лише ту інформацію, яка стосується безпосереднього завдання. Збір і перевірка значної кількості даних із соціальних мереж, наприклад, під час перевірки перед працевлаштуванням, можуть бути законними, однак дані, не використані в остаточному звіті, мають бути видалені якнайшвидше після перевірки.

3. Точність.

Регламент зобов'язує переконатися, що дані належної якості, тому не слід використовувати застарілу інформацію або дані, які є неправдивими. Особливо під час роботи з так званими системами пошуку людей аналітик може наштовхнутися на багато застарілих даних про них. Саме аналітик несе відповідальність за перевірку даних (якщо це можливо) перед подальшою обробкою чи звітністю.

4. Обмеження зберігання.

Як довго слід зберігати дані OSINT розслідувань? Регламент стверджує, що таке зберігання не повинно бути «довшим, ніж потрібно», що є досить розпливчастим формулюванням. Судові процеси можуть тривати роками, але в багатьох випадках тривалий період зберігання взагалі не потрібен. Чітке визначення політики збереження даних у плані розслідування дозволить унормувати це питання із замовниками розслідування.

5. Цілісність та конфіденційність.

Аналітик несе відповідальність за безпеку персональних даних, які він обробляє. Той факт, що аналітик зібрав всі дані з відкритих джерел, ще нічого не означає, адже ці дані не повинні бути публічно розголошені, особливо якщо були об'єднані різні джерела даних, що дозволяє визначити деталі особистого життя суб'єкта дослідження. Пропонується дотримуватися такого правила: «якщо ви не можете захистити дані — не збирайте їх»[1].

Якщо ж вести мову про національні стандарти захисту персональних даних, то в першу чергу слід згадати ЗУ «Про захист персональних

[1] Ludo Block. GDPR essentials for OSINT research. Blockint : website. URL: https://www.blockint.nl/methods/gdpr-essentials-for-osint-research/

даних», який регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема, права на невтручання в особисте життя, у зв'язку з обробкою персональних даних та який поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містяться у картотеці чи призначені для внесення до картотеки, із застосуванням неавтоматизованих засобів.

Відповідно до ст. 6 вказаного Закону, обробка персональних даних здійснюється відкрито і прозоро із застосуванням засобів та у спосіб, що відповідають визначеним цілям такої обробки.

Персональні дані мають бути точними, достовірними та оновлюватися в міру потреби, визначеної метою їхньої обробки. Склад та зміст персональних даних мають бути відповідними, адекватними та ненадмірними стосовно визначеної мети їхньої обробки. Обробка персональних даних здійснюється для конкретних і законних цілей, визначених за згодою суб'єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством.

Не допускається обробка даних про фізичну особу, які є конфіденційною інформацією, без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Якщо обробка персональних даних є необхідною для захисту життєво важливих інтересів суб'єкта персональних даних, обробляти персональні дані без його згоди можна до часу, коли отримання згоди стане можливим.

Персональні дані обробляються у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, не довше, ніж це необхідно для законних цілей, у яких вони збиралися або надалі оброблялися. Подальша обробка персональних даних в історичних, статистичних чи наукових цілях може здійснюватися за умови забезпечення їхнього належного захисту.

1.5. ЕТИЧНІ СТАНДАРТИ OSINT РОЗСЛІДУВАНЬ

Відповідно до позиції укладачів Основних стандартів дослідження для документування міжнародних злочинів в України[1], існує шість ключових етичних правил проведення розслідування:

1. Не наробити шкоди — треба бути впевненим, що документування злочинів не зашкодить самому собі, потерпілим, свідкам, колегам, місцевим жителям.

2. Дотримуватися мінімальних стандартів — треба бути впевненим, що розслідувач дотримується мінімальних стандартів етичної та професійної поведінки.

3. Неупередженість та об'єктивність: ваша роль — не обирати сторону конфлікту, але збирати об'єктивну та достовірну інформацію.

4. Знати свої межі — утримуватись від виконання завдань поза своїми можливостями та за необхідності звертатися до експертів.

5. Отримувати згоду від свідків та потерпілих на документування їхніх показань перед початком такого документування.

6. Захист конфіденційності інформації та осіб, які цю інформацію надали.

Етику можна визначити як певну сукупність моральних принципів. Хоча в цілому не існує суперечок щодо визначення сутності даного поняття, власне застосування етичних стандартів на практиці є складнішим завданням, адже моральні принципи та цінності можуть різнитися в залежності від часу, місця чи сфери застосування.

Наразі немає загальнонаціональних чи міжнародних вказівок щодо того, як збираються, аналізуються та отримують дані з відкритих джерел. Етичні межі, які стосуються інформації з відкритих джерел, постійно змінюються та розвиваються. Однак однією з найбільш стабільних позицій є та, відповідно до якої дані, зібрані з відкритих джерел, повинні використовуватися таким чином, щоб не порушити існуючи закони про конфіденційність, не повинні використовуватися у злочинних цілях і мають збиратися тільки тоді, коли це необхідно.

---

[1] Basic Investigative Standards for Documenting International Crimes In Ukraine: Guides. Global Rights Compliance. 2023. URL: https://globalrightscompliance.com/wp-content/uploads/2023/05/Basic-Investigative-Standards-for-Documenting-International-Crimes-in-Ukraine-Guides.pdf

Хоча на практиці немає «правильних» відповідей, які би стосувалися застосування етичних стандартів при OSINT розслідуваннях, схема Марккули (Markkula Framework), розроблена Центром прикладної етики Марккули в Університеті Санта-Клари (Markkula Center for Applied Ethics at Santa Clara University), пропонує покроковий підхід до вирішення етичних дилем.

Схема складається з п'яти кроків (мал. 1.3).

Мал. 1.3. Схема Марккули

1. Визначте дилему.

По-перше, спробуйте окреслити дилему у вашій конкретній ситуації. Якщо викласти дилему своїми словами та записати її, то це дозволить краще зрозуміти її масштаби. Визначте для себе, чи дійсно це етична дилема чи лише юридична проблема тощо. Багато OSINT аналітиків плутають юридичні питання з етичними. Закони часто базуються на етичних міркуваннях, але дане правило не завжди застосовується.

2. Отримайте всі факти.

Далі зберіть всі факти, які допоможуть визначити вам подальший хід дій. Визначте дані, інструменти та ресурси, які є у вашому розпорядженні. Подумайте про осіб, з якими ви можете додатково проконсультуватися з зазначеної проблеми.

3. Зважте ваші можливості.

Більшість етичних рішень не є антагоністичною грою[1] (zero sum game). Деякі дилеми можуть стосуватися таких простих питань,

[1] Ігри з двома гравцями, які мають прямо протилежні інтереси. При переході від однієї ситуації до іншої збільшення (зменшення) виграшу одного гравця тягне за собою зменшення (збільшення) виграшу іншого. Таким чином, сума виграшів гравців у будь-якій ситуації в антагоністичних іграх стала (зазвичай можна вважати, що вона дорівнює нулю). Тому антагоністичні ігри називають також іграми двох осіб із нульовою сумою (іноді — нульовими іграми).

як, наприклад, можливість публікації одних даних та захист інших на випадок, якщо вони знадобляться пізніше. Чи необхідно отримати дозвіл на публікацію? Чи можна обмежити аудиторію, яка буде знайомитися з даними? Більшість етичних дилем не такі прості, як описано вище, але уважно подумайте про різні варіанти дій. Для цього можна використовувати шість етичних підходів:

– утилітарний підхід.

Цей підхід стосується наслідків вашого рішення. Він базується на зменшенні шкоди та збільшенні користі. Оскільки ми не можемо ані повністю максимізувати користь, ані мінімізувати шкоду, ваша мета полягає в тому, щоб знайти найкращий баланс користі над шкодою. Застосовуючи його, враховуйте, кому або що принесе користь, а кому або чому — шкоду;

– правовий підхід.

Цей підхід зосереджується на тому факті, що всі люди мають вроджену гідність і права. Люди мають право вільно вибирати, що робити зі своїм життям без перешкод. Ці моральні права включають право обирати власний життєвий шлях, право на приватне життя та багато інших, які досі обговорюються в суспільстві. Основний етичний висновок даного підходу полягає в тому, що ми зобов'язані поважати права інших;

– справедливий підхід.

Арістотель сформулював цей підхід як такий, при якому ми повинні ставитися один до одного однаково, хоча з часом цей підхід еволюціонував до визнання того, що «рівно» не завжди є «справедливим». Таким чином, нині в суспільстві точаться дискусії щодо того, як ставитися до тих, хто історично перебуває в непривілейованому становищі;

– підхід спільного блага.

Інший підхід грецького походження, підхід спільного блага, розглядає громаду як благо саме по собі. Він прагне поставити користь громади над людиною. Цей підхід наголошує на загальному добробуті кожного й часто пов'язаний із публічною освітою, соціальними службами та забезпеченням тощо;

– підхід чесноти.

Цей підхід поєднує етику з певними чеснотами, такими як чесність, мужність, співчуття, щедрість, толерантність, любов, вірність,

справедливість та розсудливість. Рекомендується питати себе: «Якою людиною я стану, якщо так зроблю?»;

– підхід захисту.

Підхід захисту наголошує на взаємозалежних стосунках між зацікавленими сторонами, а не на визначенні шкоди чи користі. Використовуючи емпатію, постарайтеся поставити себе на місце кожної із зацікавлених сторін і цінувати їхню точку зору, коли справа доходить до оцінки інтересів, проблем і волі всіх сторін. Цей підхід іноді асоціюється з продовольчою безпекою, рівними правами та захистом навколишнього середовища.

4. Перевірте своє рішення серед колег чи уявіть наслідки.

Виберіть один із варіантів, які ви обрали, і перевірте його самі в своїй голові. Якщо вам зручно консультуватися з колегами, поділіться з ними і прислухайтеся до їхніх зауважень чи відгуків. Або уявіть, як відреагувала б на ваш вибір людина, якій ви довіряєте. Також рекомендується уявити, як ви оголошуєте своє рішення по телебаченню.

5. Дійте, вчіться та еволюціонуйте для наступних разів.

Тепер настав час ухвалити рішення. Ви вже визначили дилему та відповідні факти та інструменти, необхідні для ухвалення рішення. Ви також окреслили кілька варіантів і зважили їх один проти одного, використовуючи шість етичних підходів, наведених вище. Реалізуйте своє рішення якнайкраще та задокументуйте результат. Сталося щось непередбачуване? Ви навчилися зі своїх дій? Витратьте час на вивчення досвіду та подумайте про це, коли наступного разу зіткнетеся з етичною дилемою[1].

[1] Melissa Hanham. Setting Your Moral Compass: A Workbook for Applied Ethics in OSINT. The Stanley Center for Peace and Security. URL: https://stanleycenter.org/wp-content/uploads/2022/08/OSINT-Ethics-Workbook-2022.pdf

Тема 2

ПРОТОКОЛ БЕРКЛІ З ВЕДЕННЯ РОЗСЛІДУВАНЬ ІЗ ВИКОРИСТАННЯМ ВІДКРИТИХ ЦИФРОВИХ ДАНИХ

2.1 ЗАГАЛЬНА ХАРАКТЕРИСТИКА ПРОТОКОЛУ БЕРКЛІ

На 75-ту річницю з дня проведення Нюрнбергського трибуналу спеціалісти з Центру прав людини Юридичного університету Берклі (Berkeley Law's Human Rights Center — HRC) та представники Управління ООН з прав людини (U.N. Human Rights Office) представили фактично перший в світі міжнародний порадник (guidelines) для використання загальнодоступної інформації в інтернеті (включаючи фотографії, відео та інший контент, опублікований в соціальних мережах) як доказів, що можуть бути використані для міжнародних кримінальних розслідувань та розслідувань у сфері прав людини. «Протокол Берклі — це перший набір глобальних керівних положень щодо використання цифрових даних, які є у відкритому доступі, як доказів у міжнародних розслідуваннях щодо порушень прав людини. Документ містить стандарти знаходження, збирання, зберігання, перевірки та аналізу контенту із соцмереж та інших відкритих джерел»[1].

«У той час як активне використання онлайн-інформації (іноді отриманої людьми в зонах бойових дій із ризиком для власного життя)

[1] Протокол Берклі щодо розслідування із використанням відкритих цифрових даних. Юрфем : вебсайт. URL: https://jurfem.com.ua/protokol-berkli-schodo-rozsliduvannia-iz-vykorystannyam-zyfrovych-danych/

дозволяє пролити світло на порушення прав людини та потенційні воєнні злочини в усьому світі, юристи, журналісти, дослідники та правозахисники повинні знати, як поводитися з такою інформацією етично та ефективно», — каже виконавчий директор Центру прав людини Алекса Кеніг. Вона називає Протокол Берклі живим документом, який допоможе вдосконалити розслідування воєнних злочинів за допомогою методів XXI століття з метою покращення правосуддя та забезпечення притягнення винуватих в усьому світі[1].

Це новий інструмент з використання відео та іншої цифрової інформації для встановлення справедливості у випадку порушення прав людини. На основі обширних досліджень, шести семінарів і консультацій з більш ніж 150 експертами Протокол Берклі було опубліковано вісьмома мовами ООН.

У передмові самого Протоколу зазначено, що «з початку 1990-х років цифрові інструменти та інтернет, як камера і телефон перед ними, докорінно змінили спосіб отримання, збирання та поширення нами інформації про порушення прав людини та інші серйозні порушення міжнародного права, включаючи міжнародні злочини.

Сьогодні слідчі можуть збирати дані про потенційні порушення прав людини та інші серйозні порушення міжнародного права, включаючи міжнародні злочини, за допомогою великої кількості загальнодоступних супутникових знімків, відео та фотографій, включаючи матеріали, завантажені в інтернет зі смартфонів, та публікацій на платформах соціальних мереж. Такий розвиток подій допоміг слідчим обійти урядових та інших традиційних контролерів інформації для доступу до ключової інформації про правопорушення, навіть у режимі реального часу, яка в іншому випадку залишалася б прихованою для очей громадськості.

Однак цифрова інформація у відкритому доступі використовувалася переважно у конкретних випадках, оскільки правозахисні організації, міжурядові органи, слідчі механізми та суди часом намагалися адаптувати свою робочу практику, щоб включити нові цифрові

[1] Berkeley Law Center Creates First Global Protocol on Using Social Media as Evidence for War Crimes. Berkeley Law : website. URL: https://www.law.berkeley.edu/article/human-rights-center-berkeley-protocol-social-media-evidence-war-crimes-nuremberg/

методи встановлення фактів та аналізу. Однією з найбільших проблем, з якими вони стикаються, є вирішення питань виявлення та перевірки відповідних матеріалів у межах збільшення обсягу онлайн-інформації, особливо фотографій та відеозаписів, знятих на смартфони та інші мобільні пристрої, деякі з яких можуть бути скомпрометовані або неправильно віднесені.

Тим часом поява міжнародних кримінальних судів та слідчих механізмів, а також національних підрозділів у справах військових злочинів ще більше посилила потребу у спільних стандартах для збору, збереження та аналізу інформації у відкритому доступі, яка може бути представлена як доказ у кримінальних процесах. Для того щоб інформація у відкритому доступі була прийнятною як доказ у суді, прокурори та адвокати, як правило, повинні мати змогу встановити її достовірність та ланцюг забезпечення збереження.

Належне поводження та обробка цього матеріалу значно збільшить ймовірність того, що він може бути використаний прокурорами та адвокатами. Однак, якщо використовуються нерозумні методи збирання та збереження, інформація не може вважатися достовірною для встановлення фактів у справі. Суди та слідчі механізми мають користуватися чіткими критеріями для оцінки ваги інформації у відкритому доступі як зв'язку або як доказу конкретного злочину. Спільні методологічні стандарти щодо автентифікації та перевірки однаково слугуватимуть місіям з виявлення фактів у сфері прав людини, які також все частіше включають цифрові матеріали у відкритому доступі у свої розслідування.

...

Протокол Берклі включає міжнародні стандарти для проведення онлайн-досліджень щодо ймовірних порушень міжнародного права в області прав людини та міжнародного гуманітарного та кримінального права. Він також містить вказівки щодо методологій та процедур збору, аналізу та збереження цифрової інформації у професійному, юридичному та етичному порядку. Нарешті, Протокол Берклі визначає заходи, які онлайн-слідчі можуть вжити для захисту цифрової, фізичної та психосоціальної безпеки для себе та інших, включаючи свідків, жертв та осіб, які надають першу допомогу (наприклад, громадян, активістів

та журналістів), які ризикують власним благополуччям і документують порушення прав людини та серйозні порушення міжнародного права.

Протокол Берклі йде слідами двох попередніх протоколів Організації Об'єднаних Націй: Міннесотського протоколу з розслідування потенційно незаконного позбавлення життя (1991 рік, оновлено у 2016 році) та Посібника з питань ефективного розслідування і документування фактів катувань та іншого жорстокого, нелюдського чи такого, що принижує гідність, поводження або покарання (Стамбульський протокол) (1999 рік, оновлено у 2004 році). Міннесотський протокол, розроблений юристами та криміналістами, які займалися пошуком зниклих осіб у 1980-х роках, встановлює міжнародні стандарти та процедури для проведення медико-правових розслідувань щодо підозрілих смертей або смертей, залишених без уваги, та служить засобом оцінки достовірності таких розслідувань. Так само Стамбульський протокол надає лікарям та адвокатам вказівки щодо того, як розпізнавати та документувати фізичні та психосоціальні наслідки катувань, щоб документація могла служити дійсним доказом у суді чи в інших контекстах, включаючи розслідування та моніторинг прав людини. Усі три протоколи ґрунтуються на переконанні, що наука, техніка та право можуть — і повинні — працювати разом на службі прав людини».

...

Хоча керівні принципи та навчання з використання спеціальних інструментів та програмного забезпечення є суттєвою частиною покращення якості розслідувань з використанням відкритих цифрових даних, Протокол Берклі зосереджується не на конкретних технологіях, платформах, програмному забезпеченні чи інструментах, а скоріше на основних принципах та методологіях, які можна послідовно застосовувати навіть при зміні самої технології. Ці принципи визначають мінімальні правові та етичні стандарти для проведення ефективних розслідувань з використанням даних у відкритому доступі. Дотримуючись вказівок Протоколу Берклі, слідчі допоможуть забезпечити якість своєї роботи, мінімізуючи при цьому фізичні, психосоціальні та цифрові ризики для себе та інших»[1].

[1] Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних. Berkeley Law : website. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf

2.2 ПРИНЦИПИ ВЕДЕННЯ РОЗСЛІДУВАННЯ З ВИКОРИСТАННЯМ ВІДКРИТИХ ЦИФРОВИХ ДАНИХ

Професійні принципи

Підзвітність

Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні нести відповідальність за свої дії, що часто можна забезпечити чіткою документацією, веденням обліку та наглядом. Прозорість у методах та процедурах розслідування є важливим елементом забезпечення підзвітності. Таким чином, наскільки це можливо і розумно, слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні вести записи про свою діяльність. Етапи розслідування з використанням даних у відкритому доступі — від виявлення відповідного матеріалу до збору, аналізу та звітування — слід послідовно та чітко документувати. Будь-які особи, які займаються збором або обробкою інформації в інтернеті, повинні знати про можливість допиту щодо їхньої методології, включаючи можливість бути викликаними для надання свідчень у суді.

Компетентність

Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні мати належну підготовку та технічні навички для виконання діяльності, якою вони займаються. Вони повинні вести діяльність в інтернеті професійно та етично, уникаючи привласнення чужої роботи; висловлюючи подяку всім, хто бере участь у розслідуванні (коли це безпечно робити та за бажанням учасників); і точно повідомляючи дані, включаючи визнання будь-яких прогалин, які можуть існувати в онлайн-контенті. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, та процеси розслідування також повинні залишатися гнучкими, адаптуватися до нових розробок та застосовувати нові технології та методи у відповідних випадках. Крім того, організації та слідчі групи повинні мати механізми для забезпечення послідовного впровадження та дотримання процедур.

Об'єктивність

Об'єктивність — це основний принцип, який застосовується до всіх розслідувань, будь то онлайн чи офлайн. Слідчі, що ведуть розслідування

з використанням даних у відкритому доступі, повинні розуміти потенціал особистих, культурних та структурних упереджень, що впливають на їхню роботу, і необхідність вживати контрзаходів для забезпечення об'єктивності. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні переконатися, що вони об'єктивно підходять до своїх розслідувань, розробляючи та розгортаючи численні робочі гіпотези, а не віддаючи перевагу якійсь конкретній теорії для пояснення своїх аргументів. Для розслідувань з використанням даних у відкритому доступі, що проводяться в інтернеті, об'єктивність особливо важлива через спосіб структуризації та представлення користувачам інформації в інтернеті… Слідчі повинні знати, що на результати пошуку також можуть впливати інші чинники, в тому числі внаслідок розбіжностей у цифровому середовищі, у результаті чого інформація в інтернеті може бути нерівномірно доступною для певних груп чи верств суспільства. Нарешті, слідчі завжди повинні прагнути усвідомлювати та виправляти власні упередження, які можуть бути свідомими або підсвідомими.

Законність

Розслідування з використанням даних у відкритому доступі повинні відповідати чинному законодавству, а це означає, що слідчі повинні мати базове розуміння законів, які застосовуються в їхній роботі. Зокрема, слідчі повинні знати закони про захист даних та право на недоторканність приватного життя, яке охороняється міжнародним законодавством з прав людини. Незважаючи на те, що інформація може бути загальнодоступною, це не означає, що її збирання та використання не впливають на конфіденційність.

Поінформованість про безпеку

Усі особи, які проводять розслідування в інтернеті, повинні мати базову обізнаність щодо оперативної безпеки для мінімізації свого цифрового сліду та усвідомлення потенційних ризиків. Організації, які проводять розслідування з використанням даних у відкритому доступі, повинні забезпечити, щоб їхні слідчі пройшли навчання з інформаційної безпеки, для розуміння ризиків, з якими вони можуть зіткнутися, і розуміння трьох основних рівнів інформаційної безпеки: а) конфіденційність (наприклад, дозволяти лише повноважним користувачам отримувати доступ до даних); б) цілісність (забезпечення того, щоб дані

не підроблялися та не змінювалися іншим чином неавторизованими користувачами); і в) доступність (забезпечення доступності систем та даних авторизованим користувачам, коли вони цього потребують).

Методологічні принципи

Точність

Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні прагнути бути максимально правдивими та точними під час своїх розслідувань та представлення будь-яких результатів, особливо коли мова йде про визнання слабких місць у базових даних чи загальній ситуації. Точність часто підвищується за допомогою використання та перевірки кількох робочих гіпотез та/або експертної перевірки, обидві з яких можуть допомогти мінімізувати шанси упередженого відбору, інтерпретації та представлення даних.

Мінімізація даних

Принцип мінімізації даних передбачає, що збирати та обробляти цифрову інформацію можна лише у випадках, коли це: а) виправдано для чіткої мети; б) необхідно для досягнення цієї мети; і в) пропорційно здатності досягти цієї мети. У контексті розслідувань з використанням даних у відкритому доступі онлайн-контент слід збирати лише у тому випадку, якщо він має відношення до конкретного розслідування.

Збереження

Не менш важливим, ніж уникнення надмірного збору релевантної інформації, є запобігання недостатньому збору. Це може викликати особливе занепокоєння у контексті інформації в інтернеті, постійність та доступність якої часто є сумнівною. Принцип збереження покликаний уникнути недостатнього збору, щоб не втратити відповідні та потенційно переконливі докази. Платформи соціальних медіа, наприклад, можуть видаляти контент, який порушує їхні умови користувацької угоди, навіть якщо цей контент має потенційну цінність для слідчих.

Безпека за замовчуванням

Принцип безпеки за замовчуванням вимагає, щоб, наскільки це можливо, цифрова інформація та операції в інтернеті були захищені за замовчуванням. Організації, які проводять онлайн-розслідування з використанням даних у відкритому доступі, повинні інвестувати та

впроваджувати відповідні технічні та структурні заходи, щоб гарантувати належну анонімізацію та запобігання віднесенню інфраструктури за замовчуванням, включаючи апаратне та програмне забезпечення, коли слідчі виходять у мережу. Все обладнання повинно мати оновлене програмне забезпечення для захисту від шкідливого програмного забезпечення та відповідні налаштування конфіденційності та безпеки. До початку онлайн-розслідування мають бути вжиті заходи безпеки; їх слід постійно контролювати, оновлювати та коригувати у разі потреби. Слідчі, слідчі групи або організації можуть захотіти організувати постійне тестування, включаючи тестування на проникнення, щоб переконатися, що їхня система безпеки працює відповідно до проєкту.

Етичні принципи

Гідність

Розслідування слід проводити з усвідомленням та чутливістю до будь-яких проблем, пов'язаних з гідністю, особливо тих інтересів, які захищені міжнародним законодавством з прав людини. Наприклад, слідчі повинні дотримуватись принципів недискримінації, які можуть вплинути на те, що розслідується, і хто проводить розслідування або кому приписується розслідування, та інтегрувати запобіжні заходи щодо цифрової, фізичної та психосоціальної безпеки свідків, тих, хто вижив, інших слідчих, обвинувачених та інших, на кого це може негативно вплинути. Дотримання принципу гідності також може вплинути на те, що публічно повідомляється про розслідування, у тому числі в письмовій формі та у будь-яких наочних матеріалах — наприклад, не показуючи повного обсягу страждань чи насильства, якщо це не потрібно. Цей принцип гарантує, що норми прав людини є керівним набором стандартів для проведення етичних розслідувань з використанням даних у відкритому доступі.

Тактичність

Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні бути тактичними, усвідомлювати свої обмеження та бути поінформованими про те, чого вони не знають. Для належного розуміння та інтерпретації інформації у відкритому доступі може знадобитися спеціалізоване навчання або консультації з експертами.

Тактичність також означає брати на себе відповідальність за помилки. Якщо слідчі виявлять, що вони допустили помилку, її слід виправити або повідомити про це тих, хто може мінімізувати заподіяну шкоду. В ідеалі повинен існувати механізм повідомлення про помилки та виправлення, особливо для розслідувань, які є публічними та широко поширюються.

Інклюзивність

Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні забезпечити, щоб у розслідування було включено цілий ряд перспектив. Фактори, які слід врахувати, які можуть вплинути на загальну інклюзивність онлайн-розслідування, включають його географічний масштаб, порушення та/або міжнародні злочини, що розслідуються, та усвідомлення нерівномірності інформації в інтернеті щодо різних верств суспільства. Слідчі групи також повинні бути різноманітними, що включає наявність гендерного балансу. Крім того, принцип інклюзивності разом з принципом гідності може вплинути на матеріали, які слідчий вирішує зібрати та використати під час розслідування, і на те, як вони будуть представлені різним аудиторіям.

Незалежність

Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні захищати себе та свої розслідування від неналежного впливу. Вони повинні виявляти і уникати будь-яких реальних або передбачуваних конфліктів інтересів та запроваджувати запобіжні заходи для пом'якшення тих конфліктів, яких неможливо уникнути. Прозорість процесу, методів та фінансування може допомогти з оцінкою незалежності та захистити фактичну та сприйману незалежність розслідування.

Прозорість

Хоча принцип підзвітності вимагає прозорості методів слідчого та результатів, етичний принцип прозорості стосується того, як слідчі, що проводять розслідування з використанням даних у відкритому доступі, поводяться в інтернеті та у зовнішньому світі. Це означає уникати надання недостовірних даних… Одержання інформації шляхом введення в оману може порушити право цільової особи на конфіденційність та/або зашкодити розслідуванню, особливо якщо надання недостовірних даних є незаконним у відповідних юрисдикціях.

2.3 ПІДГОТОВКА ДО РОЗСЛІДУВАННЯ З ВИКОРИСТАННЯМ ВІДКРИТИХ ЦИФРОВИХ ДАНИХ

Оцінка цифрових загроз та ризиків

Роздуми про потенційні загрози та прийняття стратегії управління ризиками — фізичними, цифровими чи психосоціальними — забезпечить дотримання принципів безпеки та етики. Спочатку слід провести оцінку цифрових загроз та ризиків, щоб визначити загальні та конкретні загрози, які можуть виникнути в результаті діяльності в інтернеті, зокрема відвідування цільових вебсайтів, постійного моніторингу конкретних джерел або вилучення даних із платформ соціальних медіа. Оцінка повинна включати елементи традиційного аналізу загроз, такі як виявлення всіх потенційних суб'єктів загрози, оцінка інтересів та можливостей цих суб'єктів загрози, а також ймовірності нападу, врахування вразливостей та запровадження заходів захисту для мінімізації цих вразливостей. Такій оцінці сприятимуть консультації з експертами з безпеки або вихідні дані від них, особливо від тих, хто має досвід у галузі кібербезпеки. Оцінку слід періодично переглядати та оновлювати за необхідності. Крім того, можуть знадобитися додаткові оцінки для вирішення конкретних видів діяльності в інтернеті або впровадження нових потенційних суб'єктів загрози.

Оцінка цифрового середовища

Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні розуміти цифрове середовище досліджуваної ситуації. Тип доступної та використовуваної технології, у тому числі яким вони користуються, матиме вплив на типи доступних цифрових даних. Для цього потрібно визначити найбільш часто використовувані онлайн-платформи, послуги зв'язку, платформи соціальних медіа, мобільні технології та мобільні додатки, що використовуються у досліджуваному географічному регіоні.

Слідчі повинні вивчити категорії людей, які використовують або мають доступ до кожної з цих технологій у цьому географічному регіоні. У зв'язку з цим слідчі повинні знати, що створений користувачами загальнодоступний цифровий контент, включаючи публікації в соціальних мережах та інформацію, що передається через мережеві

платформи, не може однаково охоплювати весь обсяг порушень щодо всіх осіб та груп. Це пояснюється тим, що використання цифрових технологій може бути різним залежно від статі, етнічної приналежності, релігії, переконань, віку, соціально-економічного статусу, приналежності до расової, мовної, етнічної чи релігійної меншини, корінної ідентичності, міграційного статусу та географічного розташування. Іншим фактором може бути те, що згадані особи, можливо, не мали доступу до рівної освіти, а отже, мали менші можливості з точки зору технічних навичок. Внаслідок перетину форм дискримінації деякі верстви суспільства можуть бути вдвічі непомітними в інтернеті.

Крім того, нерівний доступ до технологій з боку всіх верств суспільства також може спотворити не тільки увагу до того, хто представлений в інтернет-контенті, а й види порушень, які доступні в інтернеті, зокрема стосовно контенту, створеного користувачами. Наприклад, коли жінки спільно користуються мобільними телефонами, що належать членам їхніх сімей чоловічої статі, або діляться обліковим записом з іншими, вони можуть не обговорювати делікатні питання, такі як сексуальне та гендерне насильство, або питання навколо сексуального та репродуктивного здоров'я. Більше того, контент, створений користувачами в соціальних мережах, включаючи фотографії та відео, може легше зобразити певні порушення, ніж інші. Наприклад, сексуальне та гендерне насильство, яке може бути вчинено у приватних умовах, може бути важче зобразити, ніж фотографії виселення, наприклад.

План онлайн-розслідування

Перед початком розслідування з використанням даних у відкритому доступі слід створити план онлайн-розслідування, який охоплює: а) загальну стратегію розслідування; і б) конкретні операції з розслідування в інтернеті. Якщо онлайн-розслідування є частиною більш широкого розслідування з використанням традиційних методів, таких як взяття показань свідків або збір речових доказів, план онлайн-розслідування слід включити до основного плану розслідування. Слідчі повинні включити гендерну перспективу до плану розслідування, щоб гарантувати, що розслідування поширюватиметься на всі проблеми, які стосуються статі, та враховуватиме диференційований характер доступу до технологій. План онлайн-розслідування має стосуватися наступних тем:

1) цілі та заплановані заходи. План повинен визначати цілі та пріоритети розслідування з використанням даних у відкритому доступі, запропоновану стратегію досягнення цих цілей та строки їхньої реалізації;
2) стратегія управління ризиками. План повинен включати основні висновки вищезгаданої цифрової загрози та оцінки ризиків, такі як потенційні кіберзагрози, а також стратегію управління ризиками, включаючи способи виявлення, реагування та відновлення після порушень чи атак;
3) відображення суб'єктів та можливостей співпраці. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, можливо, захочуть зіставити інших суб'єктів, які проводять подібні чи дублюючі розслідування, щоб оцінити, як їхня діяльність може вплинути один на одного, а також дослідити потенційні партнерські відносини та можливості для співпраці;
4) ресурси. План повинен визначати ресурси, необхідні для проведення запланованих заходів, включаючи персонал, навчання, інструменти та обладнання. Оцінка потреб у персоналі може включати кількість членів команди, необхідну для виконання завдань, їхню компетенцію, інклюзивність та різноманітність членів команди та оцінку додаткових вимог до навчання. Це може включати оцінку необхідної інфраструктури, включаючи апаратне та програмне забезпечення, та фінансові витрати на збереження цифрового матеріалу в довгостроковій перспективі. План також повинен забезпечити наявність спеціальних ресурсів для забезпечення гендерно-чутливого психологічного благополуччя слідчих, особливо в ситуаціях, коли розслідування з використанням даних у відкритому доступі стосується графічного контенту, або слідчих, або причетних третіх осіб, особливо під загрозою репресій, якщо їхня особистість або конфіденційність ставляться під загрозу;
5) ролі та обов'язки. У разі роботи в команді або із зовнішніми партнерами слід чітко визначити роль та відповідальність слідчих, що ведуть розслідування з використанням даних у відкритому доступі, враховуючи необхідність координації діяльності,

включаючи необхідність уникати дублювання діяльності та збору даних. Крім того, у цьому розділі плану слід розглянути, які спеціалізовані галузі знань можуть знадобитися для конкретного розслідування, і чи слідчим слід буде проконсультуватися або залучити експерта, якщо його немає у наявній групі. Спеціалізовані галузі знань можуть включати цифрову криміналістику, аналіз супутникових знімків та науку про дані. У деяких галузях експертизи можуть знадобитися активні зусилля для виявлення експертів різної статі та інших категорій, щоб забезпечити всебічність та різноманітність слідчої групи та її аналізу;

6) документування. Розслідування з використанням даних у відкритому доступі мають бути задокументовані таким чином, щоб забезпечити їхнє ефективне управління та дотримання принципу підзвітності. У разі судового розгляду ця документація повинна дозволити слідчим продемонструвати, що зібрані докази є актуальними та доказовими, та пояснити кроки, вжиті або не вжиті під час діяльності в інтернеті, і причини. Незалежно від того, чи було поставлено завдання самостійно або воно було отримано від керівника, система повинна мати механізм для створення завдань для конкретних слідчих заходів, включаючи діяльність в інтернеті, наприклад, запити на дослідження конкретної особи чи інші запити. Результати завдань, включаючи звіти, повинні містити посилання на використовувані методології та прийоми. Звітування повинно відокремлювати оперативну інформацію, яку, можливо, потрібно зберегти в таємниці, щоб захистити джерела та методи розслідування від інформації розслідування, яку необхідно розкрити під час судового розгляду.

План стійкості та турбота про себе

Хоча слідчі, що ведуть розслідування з використанням даних у відкритому доступі, не можуть проводити особисті опитування чи фізично відвідувати місця злочину, особливості досліджень цифрових доказів означають, що вони можуть бути піддані перегляду, збору та аналізу значної кількості графічної чи іншої травматичної цифрової інформації, що може призвести до вторинної травми. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі,

повинні знати принципи турботи про себе, а керівники розслідувань повинні створити організаційне середовище, яке цінує турботу про себе та гендерну та культурну чутливість. Це повинно бути розпочато на підготовчому етапі розслідування шляхом розробки плану сприяння стійкості та пом'якшення негативних психосоціальних наслідків розслідування, які можуть мати різні наслідки залежно від статі, культури та віку.

По-перше, слідчі повинні знати про свою власну поведінку та поведінку товаришів по команді, включаючи схеми роботи, відпочинку, сну та харчування, щоб можна було виявити та усунути відхилення. Політика того, як слідчі працюють у парах, може допомогти виявити будь-які відхилення, оскільки люди можуть не визнати або не захотіти визнати своїх власних змін у поведінці, які інші можуть легше помітити.

По-друге, слід прийняти тактику мінімізації впливу шкідливого контенту. Загальні стратегії в цьому відношенні включають вимкнення звуку при першому перегляді потенційно графічного контенту або коли це не потрібно для негайного аналітичного завдання, оскільки багато емоційного вмісту вбудовано у звук; зведення до мінімуму розмірів екранів; висвітлення графічного матеріалу при аналізі контексту навколо конкретної дії, а не самої дії; позначення будь-якого графічного контенту, що міститься у наборі даних, щоб люди не переглядали цей контент, не знаючи заздалегідь, що вони збираються побачити; попередження один одного при обміні графічним контентом, щоб пом'якшити елемент несподіванки; робота в парах; уникнення роботи ізольовано або пізно вночі; і регулярні перерви, якщо це необхідно.

По-третє, окремі особи та організації повинні виховувати почуття спільності серед членів команди, що може мати захисний ефект — по суті відтворюючи почуття товариства, яке може виникнути під час проведення розслідувань на місцях. Цього можна досягти шляхом регулярних аналізів, які можуть зменшити ізоляцію та допомогти слідчим краще зрозуміти позитивний вплив їхньої роботи; колективні виїзди, включаючи святкування важливих етапів розслідування; та навчання команди стратегіям стійкості.

2.4 ЕТАПИ ПРОВЕДЕННЯ РОЗСЛІДУВАННЯ З ВИКОРИСТАННЯМ ВІДКРИТИХ ЦИФРОВИХ ДАНИХ

Є два основні процеси для онлайн-запитів: а) пошук, тобто виявлення інформації та джерел інформації за допомогою загальних або розширених методологій пошуку; і б) моніторинг, тобто виявлення нової інформації шляхом послідовного та наполегливого огляду набору постійних джерел.

Інтернет-пошук — це діяльність, орієнтована на завдання, спрямована на виявлення нової інформації, що стосується визначеної мети або досліджуваного питання. Пошуки мають бути структурованими та систематичними, включаючи чітке досліджуване питання та параметри пошуку, а також ключові слова та операторів. Різні пошукові системи, інструменти пошуку, пошукові терміни та оператори нададуть різні результати; тому слідчі повинні проявляти певний творчий потенціал та наполегливість у слідуванні різними шляхами та каналами для пошуку відповідної інформації. Окрім пошукових систем, які використовуються для пошуку інформації на індексованих вебсайтах, структурований пошук також може використовуватися на платформах соціальних медіа та в базах даних.

Моніторинг передбачає відстеження встановленого джерела інформації, наприклад, певної теми, з плином часу. Метою є відстеження змінного контенту, що генерується постійним джерелом. Онлайн-моніторинг має бути структурованою діяльністю, яка використовує списки відомих та попередньо оцінених онлайн-джерел, таких як вебсайти чи облікові записи в соціальних мережах, а також пошукові запити, які постійно виконуються щодо визначених цілей.

Проводячи структуровані пошукові та моніторингові заходи, слідчі, що ведуть розслідування з використанням даних у відкритому доступі, завжди повинні пильно стежити за упередженням — як власним когнітивним упередженням, так і властивим упередженням в інформації, доступній в інтернеті. Наприклад, якщо слідчий шукає інформацію про згвалтування, більшість наданих даних або проблеми, що обговорюються в інтернеті, ймовірно, стосуватимуться згвалтування жінок репродуктивного віку, вчиненого поза шлюбними відносинами. Результати пошуку можуть недооцінювати менш помітні види згвалтувань.

Перш ніж збирати контент з інтернету, слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні провести попередню оцінку будь-якого матеріалу, який вони ідентифікують, щоб уникнути надмірного збору та дотримання принципів мінімізації даних та цілеспрямованого розслідування, а також для забезпечення того, щоб збір матеріалу не порушував право на приватне життя приватних осіб. Збір — це акт заволодіння інформацією в інтернеті за допомогою знімка екрана, конвертації у PDF, експертного завантаження чи іншої форми захоплення. Після того як цифровий контент буде ідентифіковано та визнано відповідним для розслідування, та prima facie відповідним та надійним для своєї мети, слідчий повинен визначити належний метод збору. Методи збору можуть змінюватись залежно від того, чи має онлайн-контент потенційну доказову силу в судових процесах, чи буде він використовуватися для прийняття рішень, чи він буде сприяти лише самому розслідуванню. У випадках, коли мова йде просто про робочий продукт, може бути достатньо скріншоту або перетворення в PDF, тоді як вміст, що має потенційну доказову силу, може вимагати більш ретельного та обґрунтованого методу збору (наприклад, шляхом визначення хеш-суми).

Збір онлайн-контенту може здійснюватися вручну за стандартною процедурою або бути автоматизованим за допомогою різноманітних інструментів або сценаріїв. Незалежно від процесу, інформація в ідеалі повинна бути зібрана в момент збору. Ця інформація може бути корисною для встановлення справжності цифрового елемента. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні збирати онлайн-контент у його рідному форматі або в стані, максимально наближеному до його вихідного формату. Будь-які зміни, перетворення або конвертації, спричинені процесом збору, повинні бути задокументовані.

У Протоколі Берклі пропонується звертати увагу на наступні елементи цифрового контенту в процесі збереження інформації:

а) цільова вебадреса: вебадресу зібраного контенту, також відому як єдиний локатор ресурсів (URL) або ідентифікатор (URI), слід записати;
б) вихідний код: слідчі повинні захопити вихідний код HTML вебсторінки, якщо це можливо. Вихідний код HTML сприятиме автентифікації зібраного матеріалу;

в) захоплення всієї сторінки: слідчі повинні спочатку зробити знімок екрана цільової вебсторінки із зазначенням дати та часу, адже це забезпечує найкраще уявлення того, що було побачено під час збору;
г) вбудовані мультимедійні файли: наприклад, якщо завантажують вебсторінку з відео або зображеннями, ці конкретні елементи також слід витягти та зібрати з вебсторінки;
д) вбудовані метадані: слідчі повинні зібрати додаткові метадані цифрового елемента, якщо вони є. Метадані можуть змінюватися залежно від джерел, але загальні метадані включають ідентифікатор користувача завантажувача; ідентифікатор публікації, зображення чи відео; дату та час завантаження; геотег; хештег; коментарі; та анотацію;
е) контекстуальні дані: контекстний контент також слід збирати, якщо він має значення для розуміння цифрового елемента. Такий контент може включати коментарі до відео, зображення чи публікації; надавати інформацію про користувача, таку як логін, справжнє ім'я чи біографію. Необхідність збору такої інформації слід визначити, виходячи зі специфіки цифрового матеріалу;
є) дані збору: слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні записати всі відповідні дані, що стосуються збору, такі як ім'я особи, яка збирає відомості, IP-адреса машини, яка використовується для збору інформації, віртуальна особистість (за наявності) та мітка часу. Слідчі повинні переконатися, що системний годинник на комп'ютері точний, бажано, шляхом його синхронізації з сервером мережевого протоколу часу. Причиною цього кроку є забезпечення того, щоб метадані, пов'язані з часом, були точно представлені у зібраних файлах. Якщо для доступу до зібраної інформації використовується віртуальна особистість, це слід зазначити;
ж) хеш-значення: хеш-значення — це унікальна форма цифрової ідентифікації, яка за допомогою криптографії підтверджує, що зібраний контент є унікальним і не змінювався з моменту збору. На момент збору слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні вручну

або автоматично додати значення хешу. Існує безліч різних типів хешів, і стандарти з часом змінилися. Слідчі повинні оцінити, який хеш використовувати, виходячи з прийнятого на даний момент стандарту.

Постійність та доступність інформації в інтернеті часто є нестабільною. Соціальні мережі можуть видаляти контент зі своїх платформ відповідно до своїх умов використання, або користувачі можуть видаляти чи редагувати власний контент. Крім того, інформацію в інтернеті можна легко деконтекстуалізувати, втратити, стерти або пошкодити. Щоб цифровий матеріал залишався доступним та використовуваним для цілей забезпечення юридичної відповідальності, його слід зберігати як у короткостроковій, так і в довгостроковій перспективі.

На думку спеціалістів, властивості цифрового елемента, який необхідно охороняти та зберігати з плином часу, включають його автентичність, доступність, ідентичність, стійкість, можливість відображення та зрозумілість.

Автентичність — це здатність продемонструвати, що цифровий елемент залишається незмінним з моменту його збирання. Це вимагає, щоб цифровий елемент залишався незмінним під час перебування в архіві або будь-які зміни до нього були задокументовані.

Доступність — це наявність цифрового елемента у простому значенні, що постійно існує та може бути відновленим, а також у юридичному сенсі забезпечення відповідних прав інтелектуальної власності на доступ та використання цього елемента.

Ідентичність відноситься до здатності цифрового елемента бути предметом посилання. Цифровий елемент має бути ідентифікованим та відрізнятись від інших цифрових елементів, наприклад шляхом реєстрації за допомогою ідентифікатора, такого як унікальний ідентифікаційний номер.

Стійкість відноситься до цілісності та життєздатності цифрового елемента в технічному плані. Бітові послідовності цифрового елемента повинні бути неушкодженими, оброблятися та вилучатися.

Можливість відображення означає здатність людей або машин використовувати або взаємодіяти з цифровим елементом за допомогою відповідного обладнання та програмного забезпечення.

Зрозумілість — це здатність передбачуваних користувачів інтерпретувати та розуміти цифровий елемент.

Слідчі також повинні розглянути та спланувати конкретні питання розслідування, які можуть виникнути або виникнуть під час процесу збереження:

а) ланцюг забезпечення збереження. Ланцюг забезпечення збереження — це хронологічна документація послідовності зберігачів інформації чи доказів, а також документація контролю, дати та часу, передачі, аналізу та розпорядження такими доказами. Після збору ланцюг забезпечення збереження цифрового елемента слід підтримувати шляхом встановлення належної системи цифрового збереження;

б) доказова копія. Доказова копія — це цифровий елемент, зібраний слідчим у його первісному вигляді, який не слід змінювати. Цифрові елементи слід зберігати в оригінальному вигляді. Це означає збереження чистого оригіналу зібраного цифрового елемента у всіх форматах, в яких він був зібраний;

в) робочі копії. Копію або копії цифрового елемента слід створити для цілей аналізу та зберігати окремо, щоб слідчі могли працювати з копією, а не з оригіналом. Це дозволяє мінімально обробляти оригінал і зменшувати ризик його компрометації або зміни. Будь-які зміни до елемента, включаючи виготовлення копій, повинні бути задокументовані. Якщо можливо, слід використовувати окремі системи зберігання для доказових копій та робочих копій;

г) зберігання. Зберігання допомагає забезпечити довготривалість цифрових елементів та можливість їхнього пошуку та відновлення. Зберігання слід розглядати не як пасивний, а як активний процес, що включає поточні, керовані завдання та відповідальність. Він включає постійне сховище, в якому носії даних відіграють роль, а також управління ієрархією сховища, заміну носія, перевірку помилок, перевірку виправлень (перевірка, щоб переконатися, що елемент не був змінений), відновлення після пошкодження, а також виявлення та повернення збережених об'єктів. Варіанти зберігання цифрового контенту включають локальний

жорсткий диск або локальний знімний носій інформації або мережевий диск, який є частиною локальної мережі або віддаленого сервера чи системи зберігання даних у хмарі. Міркування, пов'язані з вибором сховища, включають ємність сховища (простір); доступ та контроль; резервні копії; відповідний закон; та інформаційну безпеку і захист даних. Вибір сховища також повинен враховувати швидкість, доступність, вартість, стійкість, системи зберігання та пошуку.

Резервне копіювання

Якщо трапляються втрати даних або помилки, архівіст або технік може спробувати відновити дані. В ідеалі в окремому місці необхідно створити резервну копію чи дублікат даних. Експерти з інформаційних технологій рекомендують мати принаймні три копії даних принаймні у двох різних типах сховищ, при цьому принаймні одна копія має бути географічно відокремлена від інших копій.

Погіршення якості

Однією з проблем зберігання є те, що якість носіїв з часом погіршується. Архівісти можуть зменшити ризик виходу з ладу сховища за допомогою особливо міцних типів носіїв; проте будь-який запам'ятовуючий пристрій з часом стане дефектним, зношуватиметься або випадково вийде з ладу. Навіть без повного збою, під час розкладання збереженого носія можуть виникати помилки даних або пошкодження файлів. Тому важливо підтримувати резервні копії та регулярно контролювати інфраструктуру зберігання та постійність збережених файлів, наприклад, регулярно перевіряючи хеш-значення випадкових вибірок, щоб переконатися у відсутності погашення якості.

Застарілість

Цифрові файли стають застарілими, коли апаратне забезпечення, необхідне для доступу до даних, більше недоступне або не може належним чином обслуговуватися. Незалежно від того, наскільки довговічним може бути будь-який носій інформації, він також ризикує застаріти, ускладнюючи або унеможливлюючи отримання збережених даних. Таким чином, розслідування повинно гарантувати, що вони підтримують та, у разі необхідності, оновлюють носії даних, щоб підтримувати можливість відтворення та доступність даних.

Відновлення

Цифрові файли можуть бути випадково або цілеспрямовано видалені. Коли користувач «видаляє» файл на комп'ютері, контент видаленого файлу залишається на носії даних, доки поверх нього не буде записаний інший файл. Тому, чим більше активності на комп'ютері або на іншому носії інформації, тим швидше він буде перезаписаний і стане невідновлюваним. Більшість комп'ютерів мають вбудовані в операційну систему утиліти програмного забезпечення для відновлення видалених файлів. Крім того, можна придбати програмне забезпечення для відновлення даних і іноді використовувати його для «скасування видалення» файлів. Слідчим, що ведуть розслідування з використанням даних у відкритому доступі, може знадобитися допомога фахівців з інформаційних технологій для доступу до видалених даних.

Оновлення

Оновлення передбачає копіювання контенту з одного носія інформації на інший. Воно націлене лише на застарівання ЗМІ і не є всеосяжною стратегією збереження. Оновлення, однак, слід розглядати як невід'ємну частину більшої стратегії збереження.

Перевірка

Перевірка відноситься до процесу встановлення точності чи достовірності інформації, зібраної в інтернеті. Перевірка інформації у відкритому доступі може бути здійснена як частина загальнодоступного аналізу, включаючи інформацію із закритих та конфіденційних джерел, або спиратися виключно на відкриті джерела. Перевірка ділиться на три окремі етапи: аналіз джерела, технічний аналіз та аналіз контенту.

Аналіз джерел

Аналіз джерел — це процес оцінки надійності та достовірності джерела. інтернет-середовище створює труднощі для аналізу джерел, оскільки багато джерел є анонімними або псевдонімними. Для того, щоб належним чином проаналізувати джерела інформації, слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні спочатку визначити правильне джерело або джерела для аналізу, що означає віднесення інформації до її першоджерела. Аналіз віднесення означає визначення джерела цифрової інформації, яким може бути

конкретний вебсайт, передплатник чи користувач певного облікового запису чи платформи, або група осіб, які склали, створили чи завантажили певний контент. Аналіз віднесення не завжди можливий і може потребувати додаткових розслідувань в інтернеті та реальному світі або розширених методів пошуку та аналізу. Хоча визначення авторства є корисним, його відсутність, як правило, не є критичним для встановлення автентичності онлайн-елемента, оскільки існують інші способи автентифікації інформації у відкритому доступі.

1. Походження. Походження відноситься до походження чи найдавнішого відомого існування чогось. Що стосується онлайн-контенту, то походження може позначати найпершу появу в інтернеті або вихідний елемент до його завантаження в інтернет. У разі онлайн-контенту краще звертатися до «першої копії, знайденої в інтернеті», а не до «першої копії в інтернеті», оскільки оригінал, можливо, був видалений. Навіть якщо слідчі впевнені, що вони знайшли першу версію, наприклад, відеозапису чи іншої інформації з відкритих джерел у мережі, вони не можуть бути впевнені в її походженні через наявність закритих каналів, таких як електронні листи та групи приватних повідомлень, які, можливо, були використані для обміну елементом до його публічного виходу в інтернет.

2. Надійність. Історія публікацій джерела, активність в інтернеті та присутність в інтернеті можуть містити відповідну інформацію, яка свідчить проти чи на користь достовірності джерела. Слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні вивчити наявність джерела в інтернеті та історію публікацій, що може навіть допомогти виявити навмисну спробу обману.

3. Незалежність та неупередженість. Розслідування має перевірити неупередженість джерела. Це можна зробити, переглянувши будь-які групи, організації чи асоціації, з якими пов'язані окремі особи, а також те, як вони заробляють гроші та від кого вони отримують фінансування. Чи є зв'язки чи стосунки з будь-якою зі сторін, які беруть участь у справі чи інциденті, що розслідується? Розглядаючи незалежність джерел, необхідно перевірити, чи можуть вони бути пов'язані з відповідними суб'єктами (наприклад, сторонами конфлікту). Ідеологія джерела та будь-яка групова приналежність також може мати значення. Щодо всіх джерел,

слідчі повинні вивчити та виявити їхні основні мотиви, інтереси чи плани, а також ступінь того, наскільки це може вплинути на їхню достовірність.

4. Специфіка. Чим точніша інформація та твердження, тим легше їх буде довести або спростувати. Широкі та невизначені претензії, як правило, важче критично оцінити.

5. Згасання. Тексти, складені одночасно з подіями, на які вони посилаються, вважаються більш надійними, ніж тексти, написані задовго після того, як події сталися. Цей фактор може бути складним для слідчих, що ведуть розслідування з використанням даних у відкритому доступі, коли незрозуміло, коли був створений цифровий текст.

Технічний аналіз

Технічний аналіз — це аналіз самого цифрового елемента, будь то документ, зображення чи відео. Для перевірки цілісності файлу, тобто того, чи був він змінений у цифровому вигляді, маніпульований чи модифікований, слідчі, що ведуть розслідування з використанням даних у відкритому доступі, можуть вважати за доцільне піддати його судовій експертизі, яку іноді називають цифровим слідчим аналізом. Нижче наведені складові такого аналізу.

1. Метадані. Метадані — це дані, які описують та надають інформацію про інші дані. Вони можуть бути створені користувачем, який створив елемент, іншими користувачами, постачальником послуг зв'язку або будь-яким пристроєм, на якому дані створюються, передаються, отримуються або переглядаються. Метадані мають значення для опису елемента та обставин його створення, розповсюдження або зміни. Метадані можуть включати автора файлу, дату його створення, дані завантаження, зміни, розмір файлу та геодані. Метадані можуть бути вбудовані у файл, відображені на вебсторінці або міститися у вихідному коді. Деякі метадані можуть бути видалені до або під час завантаження, або в результаті використання програм у соціальних мережах, але якщо вони доступні, їх слід переглянути, якщо вони допоможуть встановити достовірність. Оригінальні метадані можуть бути втрачені, оскільки платформи часто перекодують завантажені носії, щоб оптимізувати їх для перегляду, обміну чи відтворення в інтернеті. У таких випадках метадані будуть відображенням нового файлу, а не оригіналу. Якщо метадані

були вилучені, слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні шукати інші способи перевірки елемента.

2. Дані формату файлу зображень, що обмінюються. Формат файлу зображень, що обмінюються, — це тип метаданих, що визначає формати зображень, звуку та допоміжних тегів, які використовуються цифровими камерами, сканерами та іншими системами, що обробляють зображення та звукові файли, записані цифровими камерами.

3. Вихідний код. Вихідний код — це програмування за будь-якою вебсторінкою або програмним забезпеченням. Що стосується вебсайтів, цей код може переглядати будь-хто, використовуючи різні інструменти, навіть сам веббраузер. Вихідний код вебсайту легко переглянути за допомогою ряду вільно доступних інструментів. Він може містити метаконтент або прихований або змінений контент, а також відображатиме структуру посилань та непрацюючі посилання.

Аналіз контенту

Аналіз контенту — це процес, за допомогою якого оцінюється достовірність та справжність інформації, що міститься у відео, зображенні, документі чи заяві. Аналіз контенту так само багатогранний і включає аналіз візуальних підказок або, наприклад, підтвердження зображення метаданими. Характеристики інтернет-середовища породжують численні проблеми, які можуть вплинути на фактичну чи уявну достовірність чи справжність інформації з відкритих джерел у мережі. До них належать кругові звіти, деконтекстуалізація інформації та неправильне тлумачення. Дані контенту — це дані, що містяться в цифровому елементі, такі як відео, зображення, аудіозапис, документ або неструктурований текст.

1. Унікальні ідентифікатори. У разі отримання завдання про перевірку візуального контенту слідчі повинні почати з пошуку унікальних чи ідентифікуючих ознак. Такі особливості можуть включати будівлі, рослинний і тваринний світ, людей, символи та знаки розпізнання. Особливу обережність слід застосовувати при аналізі людських особливостей з метою ідентифікації конкретної особи. Практики ідентифікації зазвичай вимагають специфічних навичок, таких як ті, що набуваються з плином часу та шляхом спеціалізованої підготовки судового експерта. Непрофесійний аналіз може бути неточним, завдати шкоди та/або

в інший спосіб бути проблематичним, якщо його проводитимуть непідготовлені фахівці.

2. Інформація, що об'єктивно перевіряється. Часто може бути корисно почати з визначення того, що саме є «інформацією, що об'єктивно перевіряється». Наприклад, погода в певний день, прізвище та звання командира чи місцезнаходження будівлі можуть бути об'єктивно перевіреними. Оцінка матеріалу у відкритому доступі повинна включати перевірку його змісту щодо такої інформації, яка має об'єктивно перевірятися.

3. Геолокація. Геолокація — це ідентифікація або оцінка розташування об'єкта, діяльності чи місця, з якого створено елемент. Наприклад, можна визначити місце, з якого було знято відео чи фотографію, завантажену з інтернету, за допомогою методів геолокації. Такі методи можуть включати, наприклад, визначення унікальних географічних об'єктів на фотографії та їхнього фактичного розташування на карті.

4. Хронолокація. Хронолокація — це підтвердження дат і часу подій, зображених у частині інформації, як правило, у візуальному образі. Наприклад, можна визначити час доби, коли була зроблена фотографія, вивчивши довжину тіней, зроблених сонячним світлом, разом з іншими показниками.

5. Повнота. Неповний документ або відеокліп все ще можуть бути доказовими, однак розрив може вплинути на доказове значення відповідного доказу. Тому при зборі інформації у відкритому доступі важливо повністю захопити цільовий файл і, коли це необхідно, захопити навколишній контекст.

6. Внутрішня узгодженість. Оцінка внутрішньої узгодженості може бути здійснена стосовно однієї інформації з відкритого джерела в інтернеті або стосовно масиву інформації з певного джерела (та/або джерел з однаковим походженням чи авторством). Оцінка внутрішньої узгодженості окремої інформації в інтернеті має на меті встановити, чи є інформація послідовною на її власних умовах. Внутрішньо послідовна частина або сукупність інформації не повинна суперечити сама собі.

7. Зовнішнє підтвердження. Зовнішнє підтвердження забезпечується інформацією, яка лежить за межами самого цифрового елемента, але збігається з його контентом і, таким чином, підтверджує достовірність контенту елемента.

Слідчий аналіз

Слідчий аналіз — це практика перегляду та інтерпретації фактичної інформації для опрацювання істотних висновків, що мають значення для прийняття рішень. Обсяг та різна якість інформації у відкритому доступі вимагають добре структурованого підходу до аналізу.

Перш ніж пройти певні види аналізу, можливо, спочатку потрібно обробити інформацію у відкритому доступі. Обробка може включати переклад з іноземних мов або сукупність різних наборів даних для аналізу поведінки окремих осіб, місцезнаходжень та об'єктів, а також відносин чи мереж, рухів, діяльності чи транзакцій. Це також може включати зміну характеру або формату цифрового елемента, щоб зробити його сумісним із певним програмним забезпеченням. Поширені типи обробки даних включають:

1) переклад: якщо дані складені мовою, якою не розмовляють слідчі або яка не обробляється програмним забезпеченням, необхідним для ознайомлення з матеріалом, дані можуть бути перекладені перед подальшими кроками;
2) агрегування: слідчим може знадобитися об'єднати різні набори даних в один більший набір даних для їхнього аналізу;
3) переформатування: для полегшення пошуку або повторного використання даних слідчим може знадобитися змінити формат цифрового елемента.

Доцільно обробляти лише робочі копії цифрового елемента, на відміну від оригіналу або доказової копії. Будь-яка обробка цифрового елемента повинна бути задокументована. Якщо дослідники використовують цифрові технології для обробки даних, наприклад, аналізу даних за допомогою алгоритмів, включаючи обробку природної мови та машинне навчання, вони повинні усвідомлювати ризик упередженості при обробці таких даних.

Після обробки інформація може бути проаналізована. Продукти аналітичної роботи з відкритою інформацією будуть змінюватися залежно від мети, типу та обсягу вихідної інформації, що лежить в основі. Вони будуть розроблені відповідно до потреб розслідування і можуть включати схеми, резюме, глосарії, словники та наочні посібники.

Слідчі повинні застосовувати жорсткі стандарти для забезпечення об'єктивності, своєчасності, актуальності та точності даних та висновків,

що містяться в аналітичних продуктах, а також для захисту конфіденційності та інших міркувань щодо прав людини, особливо при роботі з особистою інформацією. Така інформація повинна бути включена лише до продуктів, на які слідчі отримали згоду залучених осіб, і вона служить прямій меті розслідування. Її також слід розглядати у світлі юридичних та етичних обмежень, що стосуються його використання.

Аналіз порівняння зображень/відео

Порівняльний аналіз, або наука порівняння — це процес порівняння ознак об'єктів, осіб та/або місцезнаходжень з іншими невідомими та/або відомими об'єктами, коли хоча б один із предметів, про які йде мова, є зображенням. Це аналіз змісту зображень та відео, включаючи елементи порівняння між різними предметами та функціями, а також їхня якість зображення та візуальні налаштування (світло, перспектива тощо). Хоча зараз багато хто знає основи аналізу порівняння зображень, допомога експерта, який має кваліфікацію та сертифікацію відеоаналізу та/або цифрової криміналістики, може допомогти у наданні наукового аналізу. Для розслідувань у сфері прав людини також може використовуватися така експертиза для надання додаткової ваги відповідним висновкам.

Аналіз інтерпретації зображень/відео

До порівняння зображення/відео відноситься аналіз інтерпретації зображення/відео, який передбачає аналіз цифрового елемента, щоб зрозуміти його візуальний контент. Наприклад, аналіз пострілів, поранень, крові, транспортних засобів, зброї та військових засобів або аналіз швидкості руху транспортного засобу або віку окремої особи — це частина аналізу інтерпретації зображення/відео. Це може бути зроблено аналітиками для цілей розслідування або судово-медичними експертами у разі встановлення фактів у судовому процесі або висновків щодо прав людини.

Просторовий аналіз

Просторовий аналіз, або геопросторовий аналіз, може включати візуальний аналіз контенту та аналіз метаданих для елементів, які пропонують географічні координати або назви місць. Просторовий аналіз передбачає вивчення різних об'єктів та ландшафтних об'єктів з належною роздільною здатністю та перевірку на основі супутникових

чи інших зображень, геоданих та карт, належного знання випадку та контексту та інструментів геоінформаційної системи.

Відображення суб'єктів

Відображення суб'єктів — це техніка для розуміння ключових суб'єктів та визначення відносин влади та каналів впливу. Таким чином, воно починається з визначення ключових суб'єктів, а потім — визначення стосунків між ними.

Аналіз соціальних мереж

Подібно до відображення суб'єктів, аналіз соціальних мереж — це відображення та вимірювання відносин між людьми, групами, організаціями, комп'ютерами, URL-адресами та іншими пов'язаними об'єктами інформації/знань. Люди та групи часто згадуються як вузли, тоді як посилання показують зв'язок між вузлами. Аналіз соціальних мереж використовує зв'язки в соціальних медіа та інших мобільних чи вебплатформах для встановлення та розуміння стосунків між окремими людьми. Аналіз даних про з'єднання або посилання може проводитися дослідником вручну або за допомогою програмного забезпечення для аналітики.

Відображення інцидентів

Відображення інцидентів — це аналітичний прийом, що використовується для встановлення часових та географічних зв'язків між різними інцидентами, який у контексті міжнародних кримінальних порушень та прав людини може стосуватися місця таких порушень чи злочинів, включаючи попередні та наступні події. Він також може включати в себе відображення інших відповідних подій, наприклад, де і коли були зроблені заяви передбачуваних злочинців.

Аналіз картини злочину/порушення

У контексті національних правоохоронних органів картина злочину — це група з двох або більше злочинів, про які повідомляється або які виявляються правоохоронними органами, які є унікальними, оскільки вони мають принаймні одну спільність у типі злочину; поведінка правопорушників або жертв; характеристики злочинців, жертв чи цілей; вилучене майно; або місця події. Аналогічно злочини та порушення можуть бути встановлені у міжнародних кримінальних справах та справах у сфері прав людини на основі інформації у відкритому доступі.

Тема 3

ІНСТРУМЕНТИ ТА МЕТОДИ ПРОВЕДЕННЯ OSINT РОЗСЛІДУВАНЬ

3.1 ЗАГАЛЬНА ХАРАКТЕРИСТИКА ІНСТРУМЕНТІВ ТА МЕТОДІВ ПРОВЕДЕННЯ OSINT РОЗСЛІДУВАНЬ

Повний огляд інструментарію для проведення OSINT розслідувань здійснити вкрай складно, адже він є досить різноманітним та постійно оновлюється чи змінюється. Так, однією з причин змін у такому інструментарії є відкликання інструментів їхніми розробниками, як це було в червні 2019 року, коли Bazzell відкликав свій набір популярних інтерактивних онлайн-інструментів[1] або зникнення вебсайту мета-сканера searx.me. Інший аспект пов'язаний з динамічною природою соціальних мереж. Наприклад, відомо, що Facebook та Instagram активно перешкоджають використанню інструментів і методів OSINT розслідувань, тому вони блокують відповідні вебсервіси, регулярно змінюють вихідний код і обмежують можливості, які використовують OSINT аналітики[2]. Наприклад, Instagram включає спеціальне кодування символів у вихідний код свого вебсайту, щоб ускладнити пряме вилучення URL-адрес. Тим не менш, OSINT-спільнота продемонструвала певну стійкість перед загрозою цих викликів і постійно адаптує або оновлює свій інструментарій. Враховуючи вищезазначені аспекти, вибір інструментів і методів має

[1] Bazzell M (2021) Open source intelligence techniques — resources for searching and analyzing Online information, 8th edn. (self-published).

[2] Там само.

відбуватися безпосередньо перед початком розслідування, адже він може досить швидко застаріти.

У той же час існують спроби дещо унормувати OSINT інструменти. Так, популярним серед OSINT аналітиків є ресурс OSINT FRAMEWORK (https://osintframework.com), метою якого є легка ідентифікація наявних на даний момент найпопулярніших OSINT інструментів. Він створений за деревовидною структурою, де можна обрати необхідний інструмент для проведення розслідування, і ресурс запропонує окремі сайти, де ці інструменти наявні. Існує низка інших каталогів (українських та міжнародних), в яких зібрані найбільш популярні OSINT інструменти. Перерахувати їх в одному місці неможливо, проте це і непотрібно. Як було зазначено вище, OSINT інструменти постійно змінюються та оновлюються, у зв'язку з чим OSINT аналітик повинен самостійно шукати інструменти, які будуть йому потрібні для проведення розслідування. Власне, аналітик повинен ще до того, як бере на себе зобов'язання щодо проведення розслідування, розуміти, якими технічними можливостями він володіє та чи зможе він виконати завдання, яке перед ним ставиться. Не менш важливим є і питання бюджету, адже деякі сервіси вимагають оплату за користування. Тому хоча в більшості літератури цьому не приділяється окрема увага, аналітик (особливо якщо він працює самостійно) повинен встановити свої можливості та технічні знання і тільки після цього виконувати OSINT розслідування[1].

Як вже неодноразово зазначалося, інструменти OSINT розслідувань є вкрай різноманітними. Для OSINT аналітика насамперед має значення не сам інструмент, а інформація, яка може бути отримана за допомогою нього. У зв'язку з цим слід робити акцент саме на методах збирання інформації, хоча в якості демонстрації будуть надаватися окремі приклади OSINT інструментів.

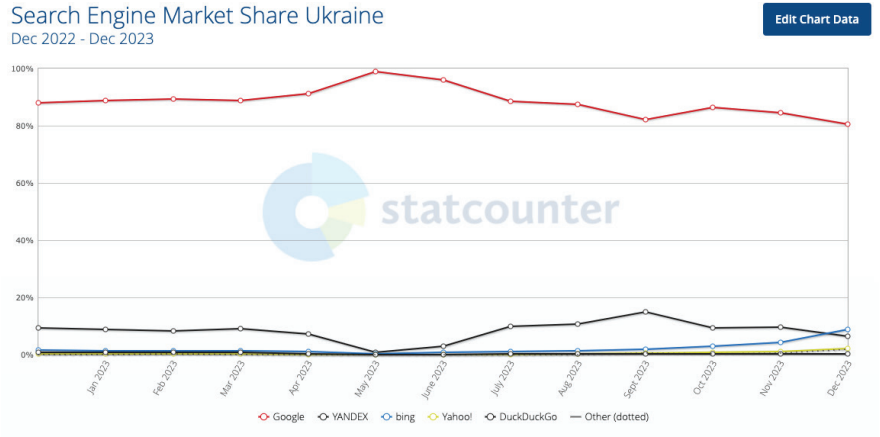
3.2 ПОШУКОВІ СЕРВІСИ ТА ПОШУКОВІ ЗАПИТИ

У більшості випадків OSINT розслідування починається саме з введення пошукового запиту в один з доступних пошукових сервісів.

[1] Böhm, Isabelle & Lolagar, Samuel. (2021). Open source intelligence: Introduction, legal, and ethical considerations. International Cybersecurity Law Review. 2.

Власне, вибір сервісу вже в значній мірі буде впливати на результати, які отримує OSINT аналітик, що вказує на необхідність правильного вибору відповідного пошукового сервісу.

Очевидно, що найпопулярнішим пошуковим сервісом в Україні та світі є Google. Відповідно до статистики, наданої сервісом Statcounter, за 2022 рік в Україні Google охопив 80,34 % всіх пошукових запитів (bing 8,91 %; YANDEX 6,47 %; Yahoo! 2,22 %; Baidu 1,83 %; DuckDuckGo 0,19 %) (мал. 3.1).



Мал. 3.1. Статистичні дані найбільш популярних в Україні пошукових сервісів за 2023 рік, за даними Statcounter

Як правило, OSINT аналітики використовують у своїй роботі саме Google, проте слід підкреслити, що це далеко не єдиний пошуковий сервіс, яким можна користуватися, адже кожен з них є унікальним та надає свої особливі переваги. Наприклад, DuckDuckGo пропонує додаткову анонімність своїм користувачам, через що деякі аналітики користуються саме ним. У той же час даний навчальний посібник не направлений на дослідження всіх можливих пошукових сервісів, тому в даному випадку в якості прикладу буде використовуватися найбільш популярний Google. І перед тим як аналізувати його пошукові здібності

для OSINT розслідувань, необхідно встановити, як взагалі працює даний сервіс.

Так, пошук Google працює в три етапи, і не всі веб сторінки проходять кожен етап:

1. Сканування: Google завантажує текст, зображення та відео зі сторінок, знайдених в інтернеті, за допомогою автоматизованих програм, які називаються сканерами.

2. Індексація: Google аналізує текст, зображення та відеофайли на сторінці та зберігає інформацію в індексі Google, який, по суті, є великою базою даних.

3. Обслуговування результатів пошуку: коли користувач шукає в Google, Google повертає інформацію, яка відповідає запиту користувача.

Сканування

Перший етап — з'ясувати, які сторінки існують у мережі. Немає центрального реєстру всіх вебсторінок, тому Google має постійно шукати нові та оновлені сторінки та додавати їх до свого списку відомих сторінок. Цей процес називається «виявлення URL-адреси». Деякі сторінки відомі, оскільки Google уже відвідував їх. Інші сторінки виявляються, коли Google переходить за посиланням із відомої сторінки на нову сторінку: наприклад, головна сторінка веде на нову публікацію в блозі. Інші сторінки виявляються, коли розробник сайту надає список сторінок (карту сайту) для сканування Google. У даному випадку необхідно наголосити, що в значній мірі саме від розробників сайтів буде залежати, чи будуть такі сайти індексуватися Google. Якщо розробник не виконає необхідні дії та не дозволить Google «знаходити» таку сторінку, то вона фактично буде відноситись до «глибокого вебу» і знайти її стандартними методами пошуку буде неможливо.

Коли Google виявляє URL-адресу сторінки, він може відвідати («сканувати») сторінку, щоб дізнатися, що на ній є. Google використовує величезну кількість комп'ютерів для сканування мільярдів сторінок в інтернеті. Програма, яка виконує вибірку, називається Googlebot (також відома як сканер, робот, бот або павук). Googlebot використовує алгоритмічний процес, щоб визначити, які сайти сканувати, як часто та скільки сторінок отримувати з кожного сайту. Однак Googlebot сканує не всі сторінки, які він виявив. Деякі сторінки можуть бути заборонені

для сканування власником сайту, інші сторінки можуть бути недоступні без входу на сайт.

Індексація

Після сканування сторінки Google намагається зрозуміти, про що йдеться на сторінці. Цей етап називається індексацією і включає обробку й аналіз текстового вмісту, ключових тегів і атрибутів вмісту.

Під час процесу індексації Google визначає, чи є сторінка дублікатом іншої сторінки в інтернеті, чи вона є унікальною (канонічною). Канонічна сторінка може відображатися в результатах пошуку. Щоб вибрати канонічну сторінку, Google спочатку групує разом сторінки, знайдені в інтернеті, які мають подібний вміст, а потім вибирає ту, яка є найбільш репрезентативною для групи.

Зібрана інформація про канонічну сторінку та її кластер може зберігатися в індексі Google — великій базі даних, розміщеній на тисячах комп'ютерів. Індексація не гарантується; не кожна сторінка, яку обробляє Google, буде проіндексована.

Обслуговування результатів пошуку

Коли користувач вводить запит, Google шукає в індексі відповідні сторінки та видає результати, які є найякіснішими та найбільш відповідними запиту користувача. Релевантність визначається сотнями факторів, які можуть включати таку інформацію, як місцезнаходження користувача, мова та пристрій (настільний комп'ютер або телефон). Наприклад, пошук за запитом «велосипедні майстерні» покаже різні результати для користувача з Парижа та для користувача з Гонконгу.

Залежно від запиту користувача функції пошуку, які відображаються на сторінці результатів пошуку, також змінюються. Наприклад, якщо шукати «велосипедні майстерні», швидше за все відображатимуться місцеві результати, але не буде зображень, однак пошук за запитом «сучасний велосипед» швидше за все покаже результати із зображеннями, але не місцеві результати[1].

Загалом базові навички роботи з пошуковими запитами відомі кожному. Проблема полягає в тому, що Google індексує величезну кількість

[1] In-depth guide to how Google Search works. Google Search Central : website. URL: https://developers.google.com/search/docs/fundamentals/how-search-works

сайтів, що може ускладнити роботу аналітиків. Задля уточнення пошуку можна використовувати низку операторів. Ось найбільш популярні з них:

Оператор:	AND
Опис:	шукає сайти, де обов'язково є ці два слова, але не показує сайти, де є лише одне зі слів
Приклад:	Панамські документи витік — 11 400 результатів Панамські документи AND витік — 2 590 результатів
Оператор:	OR
Опис:	шукає сайти чи з одним, чи з іншим словом
Приклад:	OCIHT OR OSINT
Оператор:	Мінус (-)
Опис:	шукає всі сайти, на яких немає відповідного слова (між мінусом та словом не повинно бути пробілу)
Приклад:	OSINT інструменти -платні
Оператор:	Лапки («»)
Опис:	шукає не набір слів, а конкретну фразу
Приклад:	Іванов Іван Іванович — 364 000 результатів «Іванов Іван Іванович» — 9 120 результатів[1]
Оператор:	Тильда (~)
Опис:	якщо поставити тильду перед словом, то Google буде шукати це слово та синоніми цього слова
Приклад:	~боєприпаси
Оператор:	intitle:
Опис:	пошук за словом, яке має бути в самому заголовку
Приклад:	intitle:OSINT

[1] Кожний пробіл для Гугла — це оператор «ТА», тобто в запиті Іванов Іван Іванович Гугл буде шукати всі сайти, де можна знайти слова «Іванов», «Іван» та «Іванович». Якщо ж запит подати в лапках «Іванов Іван Іванович», то будуть шукатися лише сайти, де є відповідне повне прізвище, ім'я та по батькові.

Оператор:	allintitle:
Опис:	аналогічний з «intitle:», проте в заголовку сайту мають бути всі слова, які надаються в запиті
Приклад:	allintitle:OSINT інструменти

Оператор:	related:
Опис:	Шукає сайти, які пов'язані з конкретним сайтом
Приклад:	related:unian.ua

Оператор:	Зірочка (*)
Опис:	замінює слово у фразі
Приклад:	найкращий * в OSINT розслідуваннях

Оператор:	filetype:
Опис:	пошук за конкретним типом файла
Приклад:	filetype:pdf OSINT інструменти (будуть відображені лише результати з pdf файлами)

Оператор:	site:
Опис:	пошук на конкретному сайті
Приклад:	site:unian.ua корупція (будуть відображені лише сторінки сайту Уніан з текстом «корупція»)

Це далеко не повний перелік операторів, більше можна знайти власне через Google. У даному випадку важливо пам'ятати, що декілька операторів можуть використовуватися в одному пошуковому запиті, що зможе значно спростити роботу OSINT аналітика. Наприклад, запит

site:https://www.unian.ua AND intitle:OSINT

дозволить шукати новини на сайті Уніан, де в заголовку має бути слово OSINT.

Також можна надати декілька загальних порад щодо формулювання Google запитів:

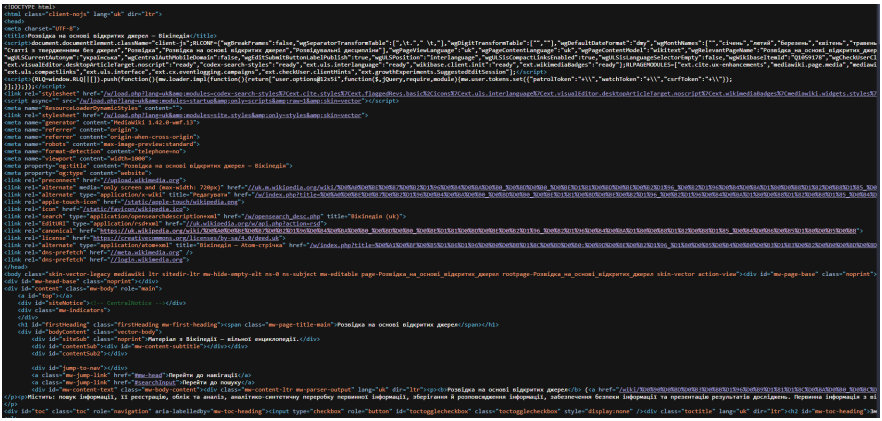
- регістр не має значення. Не важливо, чи вводиться запит великими або маленькими літерами, для Google це не має значення;
- пробіл для Google є оператором «AND». Тобто якщо необхідно знайти велику фразу в запиті, необхідно взяти цю фразу в лапки, інакше Google буде шукати і фразу, і окремі слова, що значно збільшить результати пошуку та ускладнить роботу аналітика;
- Google може змінювати слова за відмінками. Якщо не використовуються лапки в запиті, то саме слово можна не змінювати, Google все одно знайде ці слова;
- Google сортує результати за релевантністю, яка не завжди відповідає потребам аналітика;
- Google шукає тією мовою, якою було зроблено запит;
- на результати пошуку впливають попередні запити. Для того, щоб такого не відбувалося, краще здійснювати пошук в «режимі інкогніто». Або використовувати окремий браузер тільки для OSINT розслідувань;
- на результати пошуку також впливає геопозиція. Це необхідно враховувати, особливо якщо OSINT аналітик використовує VPN-сервіси.

3.3 АНАЛІТИКА ВЕБСАЙТІВ. СОЦІАЛЬНІ МЕРЕЖІ. ТІНЬОВИЙ ІНТЕРНЕТ (DARK WEB)

Після того, як аналітик сформував правильний запит до пошукового сервісу та отримав необхідний результат, він приступає до аналізу власне сторінок, які його цікавлять. Загалом аналітик починає одразу аналізувати контент — текст, зображення, відео тощо. У той же час необхідно зауважити, що інколи доцільно також проводити аналітику самого вебсайту, адже в коді сторінки також може міститися інформація, яка може мати значення для розслідування.

Будь-який веббраузер дозволяє переглядати код вебсторінки, достатньо лише натиснути правою кнопкою миші на будь-яке неінтерактивне місце сайту та обрати пункт «Джерело сторінки» чи «Переглянути джерело сторінки» (формулювання можуть змінюватися в залежності

від веббраузера). Після цього аналітику відкривається код відповідної сторінки (мал. 3.2).



Мал. 3.2. Код сторінки «Розвідка на основі відкритих джерел» з Вікіпедії

Очевидно, що для того, щоб повністю зрозуміти, що зазначено в коді, необхідно мати досить глибокі знання в сфері програмування. У той же час OSINT аналітику достатньо лише певних базових знань для того, щоб отримати корисну для себе інформацію.

Переважна більшість вебсайтів створена за допомогою стандартизованої мови розмітки документів HTML. Відповідно, HTML має свою певну структуру, знання якої допоможе краще розібратися в кодах вебсторінок. Так, загальна структура HTML виглядає наступним чином

```
<! DOCTYPE html>
<html>
        <head>
                <title>Це Заголовок. Саме ця назва буде відображатися в пошуковому сервісі, коли користувач буде шукати цю сторінку</title>
        </head>
        <body>
                <p>Це зміст самої сторінки, яку буде бачити користувач, коли зайде на сайт</p>
        </body>
</html>
```

Стандартний документ HTML складається з трьох частин, кожна з яких відокремлюється тегом (всі теги беруться в дужки <тег>). Так, першим елементом є декларація типу документа <! DOCTYPE html>, в якому розробник сайту повідомляє, що це за документ. Найчастіше в інтернеті використовують саме html, що і зазначено в прикладі. Ця частина, як правило, не містить важливої інформації для OSINT аналітика та складається лише з одного рядка (хоча можуть бути і винятки).

Далі розробник сайту має на програмному рівні повідомити, що починається власне сайт, який має розпізнаватися насамперед пошуковими сервісами. Це повідомляється шляхом використання тегу <html>, що означає, що за цим тегом починається опис та вміст сайту. Звертаємо увагу, що значна кількість тегів в HTML працює як дужки в математичному рівнянні — якщо дужка була відкрита, то вона має бути і закрита. Відкритий тег виглядає як <html>, закритий </html>. Це дозволяє комп'ютеру зрозуміти, що між цими двома тегами міститься інформація, яка стосується самого сайту. Звертаємо увагу, що абзаци та відступи не мають ніякого впливу на те, як буде інтерпретуватися код сторінки, абзаци та відступи робляться лише для того, щоб програмістам чи іншим особам було легко створювати, оновлювати та переглядати код. Ключовими в даному випадку будуть теги, які показують початок та кінець відповідної частини коду.

Після тегу <html> починається друга частина сайту — шапка документа, в якій записано загальні технічні відомості або додаткова інформація про документ, яка не відтворюється безпосередньо в браузері. Шапка документа міститься між тегами <head> та </head>. Саме в цій частині буде надаватися вся інформація, яка стосується функціонування самої сторінки вебсайту, яка не буде відображена на головному екрані. Як правило, саме ця частина вебсайту містить найцікавішу для OSINT аналітика інформацію. Зазначаємо, що в межах одного тегу можуть бути і інші. Так, в прикладі, який було надано вище, в тегу <head> також присутні теги <title> та </title> (title — заголовок). Це означає, що в шапці документа буде міститься заголовок, який поміщено між цими тегами. Закриття тегу </title> не означає, що було закрито тег <head>, а отже, шапка сайту продовжується.

Саме в шапці документа можуть міститися теги, які мають значення для OSINT аналітиків. Насамперед це стосується метаданих та, відповідно, тега <meta>. Метадані — це певна інформація про дані. HTML тег <meta> зберігає інформацію, призначену для браузерів і пошукових систем. Наприклад, механізми пошукових систем звертаються до метатегів для отримання опису сайту, ключових слів та інших даних. Метадані не відображаються на сторінці, але браузери та пошукові системи будуть їх інтерпретувати. Часто використовуються декілька тегів <meta>. Метадані можуть бути використані браузерами (наприклад, як правильно відобразити контент), пошуковими системами (наприклад, для визначення опису сайту, ключових слів та інших даних), або іншими вебсервісами.

Після того як закінчується шапка документа, ставиться тег </head> та починається третя частина — тіло документа, що розпочинається з тега <body>. У межах тегів <body> та </body> надається вся інформація, яку може побачити користувач на своєму браузері. Як правило, це найбільш масивна за обсягом частина коду, яка має досить складну структуру. Шукати певну інформацію вручну в цій частині досить незручно, тому OSINT аналітики використовують функцію пошуку (Ctrl+F для Windows або Command+F для Mac), коли в змісті сайту необхідно знайти конкретне посилання, IP адресу, ідентифікатор користувача тощо. У даному випадку все буде залежати від потреб конкретного OSINT розслідування. Тут також необхідно зазначити, що серед OSINT аналітиків існує окремий процес, який має назву вебскрейпінг (Web Scraping), тобто процес збору даних сайту, який включає в себе надсилання запиту до сервера, отримання HTML вмісту сторінки та копіювання цього змісту. Досить часто для цього застосовують окреме програмне забезпечення. Не вдаючись до деталей вебскрейпінгу, необхідно лише зауважити, що цей процес може суперечити правилам користування сайтом чи навіть бути незаконним в окремих країнах. Тому OSINT аналітику необхідно уважно дослідити питання законності перш ніж здійснювати вебскрейпінг.

Як вже було неодноразово зазначено, обсяги та детальність проведення OSINT розслідування будуть залежати від завдань, які ставляться перед аналітиками. Даний підручник не ставить за мету описати всі можливі способи отримання інформації, але надає лише певні вказівки,

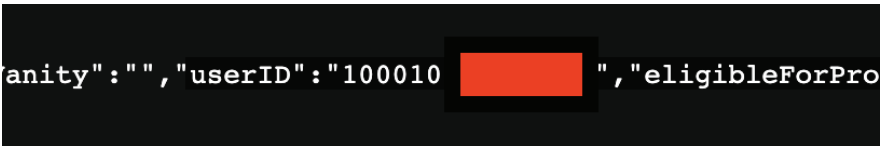
які мають допомогти розібратися в базових методиках проведення OSINT розслідувань.

Продовжуючи аналіз контенту різних інтернет-сайтів, необхідно перейти до аналітики соціальних мереж. Перш ніж розпочинати пошук в соціальних мережах, для початку необхідно в них зареєструватися (хоча це може бути необов'язкова умова). Якщо особа не обмежила доступ до свого профілю, то для соціальних мереж, які вимагають реєстрації, цього вже має бути достатньо, щоб отримати важливу інформацію про особу, яка представляє інтерес для OSINT аналітиків. Також можна використовувати додаткове програмне забезпечення, яке дозволяє автоматично завантажувати вміст сторінки та яке розроблено під конкретну соціальну мережу. Крім того, існує низка програм або розширень для браузера, що спеціалізуються на різних соціальних мережах, які пропонують вилучення певної інформації. Також існує спеціальний інструментарій для того, щоб здійснювати перегляд закритих сторінок. У даному випадку необхідно наголосити, що такий інструментарій має бути обмежений, а його використання чітко санкціоноване у спосіб, передбачений чинним законодавством, адже проникнення до приватних профілів прирівнюється до негласних слідчих (розшукових) дій, які суттєво обмежують права та свободи людини. Ось чому будь-який OSINT аналітик повинен чітко знати ліміти своєї «білої», активності, яка не порушує приписи законодавства. Додатковий інструментарій також може бути застосований, але він обов'язково має відповідати вимогам КПК України та інших профільних законів чи підзаконних нормативно-правових актів. У той же час OSINT аналітики можуть продовжувати свої пошуки без негласного доступу до закритих профілів, наприклад, шляхом аналізу пов'язаних сторінок у соціальних мережах із цільовою сторінкою. Слід нагадати, що для досягнення результату будь-якого OSINT розслідування необхідно не лише збирати інформацію, а і проводити її аналітику. Інколи краще отримати інформацію не напряму, а через суміжні джерела, які в своїй сукупності дозволяють зробити висновок про об'єкт, який цікавить OSINT аналітика.

При цьому також необхідно враховувати, що соціальні мережі постійно оновлюються з точки зору функціоналу, який ускладнює роботу аналітиків. Насамперед це робиться саме задля захисту приватності

користувачів таких соціальних мереж. Наприклад, у Facebook в 2014 році частково зникла функція пошуку за зображеннями, аж поки її повністю не прибрали в 2019 р. У 2015 р. Facebook видалив можливість проводити детальний пошук профілів користувачів у полі пошуку; у 2020 р. було вилучено оператор «*», який дозволяв замінювати символи у полі пошуку. Також почали зникати і інші оператори пошуку, про які мова велася вище. Частина науковців припускає, що це робиться саме задля перешкоджання збору даних, що підтверджується великою кількістю вебскрейперів. Крім того, регулярно блокуються облікові записи користувачів Facebook, які використовують інструменти та методи OSINT (Bazzell 2021)[1]. Загалом логіка такої поведінки адміністрації Facebook є цілком зрозумілою — вони намагаються гарантувати захист персональних даних власних користувачів та мінімізувати ризики витоку інформації. Варто пам'ятати, що OSINT технології можуть використовуватися і зловмисниками для вчинення шахрайських дій або інших злочинів. Ось чому слід ще раз наголосити, що OSINT аналітики мають чітко розуміти правила поведінки на сайтах, чинне законодавство та загальні стандарти захисту персональних даних задля уникнення випадкового вчинення незаконних дій в процесі проведення розслідування.

При цьому способів збору інформації в соціальних мереж все одно є досить багато. Наприклад, можна зайти на сторінку користувача Facebook, який цікавить OSINT аналітика, відкрити джерело сторінки (про що велася мова вище), та у функції пошуку ввести «UserID», що дозволить знайти ідентифікатор даного користувача (мал. 3.3).

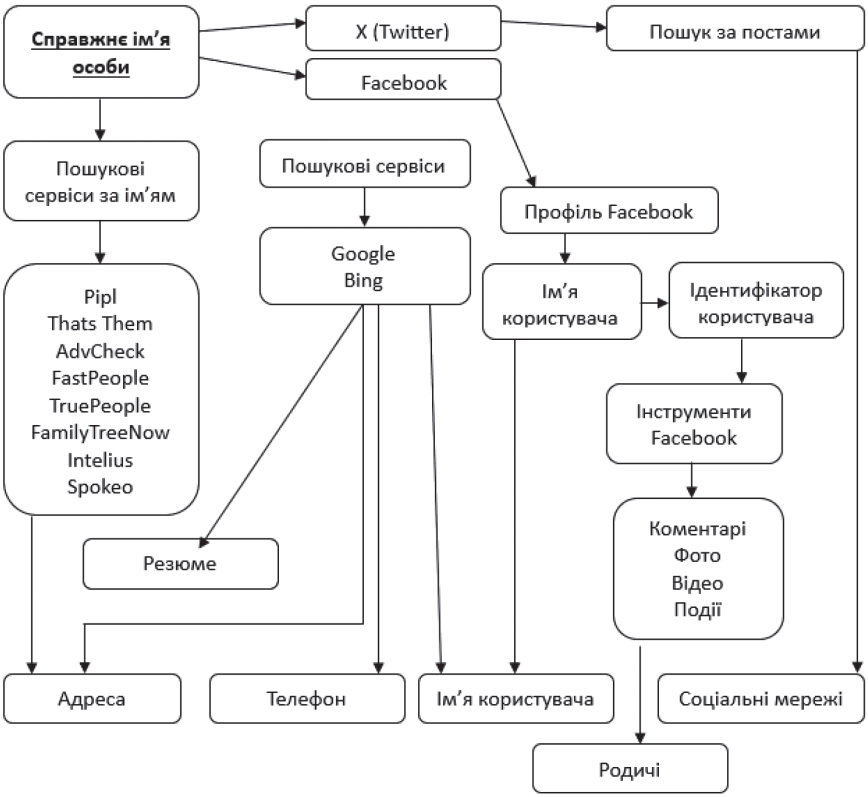


Мал. 3.3. Приклад ідентифікатора UserID користувача Facebook в коді HTML сторінки

[1] Bazzell M. (2016). Open source intelligence techniques: resources for searching and analyzing online information. CCI Publishing.

Маючи цей числовий ідентифіктор користувача, можна отримати досить багато інформації про самого користувача з відкритих джерел, користуючись додатковим програмним забезпеченням.

Власне, існують навіть цілі алгоритми того, як можна знайти корисну інформацію, знаючи, наприклад, лише справжнє ім'я особи, яка цікавить OSINT аналітика (мал. 3.4).



Мал. 3.4. Алгоритм роботи аналітика з відкритими джерелами, якщо йому відоме справжнє ім'я особи[1]

[1] Open Source Intelligence Techniques (OSINT) for Fraud Prevention. SEON Technologies Ltd. URL: https://resources.cdn.seon.io/uploads/2022/02/SEON_Guide_to_OSINT.pdf

Таким чином, OSINT аналітик повинен постійно шукати не лише конкретну особу, яка його цікавить, а і будь-які зв'язки з цією особою, адже саме ці зв'язки можуть дати критично важливу інформацію для розслідування. Тому пошук необхідно проводити серед усіх доступних джерел. У даному випадку слід наголосити, що, крім «видимого» для звичайного користувача інтернету, існують і додаткові його «шари», один з яких має назву дарк веб і потребує спеціальної підготовки та програмного забезпечення для того, щоб ним користуватися.

Якщо дивитися на інтернет саме через призму шарів, то прийнято виділяти три шари — поверхневий інтернет (Surface Web), глибокий інтернет (Deep Web) та тіньовий інтернет (Dark Web). Поверхневий інтернет — це та частина інтернету, яка доступна всім користувачам через звичайні пошукові сервіси (наприклад, сайти новин, відкриті пости блогерів, соціальні мережі тощо). З загального обсягу такі сторінки (тобто поверхневий інтернет) займає 4 % (при цьому через пошукові сервіси можна знайти лише 0,03 % всіх інтернет-сторінок, які існують в мережі). Глибокий інтернет — це сторінки, на які неможливо потрапити через пошукові сервіси та які потребують певного рівня доступу. Сюди відносяться бази даних банків, лікарень тощо. Наприклад, кожен може потрапити на головну сторінку банку, який його обслуговує, через звичайний пошук в Google (поверхневий інтернет), проте зайти на конкретну сторінку конкретного користувача можна лише за допомогою логіну та паролю. На цю сторінку неможливо потрапити сторонній особі лише через пошуковий запит в Google, адже пошукові сервіси такі сторінки спеціально не індексують. На глибокий інтернет приходиться 96 % всього контенту в мережі.

Тіньовий інтернет працює дещо інакше. Насамперед необхідно зазначити, що Dark Web з'явився задля забезпечення анонімності його користувачів. Оскільки інтернет продовжував розвиватися в середині-кінці 1990-х років, в глобальному масштабі він почав змінювати багато сфер життя, особливо способів обміну інформацією. Проблема полягала в тому, що інтернет з самого початку не розроблявся з урахуванням конфіденційності та анонімності користувачів. Проте деякі користувачі дуже турбувалися про свою анонімність і основним серед них був Федеральний уряд США. Так, команда програмістів та математиків,

які працювали в одному з відділень ВМС США, розробили нову технологію під назвою Onion Routing («цибулева маршрутизація», за аналогією з цибулею, яка складається з багатьох шарів). Мережа, яка використовує «цибулеву маршрутизацію», називається Dark Net. Відповідно, Dark Web — це сукупність всіх мереж Dark Net.

Dark Web є частиною всесвітньої мережі Інтернет, але не є частиною поверхневого інтернету та до нього неможливо отримати доступ через звичайне програмне забезпечення. Власне, рівень анонімності, який забезпечується в Dark Web, став приводом для того, що дана мережа є вкрай популярною для розповсюдження незаконного контенту та вчинення інших злочинів. Так, одне дослідження показало, що з 2723 сайтів в Dark Web, які аналізувалися протягом п'яти тижнів, у 57 % було виявлено незаконні матеріали[1]. У той же час ми маємо підкреслити, що далеко не все, що є в даркнеті, є незаконним. Досить часто цю мережу використовують журналісти для анонімного спілкування зі своїми джерелами, або через даркнет користувачі можуть написати скарги на будь-яких офіційних осіб, якщо вони бояться переслідування. У розумних руках це може бути дуже сильним інструментом, у тому числі при проведенні OSINT розслідувань.

Загалом необхідно зазначити, що досить рідко коли OSINT розслідування поверхневого інтернету змусить аналітика також проводити розслідування в тіньовому інтернеті. Мова йде про те, що незаконна активність, яка відбувається в поверхневому інтернеті (наприклад, незаконні фінансові махінації, заклики до вчинення терористичних актів тощо), рідко коли пересікається з активністю в тіньовому інтернеті (торгівля наркотиками, зброєю, підробними документами тощо), і навпаки. OSINT аналітик, який буде проводити розслідування в тіньовому інтернеті, як правило, буде робити це саме у зв'язку із вчиненням злочинів конкретно в Dark Web, а не через те, що йому необхідно отримати додаткову інформацію про об'єкт розслідування, відомості про який містяться в поверхневому інтернеті. Тому OSINT розслідування в тіньовому інтернеті має низку своїх особливостей.

[1] Daniel Moore & Thomas Rid (2016) Cryptopolitik and the Darknet, Survival, 58:1, 7–38.

Так, першим завданням, яке ставиться перед OSINT аналітиками, є виявлення вузлів даркнету, які використовуються для незаконної активності. Інколи буває це зробити досить проблематично, адже в тіньовому інтернеті не працюють звичайні пошукові сервіси, а ті, які наявні, все ще далекі від ефективного пошуку в мережі.

Після виявлення вузла (сайту) наступним завданням є виявлення особи (осіб), яка причетна до його діяльності. Як вже зазначалося, основною перевагою тіньового інтернету є високий рівень анонімності користувачів, тому ідентифікувати IP-адреси вкрай складно. У зв'язку з цим пропонується зосередитися на ідентифікації географічного розташування осіб, які причетні до злочинної діяльності в Dark Web. У поверхневій мережі це зробити набагато легше, адже, як показують дослідження, приблизно 1,5 % всіх повідомлень в X (Twitter), мають геотеги. В Instagram цей показник вже збільшується до 20 %. Очевидно, що очікувати на геотеги в тіньовому інтернеті не варто. Іншим методом геолокації людей, які цікавлять OSINT аналітиків, була б перевірка змісту їхніх постів, біографії чи оголошень, які ними публікуються. Проте і такий метод складно назвати успішним саме через те, що злочинці в тіньовому інтернеті не публікують будь-які особисті дані, які дозволять їх ідентифікувати. Той факт, що визначення місцезнаходження злочинців в тіньовому інтернеті є настільки проблематичним, призводить до того, що правоохоронці навіть не знають, де саме знаходиться злочинець, та часто взаємодіють з цілою групою осіб, які залучені до незаконної діяльності, які можуть знаходитися в різних кінця світу. Навіть існує висока вірогідність того, що через обмеженість фінансового та людського ресурсу керівництво може просто припинити розслідування злочинів, які вчиняються в тіньовому інтернеті.

На сьогоднішній день найбільш дієвим способом припинення незаконної діяльності в тіньовому інтернеті є переміщення злочинної діяльності з цифрового світу в реальний, наприклад в процесі передачі наркотичних препаратів, які були придбані через тіньовий інтернет. Зазвичай це означає, що або агент правоохоронних органів вступає в контакт з онлайн-злочинцем і змушує його зустрітися в реальному житті, або, навпаки, особа намагається придбати незаконний

товар, який пропонують представники правоохоронних органів під прикриттям, що також дає можливість фізичного контакту з такою особою. Проте саме надмірна анонімність та відсутність єдиної системи розслідування злочинів в тіньовому інтернеті є однією з найбільших труднощів, які стоять перед представниками правоохоронних органів, адже досить часто трапляються ситуації, коли правоохоронці виходили «на самих себе» при спілкуванні зі злочинцями, які також виявлялися агентами, які проводили власне аналогічне розслідування[1].

3.4 АНАЛІТИКА ЗОБРАЖЕНЬ ЗА ДОПОМОГОЮ OSINT ІНСТРУМЕНТІВ

Інформаційні технології постійно розвиваються, і мережа Інтернет не є винятком. Підвищення доступності всесвітньої мережі та збільшення швидкості доступу дозволило розробникам вебконтенту та користувачам зробити інтернет більш графічним. Зараз складно навіть уявити собі соціальну мережу або блог без фотографії автора, місцевості, про яку йде мова, або об'єкта, який описується. Все це вказує на те, що будь-які зображення стають так само важливим джерелом інформації, який не можуть ігнорувати OSINT аналітики. До того ж інколи зображення, які публікуються в інтернеті, можуть розповісти більше, ніж власник цього зображення планував, адже в зображеннях може міститися прихована інформація, яку реалістично отримати за допомогою відносно поширеного програмного забезпечення. Зображення можуть надати дуже багато корисної інформації OSINT аналітикам, адже вони можуть показати, як виглядає певна особа, де вона перебувала, якими транспортними засобами користувалася тощо. Встановлення цієї інформації може значно спростити спостереження за особою та її можливе подальше затримання, що було б неможливо лише на основі текстової інформації, наявної в інтернеті.

Для прикладу можна взяти фотографію візиту Бориса Джонсона до Києва з офіційного вебсайту Президента України (мал. 3.5).

---

[1] Akhgar, Babak & Bayerl, Petra & Sampson, Fraser. (2016). Open Source Intelligence Investigation: From Strategy to Implementation.

Мал. 3.5. Володимир Зеленський та Борис Джонсон у Києві, 2022 рік[1]

Уявімо, що в OSINT аналітика наявна лише частина цього фото не надто високої якості (мал. 3.6) і йому необхідно отримати максимальний обсяг інформації з такої світлини.

Мал. 3.6. Частина фото, яка є в розпорядженні умовного OSINT аналітика

[1] Volodymyr Zelenskyy and Boris Johnson visited St. Michael's Golden-Domed Monastery and had a walk in Mykhailivs'ka Square. PRESIDENT OF UKRAINE. Official websit. URL: https://www.president.gov.ua/en/news/volodimir-zelenskij-i-boris-dzhonson-vidvidali-svyato-mihajl-75873

Інколи спочатку необхідно спробувати покращити якість самого зображення. Для цього вже розроблені спеціальні онлайн-сервіси, які є у відкритому доступі. До таких, наприклад, відноситься Remini (https://app.remini.ai) (безкоштовний функціонал є дещо обмежений, але для базового OSINT розслідування навіть його буде достатньо), який за допомогою штучного інтелекту «домальовує» або деталізує елементи зображення, яке йому надається (мал. 3.7).

Мал. 3.7. Результат покращення якості фото за допомогою сервісу Remini

Далі OSINT аналітик використовує пошукові системи, які можуть шукати за зображеннями в інтернеті. На даний момент таких систем є досить багато як платних, так і безкоштовних. До найбільш популярних часто відносять Google Images (https://www.google.com/imghp) та TinEye (https://tineye.com). При цьому необхідно зазначити, що пошуковий сервіс Google Images більше спеціалізується на пошуку подібних зображень, тому якщо особа, яка цікавить аналітика, не є досить відомою, то шанси знайти її саме через Google Images відносно невеликі. У такому випадку краще застосовувати саме TinEye. «Причина, чому він працює краще, ніж пошукові гіганти, такі як Google і Bing, полягає в тому, що TinEye використовує спеціальний алгоритм розпізнавання облич. Google і Bing використовують різні підходи та зосереджуються на алгоритмах схожості зображень. Наприклад, якщо у вас є фотографія жінки в червоній сукні, яка стоїть перед деревом, Google і Bing спробують знайти інших жінок у червоній сукні, які стоять перед деревом. Вони вважатимуть риси обличчя

менш важливими. Спеціалізовані ж засоби пошуку будуть зосереджені виключно на обличчі та ігноруватимуть фон та одяг»[1].

За пошуком оригінального зображення TinEye не зміг визначити першоджерело (сайт Президента України), проте надав в якості результатів інші сайті новин, за якими можливо визначити особу на фото. У даному випадку необхідно звернути увагу на декілька цікавих особливостей. Так, інколи пошук зображення гіршої якості, яке не було вдосконалено за допомогою штучного інтелекту, може надати більше результатів, ніж пошук вдосконаленого зображення. Це означає, що OSINT аналітик повинен шукати за всіма типами зображень, які у нього наявні. Також інколи TinEye в якості результату шукає не лише те фото, яке надавалося для пошуку, а трохи інше (наприклад, фото тієї самої людини могло бути зроблене з іншого ракурсу або з іншим виразом обличчя). Такі результати пошуку ще раз демонструють здібності даного сервісу до пошуку саме за рисами обличчя.

Очевидно, що наведене в якості прикладу фото є відносно популярним, а тому знайти джерело такого фото та ідентифікувати людей, які на ньому зображені, відносно легко. У реальності OSINT аналітики будуть шукати людей маловідомих або взагалі невідомих, а тому результати будуть не такими чіткими. У той же час можливість розпізнавання обличчя дозволяє знаходити і таких осіб. Необхідно бути готовим, що фотографії, які будуть знайдені, будуть низької якості, на них можуть бути особи, які лише схожі на суб'єкта пошуку або взагалі не мають ніякого відношення до розслідування. Як вже було неодноразово зазначено, OSINT розслідування є процесом тривалим та багатоаспектним, а результати розслідування насамперед залежать від аналітики, яка буде зроблена за результатами всіх можливих пошуків, у тому числі і пошуків за зображенням. Неправильно буде посилатися лише на одне джерело, адже будь-який доказ має підтверджуватися іншими, бажано — незалежними доказами. OSINT аналітик повинен розуміти, що пошук за зображенням може бути як проривом у розслідуванні, так і лише одним шматочком пазлу, який необхідно зібрати.

---

[1] How to find anyone by photo. The secrets of Reverse Image Search. Osintteam: website. URL: https://www.osintteam.com/how-to-find-anyone-by-photo-the-secrets-of-reverse-image-search/

Існують наступні поради щодо покращення результатів пошуку за зображенням:

– вдосконалити якість фото (хоча, як показують приклади, далеко не завжди це дійсно дозволить покращити результати пошуку);
– ділити фото на окремі частини і шукати за цими частинами. Якщо на фотографії є декілька осіб, то набагато ефективніше буде шукати не ціле фото, а кожну особу окремо;
– прибрати фон. Інколи фон може погіршити результати пошуку обличчя людини на фотографії, тому рекомендується за можливості фон прибирати (зараз є безліч безкоштовних онлайн-сервісів, які пропонують такі послуги).

Також необхідно пам'ятати, що за допомогою аналітики можна встановити місце, де було зроблене фото, яке цікавить OSINT аналітика, що інколи може бути критично важливим для розслідування. Для цього також існує низка інструментів, якими користуються OSINT аналітики.

Так, група експертів детально описала[1] процес встановлення геолокації лише за одним фото (мал. 3.8).

За допомогою пошуку Google Images та назви вулиці, яку можна побачити на фото, аналітики визначили назву церкви, яка (потенційно) зображена на фото. Далі за допомогою сервісів https://satellites.pro та Google Earth (https://earth.google.com) було знайдено супутникові знімки саме цієї церкви, де були

Мал. 3.8. Фото, яке було надано OSINT аналітикам для визначення геолокації

[1] Imagery as the key to deep geoanalysis within OSINT. Hack Your Mom : website. URL: https://hackyourmom.com/en/kibervijna/zobrazhennya-yak-klyuch-do-glybokogo-geoanalizu-v-ramkah-osint/

порівняні деталі будівлі, які можна легко упізнати. Також було використано пошук зображення за назвою церкви, щоб порівняти характерні архітектурні особливості будівлі з оригінальним фото (мал. 3.9).

Мал. 3.9. Результат, який було знайдено OSINT аналітиками

Завдяки цьому були встановлені координати того місця, з якого було зроблено оригінальне фото. Очевидно, що сам процес встановлення геолокації даного фото включав у себе безліч пошукових запитів та сумарно тривав годину, проте в цілому аналітиком були пройдені відносно «стандартні» способи пошуку зображення в інтернеті. Для встановлення геолокації наразі використовуються також більш складні онлайн-сервіси та способи аналітики, які також дозволяють визначати час, коли було зроблено фото, завдяки розміру та куту нахилу тіні, аналізують специфічні риси пейзажу, рослинність, тобто будь-що, що дозволить визначити геолокацію фото. Така аналітика є відносно складною та потребує додаткових знань, вмінь та навичок. Проте вкрай складною її також назвати не можна. На даний момент в мережі Інтернет є безліч інструкцій, курсів, статей та підручників, які стосуються суто визначення геолокації фото. Крім того, також є велика кількість програм та сервісів, які значно спрощують таку аналітику. Очевидно, що описати

всі методи та способи в даному підручнику неможливо, особливо з урахуванням того, що вони постійно змінюються та оновлюються. Проте навіть таких базових знань буде достатньо щоб розпочати OSINT розслідування та в процесі вивчати нові способи та методи аналітики фотографій.

3.5 МЕТАДАНІ

У найбільш простому формулюванні метадані — це дані про дані. У Вікіпедії зазначено, що метадані — «це дані, що характеризують або пояснюють інші дані. Наприклад, значення «123456» само по собі недостатньо виразне. А якщо значенню «123456» зіставлено достатньо виразне ім'я «поштовий індекс» (що вже є метаданими), то в цьому контексті значення «123456» більш осмислене — можна витягати інформацію про місцеположення адресата, що має даний поштовий індекс»[1].

Метадані можуть міститися в різних цифрових елементах, таких як вебсайти, фотографії, відео тощо. Без метаданих результативність OSINT розслідування за зображенням чи відео може значно зменшитися. Метадані дозволяють OSINT аналітикам бути впевненими в тому, що вони працюють з найбільш релевантною інформацією, що має суттєве значення в процесі розслідування. «Уявіть, що ви маєте 1 мільйон випадкових статей і ви шукаєте конкретну статтю про подію, що сталася на минулих вихідних в Техасі. Замість того, щоб переглядати 1 мільйон статей, чи не буде зручніше відсортувати статті за місцем їх створення чи місцем, на яке в статті є посилання? Саме тут в нагоді стануть метадані»[2].

На даний момент існує безліч онлайн-сервісів, які дозволяють переглянути метадані. При цьому слід наголосити, що метадані можуть міститися у фото, відео, вебсайті, pdf файлі тощо, адже метадані надають відомості про саме джерело інформації незалежно від його типу.

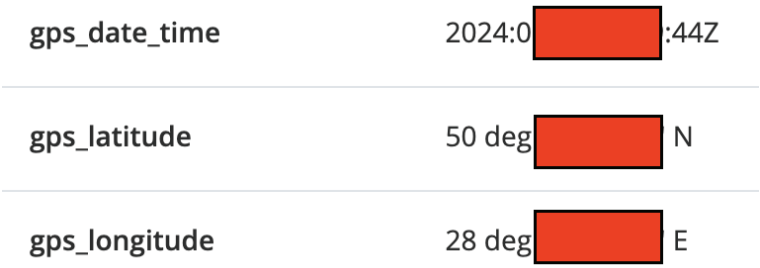
---

1 Метадані. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Метадані

2 Meet Your Data: Metadata & Why It Matters To Intelligence Researchers. Media Sonar : website. URL: https://mediasonar.com/2021/02/18/metadata-why-it-matters-to-intelligence-researchers/

Очевидно, що для перегляду метаданих відеофайлу та pdf файлу можуть знадобитися різні сервіси, але завдяки їхній доступності пошук таких сервісів не має бути чимось занадто складним.

Так, наприклад, для перегляду метаданих зображень, відео, doc, pdf та низки інших типів файлів можна використовувати сервіс https://www.metadata2go.com. За допомогою цього сервісу можна побачити інформацію про файли, які цікавлять OSINT аналітика. Наприклад, при перегляді метаданих завантаженого фото можна побачити тип пристрою, на який було зроблене фото, дату, час та навіть координати місця, де це фото було зроблено (мал. 3.10).



Мал. 3.10. Приклад метаданих, де зазначені координати та час зробленого фото

Аналогічну інформацію можна отримати і з відеофалів чи текстових документів. Метадані можуть містити дуже важливі дані, про які автор файлу, що досліджується, може навіть не здогадуватися. Крім того, метадані можна знайти і в HTML коді вебсайтів. У даному випадку використовується тег <meta> в головній частині коду сайта. Метадані сайту можуть бути різноманітними та в більшості випадків стосуються технічних особливостей роботи вебсторінок. У той же час досвідчені OSINT аналітики також можуть зібрати необхідну для себе інформацію і з таких джерел.

Наприклад, тег

<meta name="author" content="John">

в головній частині сайту зазначає, що даний елемент метаданих має відношення («називається» — name) до автора сайту (author), а конкретніше автором цього сайту є John. У даному випадку наведено лише приклад одного з тегів метаданих вебсайту, їх є набагато більше, а тому особи, які проводять розслідування, повинні чітко знати, які саме метадані їх цікавлять.

Аналізуючи метадані, можна дізнатися набагато більше, ніж вивчаючи лише зміст файлу, який цікавить OSINT аналітика. У той же час необхідно пам'ятати про низку правил та пересторог. Так, для перегляду метаданих бажано використовувати одразу декілька різних сервісів, щоб можна було підтвердити правильність отриманої інформації. Крім того, необхідно пам'ятати, що метадані не є панацеєю. У вільному доступі існує програмне забезпечення, яке дозволяє прибирати метадані з файлів. Деякі соціальні мережі автоматично видаляють дані про координати місця, де було зроблено фото, одразу після завантаження такого фото у відповідну мережу. У налаштуванні деяких мобільних пристроїв можна змінити обсяг метаданих, який буде фіксуватися разом з фото чи відео. Відповідно, аналітика таких фотографій за допомогою метаданих буде значно обмеженою.

Також існують способи модифікації метаданих, тобто зміни первинних відомостей на ті, які потрібні користувачу. Тобто навіть якщо аналітик виявив метадані файлу, вважати їх стовідсотково правильними не можна. Відомості, отримані з метаданих, самі по собі не можуть використовуватися як докази в розслідуванні. Метадані можуть вказувати на інші відомості, які також необхідно верифікувати. Такі дані можуть використовуватися як додаткова перевірка відомостей, які вже були отримані в ході OSINT розслідування. У будь-якому випадку метадані необхідно розглядати не як єдине та беззаперечне джерело інформації, а лише як одне з джерел отримання інформації, яка все одно потребуватиме перевірки іншими доказами.

3.6 ШТУЧНИЙ ІНТЕЛЕКТ ТА OSINT

Велика кількість OSINT аналітиків, спеціалістів з кібербезпеки та вчених висловлюють однакові думки відносно того, що штучний

інтелект (ШІ) здійснить революцію у багатьох сферах. За прогнозами спеціалістів, ринок ШІ збільшиться з 119 мільярдів доларів у 2022 р. до 1,59 трильйону доларів у 2030[1].

Очевидно, що ШІ не може не вплинути і на OSINT розслідування. Завдяки своїй здатності обробляти величезні обсяги даних та встановлювати в них закономірності, ШІ дав можливість аналітикам та дослідникам виявляти важливу інформацію зі значного обсягу даних, які були наявними у вільному доступі. Поєднання ШІ та OSINT — це дещо більше, ніж лише поєднання методики розслідування з певним інструментарієм. Так, виділяють наступні способи покращення OSINT розслідування за допомогою ШІ:

– підвищення точності даних.

Здатність ШІ аналізувати дані без будь-яких упереджень, які притаманні людині, значно підвищує точність та зменшує кількість помилок такої аналітики;

– швидкість отримання інформації.

У швидкоплинному світі інформації своєчасність інколи може мати вирішальне значення. Швидкість ШІ, з якою він може обробляти інформацію, означає, що статистичні дані можна генерувати в режимі реального часу, що дає аналітикам перевагу в оперативності реагування на ситуації, які виникають;

– прогнозування.

Прогностичні можливості ШІ є скарбом для OSINT аналітиків. Виявляючи тенденції та екстраполюючи майбутні сценарії, аналітики можуть швидко реагувати на потенційні загрози, що значно покращує планування та проведення розслідування.

Експерти вказують на такі способи вдосконалення OSINT розслідувань за допомогою технології ШІ:

– збільшення масштабу збору та обробки даних.

ШІ може швидко аналізувати величезні обсяги даних з різних джерел. Це стосується не лише тексту, а і зображень, відеофайлів чи інших типів медіафайлів. Це дозволяє аналітикам ефективно збирати

[1] Artificial Intelligence (AI) Market — Global Industry Analysis, Size, Share, Growth, Trends, Regional Outlook, and Forecast 2023–2032. Precedence Research : website. URL: https://www.precedenceresearch.com/artificial-intelligence-market?ref=blog.sociallinks.io

інформацію з різноманітних платформ незалежно від мови джерела. Однією з найважливіших переваг ШІ в OSINT є його здатність обробляти величезні обсяги даних за лічені хвилини. Традиційні «ручні» методи збору та аналізу даних не можуть зрівнятися з вміннями ШІ обробляти великі обсяги даних. Алгоритми ШІ можуть швидко сканувати численні вебсайти, соціальні мережі, форуми та новини, щоб зібрати потрібну інформацію — завдання, яке у людей-аналітиків може зайняти години чи навіть дні;

– визначення зв'язків.

Алгоритми ШІ створені для визначення закономірностей і зв'язків у даних, які складно помітити аналітикам. Такі алгоритми можуть надавати важливу інформацію про тенденції, взаємозв'язки та потенційні загрози. Надаючи ШІ різні набори даних, аналітики можуть розробляти інструменти, які визначатимуть, на перший погляд, непомітні зв'язки між даними;

– автоматизація повторюваних завдань.

ШІ може автоматизувати завдання, які потребують багато часу та повторюються, наприклад моніторинг змін вебсайтів, відстеження розмов у соціальних мережах тощо. Це дозволяє OSINT аналітикам концентруватися на інших, більш складних завданнях[1];

– обробка природної мови (Natural Language Processing — NLP).

NLP дозволяє системам ШІ розуміти та обробляти людську мову. Це важливо для таких завдань, як аналіз настроїв населення, узагальнення текстового вмісту повідомлень у соціальних мережах чи новинах. Обробка людської мови — це один з напрямів ШІ, який дозволяє комп'ютерам розуміти, інтерпретувати та генерувати людську мову (як то ChatGPT). Такий лінгвістичний аналіз забезпечує цілісне уявлення про суспільні настрої та думки, що є дуже важливим в процесі прийняття рішень OSINT аналітиками.

Так, аналітики можуть використовувати ChatGPT для перетворення неструктурованих даних у зручний табличний формат. Більш нові моделі NLP продемонстрували непогані результати при узагальненні

[1] Inderjeet Singh. AI in OSINT: Revolutionizing Open Source Intelligence. Medium : website. URL: https://inderbarara.medium.com/ai-in-osint-revolutionizing-open-source-intelligence-131ab8c79467

великих текстів, що дозволяє зекономити OSINT аналітику багато часу. Моделі відповідей на запитання дозволяють аналітикам ставити питання звичайною мовою щодо неструктурованих даних, які обробляються, і отримувати релевантні та точні відповіді, що полегшує пошук інформації;

– аналітика зображень.

ШІ вже на даний момент здатний аналізувати та інтерпретувати візуальні дані. Вже розроблено програму для аналізу супутникових фото, яка може автоматично визначати геолокацію таких світлин[1]. Також ШІ можна використовувати для класифікації зображень і виявлення об'єктів, які цікавлять аналітика (наприклад, розпізнання зброї на фото в соціальних мережах)[2]. У даному підручнику вже наводився приклад того, як за допомогою ШІ можна покращувати якість фото. Окремі досить потужні платформи ШІ вже доступні будь-кому, в тому числі і OSINT аналітикам, головне — оцінити їхні можливості в процесі проведення розслідувань. Напевно, найяскравішим прикладом масового використання ШІ є NLP системи, і в насамперед мова йде про ChatGPT від OpenAI.

Сам ChatGPT наступним чином описує свої можливості: «Моя головна можливість полягає в аналізі тексту та генерації відповідей на різноманітні запитання. Я можу надавати інформацію з різних галузей знань, допомагати з розв'язанням завдань, надавати поради, писати тексти на різні теми та багато іншого. Моя здатність до навчання стосується даних, які були доступні до мого останнього оновлення в січні 2022 року». ChatGPT навчався з використанням величезних обсягів тексту з інтернету, від електронних книг до баз даних. Хоча точні дані навчання чат-бота залишаються закритими, його попередник, GPT-3, навчався на наборі даних із приблизно 1 трильйона слів. Така величезна кількість даних і є головним секретом потужності чату. Завдяки постійному

---

1 A 'ChatGPT' For Satellite Photos Already Exists. Defence One : website. URL: https://www.defenseone.com/technology/2023/04/chatgpt-satellite-photos-already-exists/385305/

2 Charlie Winter, John Gallacher and Alexander Harris. Artificial Intelligence, OSINT and Russia's Information Landscape. Centre for Emerging Technology and Security. URL: https://cetas.turing.ac.uk/sites/default/files/2023-02/cetas_expert_analysis_-_artificial_intelligence_osint_and_russias_information_landscape.pdf

тривалому навчанню на основі відгуків мільйонів користувачів ChatGPT має великі перспективи як інструмент, який може революціонізувати різні галузі[1].

ChatGPT сам зазначає, що його можливості в сфері OSINT розслідувань включають:

«Аналіз тексту: Я можу аналізувати текст з вебсторінок, соціальних мереж, новин та інших джерел для виявлення важливої інформації або зв'язків.

Пошук інформації: Я можу шукати інформацію за ключовими словами або фразами на різних вебсайтах, форумах, блогах тощо.

Аналіз соціальних мереж: Я можу допомогти в аналізі профілів соціальних мереж, виявленні зв'язків між користувачами, аналізі публічних обговорень та іншого контенту.

Геолокацію: Я можу допомогти визначити місцезнаходження за допомогою геотегів на фотографіях або інших географічних даних.

Аналіз зображень: Я можу аналізувати зображення для виявлення об'єктів, людей, місць тощо.

Структурування інформації: Я можу допомогти організувати зібрану інформацію в зручний для подальшого аналізу формат».

Тестуючи такі можливості, спеціалісти виділили декілька сфер, в яких допомога чату може бути дійсно корисною:

– збір інформації: ChatGPT може збирати інформацію з різних джерел, таких як соціальні мережі, вебсайти новин, форуми та блоги. Увівши певний запит, ChatGPT може сканувати кілька онлайн-джерел і збирати відповідну інформацію в одному місці;
– аналіз даних: ChatGPT може аналізувати великі обсяги даних і давати уявлення про тенденції, настрої та моделі. Вводячи набори даних, ChatGPT може ідентифікувати кореляції та зв'язки, які можуть бути не відразу очевидними для аналітиків;
– відстеження подій: ChatGPT може відстежувати події та стежити за оновленнями в режимі реального часу на платформах соціальних мереж. Увівши певну подію чи хештег, ChatGPT може сканувати

[1] Using the Power of ChatGPT for OSINT. Social Link : website. URL: https://blog.sociallinks.io/using-the-power-of-chatgpt-for-osint/

численні соціальні медіаплатформи та надавати живі оновлення події у міру її розвитку[1];

– аналіз настроїв: класифікація великої кількості тексту на основі суб'єктивного вмісту може бути складною та займати багато часу. Обробка природної мови (NLP) може використовуватись, щоб визначити, чи має вміст тексту позитивний, негативний чи нейтральний тон і подальше використання ШІ демонструє підвищення точності та ефективності даного процесу. Було продемонстровано, що ChatGPT є цінним інструментом для ефективного аналізу великих наборів даних і представлення результатів у відповідній формі[2].

NLP може суттєво спростити такий етап OSINT розслідування, як формування завдання. Так, в OSINT часто проводиться «соціальне прослуховування», яке використовується для визначення громадської думки в соціальних мережах. Соціальне прослуховування дозволяє проводити аналіз настроїв і виявляти тенденції до соціальних заворушень або більш конкретні загрози для окремих осіб. Наприклад, сплеск негативних настроїв у соціальних мережах у певній географічній зоні може автоматично попередити аналітика про необхідність уважніше вивчити проблему, яка склалася. Проблема з поточним «звичайним» програмним забезпеченням для «прослуховування» соціальних мереж полягає в тому, що твіт: «Я готовий померти від щастя» буде вказувати на необхідність аналітика звернути на нього увагу, адже наявне слово «померти», на яке повинно зреагувати «звичайне» програмне забезпечення, хоча з контексту даного повідомлення можна зрозуміти, що слово використано у позитивному значенні. Такі твіти чи повідомлення можуть створювати «інформаційний шум» та забирати дорогоцінний час аналітика, який має на них відволікатися. Великі мовні моделі, такі як ChatGPT, можуть значно покращити програмне забезпечення для соціального прослуховування, оскільки ці моделі можуть також розпізнавати контекст. «Це повідомлення має позитивний відтінок. Воно

---

[1] ChatGPT: The AI-Powered Secret Weapon for OSINT. Medium : website. URL: https://blog.gopenai.com/chatgpt-the-ai-powered-secret-weapon-for-osint-133a68d8302e

[2] Using the Power of ChatGPT for OSINT. Social Link : website. URL: https://blog.sociallinks.io/using-the-power-of-chatgpt-for-osint/

виражає глибоке відчуття щастя або радості до такого ступеня, коли людина готова померти від цього відчуття. Таке висловлення зазвичай означає, що людина переживає надзвичайно позитивні емоції, які перевершують будь-які інші відчуття і можуть викликати сильну емоційну реакцію», — саме так ChatGPT оцінив дане повідомлення[1].

У той же час необхідно пам'ятати і про ризики, які можуть виникати при роботі з NLP. Напевно, найбільшим головним ризиком використання ChatGPT є те, що його завданням є надання відповіді, а не обов'язково правильної відповіді. Це означає, що інколи він може самостійно вигадувати факти та обставини, яких насправді не було, адже цій системі набагато важливіше задовольнити запит користувача, ніж повідомити, що він не знає відповіді (в мережі таку вигадану інформацію від чат-ботів називають «галюцинаціями»)[2]. Відповідно, працюючи з ChatGPT, необхідно ставитися до відповідей, які він надає, з певною долею скептицизму.

3.7 БЕЗПЕКА OSINT АНАЛІТИКА

Будь-які OSINT розслідування мають певні ризики для тих, хто їх проводить. Насамперед це пов'язано з деанонімізацією аналітика, який може поставити під загрозу власну безпеку через те, що його буде ідентифіковано в процесі розслідування. Крім того, існує ризик того, що особа, відносно якої проводиться OSINT розслідування, зможе про це дізнатися через необережні дії аналітика, який проводитиме збір інформації без дотримання базових правил безпеки. Все це вказує на необхідність вивчення цих правил, про які повинен знати та пам'ятати кожен OSINT аналітик в процесі проведення розслідування.

Власне, питання безпеки в мережі не є новим та досліджується досить давно. Більше того, існує навіть спеціальний термін — OPSEC (Operational

---

1 ChatGPT for OSINT? Integrating AI Chatbots in the Open Source Intelligence Cycle. Intelligence Fusion : website. URL: https://www.intelligencefusion.co.uk/insights/resources/article/chatgpt-for-osint-integrating-ai-chatbots-in-the-open-source-intelligence-cycle/

2 ChatGPT for OSINT: tips, precautions and ethical considerations. Autentic8 : website. URL: https://www.authentic8.com/blog/chatgpt-for-osint

Security — оперативна безпека), який можна визначити як набір принципів та методів, які використовуються для захисту конфіденційної інформації та забезпечення безпеки операцій. OPSEC в основному застосовувався у військових та розвідувальних сферах, проте з часом поширився на корпоративну безпеку та особисту конфіденційність. OPSEC було розроблено як системний процес виявлення та мінімізації вразливостей, які можуть ставити під загрозу операційну безпеку.

Принципи OPSEC включають аналіз загроз і вразливостей, оцінку ризиків і впровадження контрзаходів для захисту інформації та операцій. OPSEC наголошує на необхідності розуміти потенційних противників та контролювати розкриття конфіденційної інформації. Загалом, OPSEC — це проактивний і комплексний підхід до захисту інформації та операцій шляхом зменшення вразливості та запобігання збору важливої інформації небажаними особами. Підтримка OPSEC під час OSINT розслідувань має вирішальне значення для захисту особи та забезпечення цілісності розслідування. Під час проведення OSINT розслідування є кілька факторів, які слід враховувати для забезпечення оперативної безпеки.

1. Інструменти.

Беручи участь в OSINT розслідуваннях, дуже важливо ретельно враховувати потенційні ризики, пов'язані з інструментами, які використовує аналітик. Деякі інструменти, як, наприклад, програми для автоматичного збору інформації, можуть ненавмисно привернути увагу та поставити під загрозу конфіденційність аналітика. Щоб мінімізувати такі ризики, вкрай важливо діяти так, щоб це було схожим на поведінку звичайного користувача, щоб не викликати підозр.

Щоб гарантувати належний рівень безпеки, бажано обирати інструменти з надійного та перевіреного джерела. Таким чином, аналітик може бути впевнений у надійності та безпеці цих інструментів. Важливо оцінити потенційні ризики, пов'язані з кожним інструментом, гарантуючи, що вони не призведуть до витоку конфіденційної інформації. При виборі правильних інструментів необхідно віддавати перевагу обережності. Мета аналітика полягає в тому, щоб бездоганно злитися з переважною більшістю користувачів інтернету. Використовуючи інструменти, які відповідають цьому рівню

анонімності, можна уникнути привертання непотрібної уваги з боку суб'єкта, за яким ведеться розслідування. Проте необхідно зазначити, що інколи це може бути спеціальним тактичним ходом — використовувати більш доступні інструменти, щоб повідомити суб'єкту, що за ним відбувається спостереження.

2. Джерела.

Окрім аналізу інструментів, які використовує аналітик, не менш важливим є вибір джерела, на які буде покладатися аналітик під час OSINT розслідувань, та визначення рівня їньої видимості. Різні джерела представляють різні ступені ризику. Так, деякі джерела можуть становити мінімальний ризик, тоді інші можуть належати уявному противнику або контролюватися ними, потенційно викриваючи діяльність OSINT аналітика. Необхідно уважно вивчити наслідки доступу до джерела та взаємодії з ними. Слід визначити, чи може джерело викликати підозру и привертати увагу до OSINT розслідування. Перш ніж звертатися до джерела, аналітик повинен продумати, в який спосіб він може менше привертати до себе уваги. Можливо, є сенс змінити налаштування мови на сайті або часовий пояс, щоб «злитися» з іншими відвідувачами цільового вебсайту.

Також якщо відбувається розслідування відносно особи, то аналітик повинен чітко визначити години своєї присутності в інтернеті. Якщо особа, яка цікавить аналітика, працює в межах певного періоду часу, то аналітик повинен підлаштувати своє розслідування під ці години. Щоб ще більше покращити OPSEC, доцільно використовувати окремий комп'ютер для проведення лише OSINT розслідувань. Використовуючи окремий комп'ютер, аналітик мінімізує ризик витоку персональних даних, які можуть бути на його особистому комп'ютері.

3. Комп'ютер для OSINT розслідувань.

Коли мова стоїть щодо вибору пристрою для проведення розслідувань, то необхідно враховувати низку факторів, насамперед — бюджет. Очевидно, що бюджет завжди буде обмежений, проте навіть невеликих коштів може бути достатньо для того, щоб підвищити рівень OPSEC. Аналітик має подбати про те, щоб видалити чи повністю відключити вбудовані мікрофони та вебкамери, оскільки ці пристрої потенційно можуть бути використані зловмисниками, щоб отримати

несанкціонований доступ до комп'ютера аналітика. Окрім фізичного удосконалення комп'ютера, також необхідно враховувати і вдосконалення програмного забезпечення, тому доцільно встановити програми, які блокують несанкціонований доступ до камери та мікрофону.

Для додаткового захисту своєї діяльності в інтернеті доцільно розглянути можливість використання проксі-серверів або VPN (Virtual Private Networks — віртуальних приватних мереж), щоб замаскувати IP-адресу комп'ютера та країну, з якої аналітик отримуєте доступ до інтернету. Це допомагає захистити анонімність та створює додатковий бар'єр для потенційних загроз. Іншим важливим фактором є блокування файлів cookie, за допомогою яких вивчається поведінка користувача в інтернеті, що може скомпроментувати OSINT розслідування. Необхідно налаштувати веббраузер таким чином, щоб він блокував або обмежував використання файлів cookie. Завдяки цьому можна підвищити свій рівень конфіденційності в мережі Інтернет. Регулярне оновлення програмного забезпечення, за допомогою якого проводиться розслідування, дозволяє гарантувати кращий рівень захисту.

Якщо через бюджетні обмеження неможливо придбати окремий комп'ютер для проведення OSINT розслідування, то доцільно використовувати віртуальні машини (ВМ) в якості ефективної альтернативи. ВМ можна використовувати для імітації різних пристроїв та операційних систем. Наприклад, аналітик може запустити віртуальний смартфон чи планшет на своєму ноутбуці або поекспериментувати з різними операційними системами. Використовуючи ВМ, аналітик може суттєво розширити свої дослідницькі можливості без значних фінансових витрат[1].

Крім захисту фізичного, також необхідно пам'ятати про захист ментальний. OSINT аналітик, проводячи своє розслідування, може стикнутися з, наприклад, різними графічними матеріалами, які можуть мати травматичні наслідки для психіки аналітика. Тому аналітик вже на початку розслідування повинен розуміти, з якими даними він буде працювати та яку інформацію може знайти.

---

[1] Securing Your OSINT Investigations: Maintaining OPSEC for Effective Research. Medum : website. URL: https://medium.com/@alisagbiorczyk/securing-your-osint-investigations-maintaining-opsec-for-effective-research-f61b29cf2797

Іншим фактором запобігання таким негативним наслідкам є необхідність розуміння особистого зв'язку з роботою, яку проводить аналітик. Так, існує шість практик, які дозволяють мінімізувати такі негативні наслідки: обробка графічного вмісту; обмеження впливу графічного вмісту; проведення межі між особистим життям та розслідуванням; внесення позитиву в розслідування; навчання у більш досвідчених колег; та комбінація технік[1].

[1] Elise Baker, Eric Stover, Rohini Haar, Andrea Lampros, and Alexa Koenig. Safer Viewing: A Study of Secondary Trauma Mitigation Techniques in Open Source Investigations. Health and Human Rights Journal. June 2020. Volume 22. Number 1. P. 293–304.

Тема 4

ОСОБЛИВОСТІ ДОКАЗУВАННЯ У КРИМІНАЛЬНОМУ ПРОЦЕСІ ЗА ДОПОМОГОЮ ЕЛЕКТРОННИХ ДОКАЗІВ

4.1 ПОНЯТТЯ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОЦЕСІ

Під час OSINT розслідувань докази збираються з відкритих джерел, і майже завжди такі відкриті джерела знаходяться в мережі Інтернет. Таким чином, виникає цілком логічне питання щодо «легалізації» доказів, отриманих в результаті проведення OSINT розслідування в кримінальному процесі, адже будь-яке кримінальне провадження повинно відбуватися в порядку, передбаченому кримінальним процесуальним законодавством, а способи збирання та закріплення доказів мають чітко відповідати тим вимогам, які встановив законодавець. Можна провести дуже ефективне OSINT розслідування, знайти інформацію, яка підтверджує факт кримінального правопорушення, проте допустити помилки при «введенні» таких даних в кримінальний процес, що зведе нанівець всі зусилля OSINT аналітика. Для того щоб фактичні дані в подальшому могли використовуватися у кримінальному провадженні як докази, вони мають отримуватися в передбаченому процесуальним законом порядку, у протилежному випадку вони будуть визнаватися очевидно недопустимими доказами[1].

[1] Про деякі питання порядку здійснення судового розгляду в судовому провадженні у першій інстанції відповідно до Кримінального процесуального кодексу України: Інформаційний лист Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ від 5 жовт. 2012 р. URL: http://zakon2.rada.gov.ua/laws/show/v1446740–12

На даний момент у кримінальному процесуальному законодавстві відсутнє легальне визначення електронних доказів. Законодавець обмежується лише загальним визначенням, відповідно до якого доказами є фактичні дані, отримані у передбаченому КПК України порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню (ч. 1 ст. 84 КПК України). Відповідно до ч. 2 ст. 84 КПК України процесуальними джерелами доказів є показання, речові докази, документи та висновки експертів (також існують додаткові джерела доказів при розслідуванні кримінальних проступків, проте серед них також немає жодної вказівки на електронні докази). Таким чином, законодавець фактично ігнорує електронні докази як окремий вид, хоча в інших галузях права ситуація з нормативним регулюванням є значно кращою.

Так, відповідно до ст. 100 ЦПК України, електронними доказами є інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи, зокрема, електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), вебсайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі. Такі дані можуть зберігатися, зокрема, на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (в тому числі в мережі Інтернет). Електронні докази подаються в оригіналі або в електронній копії, на яку накладено кваліфікований електронний підпис відповідно до вимог законів України «Про електронні документи та електронний документообіг» та «Про електронну ідентифікацію та електронні довірчі послуги». Законом може бути передбачено інший порядок засвідчення електронної копії електронного доказу.

Подібні положення присутні і в інших процесуальних кодексах, таких як ГПК та КАС. Проте в КПК України всі вказівки про електронні докази фактично зводяться до ст. 99 КПК України, де зазначено, що одним з джерел доказів є документ, тобто спеціально створений з метою збереження інформації матеріальний об'єкт, який містить зафіксовані

за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження. До документів, крім інших, можуть відноситись матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі комп'ютерні дані). Власне, п. 1 ч. 2 ст. 99 КПК України і є найближчим формулюванням електронних доказів, яке надано в кримінальному процесуальному законодавстві. Власне в науці також існує позиція, що «якщо електронний документ, який був знаряддям вчинення кримінального правопорушення, зберіг на собі його сліди, або був об'єктом кримінально-протиправних дій, то у таких випадках він буде речовим доказом. Для такого різновиду речових доказів важливу роль відіграє матеріальний носій електронного документа, а інформація, яка на ньому міститься, нерозривно з ним пов'язана»[1]. В якості однієї з підстав розмежування речових доказів і документів, коли мова йде про електронні документи, пропонується звертати увагу на те, що саме може бути використане як доказ факту чи обставин, що встановлюються під час кримінального провадження: інформація чи фізичний носій інформації[2]. З урахуванням того, що при OSINT розслідуванні найчастіше використовується інформація, отримана з мережі Інтернет, у кримінальному провадженні вона буде підпадати саме під категорію «документ». Також «важливе значення має розмежування за тим, що саме має доказове значення: зміст чи форма. Якщо доказове значення має інформація, яка збережена в електронній формі, то це електронний документ. Наприклад, електронний лист на поштовій скриньці, отриманий через мережу Інтернет з інформацією, яка має значення для кримінального провадження. Комп'ютерна програма, збережена на носії інформації, за допомогою якої відбулося несанкціоноване втручання в роботу комп'ютера буде речовим доказом. Носій інформації без вищевказаної комп'ютерної програми на ньому не має жодного доказового значення»[3].

---

1 Ратнова А.В. Кримінальні процесуальні та криміналістичні основи використання електронних документів в доказуванні : дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 081 «Право». Львів, 2021. 248 с.

2 Там само.

3 Там само.

Власне, також існує позиція, що цифрова доказова інформація має отримуватися з окремо закріпленого процесуального джерела — носія цифрового доказу, яким буде відповідний файл. Носій же цифрових даних, з яких така інформація утворюється, фактично буде носієм цифрового доказу[1].

Також необхідно зауважити, що в абз. 2 ч. 2 ст. 237 КПК України законодавець несподівано вводить додатковий термін «комп'ютерні дані», коли описує специфіку огляду даних, які зберігаються на електронних обчислювальних машинах. Власне, даний термін з'явився в КПК України відповідно до ЗУ «Про внесення змін до Кримінального процесуального кодексу України та Закону України "Про електронні комунікації" щодо підвищення ефективності досудового розслідування "за гарячими слідами" та протидії кібератакам», який, відповідно до пояснювальної записки, було прийнято через те, що «в КПК України досі не імплементовано жодного із спеціально передбачених у Конвенції про кіберзлочинність тимчасових заходів, спрямованих на ефективну міжнародну співпрацю щодо протидії кіберзлочинності». Проблема в даному випадку полягає насамперед в тому, що в самому КПК України не надається визначення «комп'ютерних даних», як не надається таке визначення в ЗУ «Про електронні комунікації». У Конвенції про кіберзлочинність зазначено, що комп'ютерні дані — це «будь-яке представлення фактів, інформації або концепцій у формі, яка є придатною для обробки у комп'ютерній системі, включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп'ютерною системою». Можна було б стверджувати, що найбільш доцільним у даному випадку буде використання терміна «комп'ютерні дані» як такого, що використовується законодавцем у КПК України, проте все одно більш доцільним є використання терміна «електронні докази». По-перше, цей термін є загальновживаним у зарубіжній науковій літературі та законодавстві, що робить його міжнародно визнаним та універсальним. Відповідно, його використання значно полегшить роботу з іноземними науковими та нормативними джерелами. По-друге, термін «електронні докази»

[1] Скрипник А.В. Використання цифрової інформації в кримінальному процесуальному доказуванні : монографія. Харків : Право, 2022. 408 с.

вже вказує, що такі відомості мають властивості доказів, тобто є належними, допустимими, достовірними. Комп'ютерні ж дані лише вказують на специфіку форми самої інформації, місце її зберігання та особливості отримання. Відповідно, комп'ютерні дані стануть електронними доказами після їхньої оцінки, як це відбувається і з іншими доказами.

Взагалі, використовуючи термін «електронні докази», необхідно зазначити, що досить часто в якості синоніма також використовується поняття «цифрові докази». Так як кримінальним процесуальним законодавством дана термінологія не регулюється, ці терміни можна використовувати як синоніми. Проте більш популярним є саме термін «електронні докази», про що свідчить і аналіз судової практики, і приклади з інших процесуальних галузей права, тому в даному випадку використовуватися буде саме він.

Таким чином, електронні докази визначають «як докази у кримінальних провадженнях, які можна отримати в електронній формі. Електронні докази отримують за допомогою електронних пристроїв, комп'ютерних носіїв інформації, а також комп'ютерних мереж, у тому числі через мережу Інтернет. Вони стають доступними для сприйняття людиною після обробки засобами комп'ютерної техніки»[1]. Також їх можна визначити як «інформація, що зберігається в електронному вигляді на будь-яких типах електронних носіїв, в електронних пристроях чи електронних інформаційних системах та відповідає вимогам ст. 84 КПК»[2] або «дані, які підтверджують факти, інформацію або концепцію у формі, придатній для обробки за допомогою комп'ютерних систем, у тому числі програми виконання комп'ютерною системою або інших дій»[3].

Рада Європи визначає електронні докази як будь-які докази, отримані з даних, що містяться на будь-якому пристрої або вироблені ним, функціонування якого залежить від програмного забезпечення або

---

1 Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. реком. / М.В. Гуцалюк, В.Д. Гавловський, В.Г. Хахановський та ін. ; за заг. ред. О.В. Корнейка. Вид. 2-ге, доп. Київ : Вид-во Нац. акад. внутр. справ, 2020. 104 с.

2 Доказування у кримінальному провадженні : навч.-практ. посібн. / кол. авт. К. : Національна академія прокуратури України, 2017. 346 с.

3 Ахтирська Н.М. До питання доказової сили кіберінформації в аспекті міжнародного співробітництва під час кримінального провадження. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2016. Вип. 36(2). С. 123–125.

даних, що зберігаються або передаються через комп'ютерну систему чи мережу[1].

Виділяють такі ознаки електронних доказів: «існують у нематеріальному вигляді; можуть бути створені людиною або бути результатом діяльності інформаційної системи; не можуть існувати поза межами технічного носія або каналу зв'язку; немає нерозривного зв'язку з предметним носієм; вільно переміщуються в електронній мережі; сприймати та досліджувати їх можна тільки за допомогою технічних і програмного забезпечення; потребують спеціального порядку збирання, перевірки, оцінки; можуть бути переміщені на інший носій без втрати своїх характеристик; можливість дистанційного внесення змін до них та їх видалення»[2].

Електронні докази мають спільні риси з традиційними доказами, але водночас мають низку унікальних характеристик: 1) їх не видно неозброєним оком: вилучити їх подекуди може лише спеціаліст; 2) вони є нестійкими, за певних обставин інформація в пам'яті пристрою може бути змінена або втрачена. Наприклад, у разі розрядки пристрою або недостатності пам'яті система накладає (записує) нову інформацію замість попередньої, а це значить, що й докази можуть бути знищені. Комп'ютерна пам'ять може бути пошкоджена або знищена під впливом фізичних факторів (високий рівень вологості, висока температура) та електромагнітних хвиль; 3) їх можна копіювати без втрати якості необмежену кількість разів, і будь-яка наступна копія не буде відрізнятися від оригіналу[3]; 4) можуть як бути створені людиною, так і бути результатом функціонування інформаційної системи; 5) вільно переміщуються в електронній мережі без технічного носія та не мають нерозривного зв'язку з матеріальним носієм; 6) потребують специфічного порядку збирання, перевірки й оцінки[4].

---

1 Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings. Council of Europe : website. URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680902e0c

2 Дегтярьова О. Доказування в кримінальному провадженні на підставі електронних доказів. *Юридичний вісник*. 2021. № 5. С. 273–278.

3 Ахтирська Н.М. До питання доказової сили кіберінформації в аспекті міжнародного співробітництва під час кримінального провадження. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2016. Вип. 36. Т. 2. С. 123–125.

4 Алєксєєва-Процюк Д.О., Брисковська О.М. Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти застосування. *Науковий вісник публічного та приватного права*. 2018. Вип. 2. С. 247–253.

Під час роботи з електронними доказами спеціалісти рекомендують дотримуватися таких принципів:

1. Законність. Працівники та підрозділи, що провадять розслідування і досліджують докази в електронній формі, зобов'язані дотримуватися чинного законодавства, загальних процесуальних та криміналістичних принципів.

2. Цілісність даних. Дії фахівця не повинні призводити до матеріальних змін даних, електронних пристроїв чи носіїв інформації, які можуть використовуватись як докази.

3. Документування процесу. Документують будь-які дії, виконувані стосовно електронних доказів, і зберігають ці документи на випадок перевірки, щоб незалежна третя сторона могла повторити ці дії та отримати аналогічний результат.

4. Експертна підтримка. Якщо передбачається, що при огляді (обшуку) можуть бути виявлені електронні докази, отримують підтримку фахівців (спеціалістів), забезпечивши, за можливості, їхню присутність на місці події.

5. Відповідна фахова підготовка. Якщо при огляді (обшуку) відсутні фахівці з електронних доказів, першочергові дії на місці події здійснюють особи, які мають необхідні знання та навички для виявлення і збирання доказів.

6. Розумна обережність. Уникають будь-яких навмисних або ненавмисних дій, які можуть призвести до пошкодження потенційних доказів, представлених у цифровій формі[1].

4.2 НАЛЕЖНІСТЬ ТА ДОПУСТИМІСТЬ ЕЛЕКТРОННИХ ДОКАЗІВ

Будь-який доказ, який використовується в кримінальному провадженні, має бути належним та допустимим. З урахуванням того, що законодавець не надає жодних спеціальних уточнень щодо порядку використання електронних доказів, можна зробити однозначний висновок, що такі саме умови ставляться і до них.

---

[1] Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. реком. / М.В. Гуцалюк, В.Д. Гавловський, В.Г. Хахановський та ін.; за заг. ред. О.В. Корнейка. Вид. 2-ге, доп. Київ : Вид-во Нац. акад. внутр. справ, 2020. 104 с.

Насамперед електронні докази мають оцінюватися з точки зору належності. Загалом, значних уточнень щодо оцінки належності доказів, отриманих за допомогою OSINT розслідування, немає. У будь-якому випадку має визначатися зв'язок конкретного доказу з обставиною, яку він буде доводити та яка включається в предмет доказування. «З аналізу судових вироків можна зробити висновок, що прямими доказами у кримінальних провадженнях, пов'язаних з незаконним поширенням наркотиків, можуть бути: листування в соціальній мережі «Telegram» щодо замовлення наркотичних засобів, психотропних речовин і прекурсорів, замовлення наркотичних засобів, психотропних речовин і прекурсорів через інтернет-магазин, отримання інформації про «закладку» (схованку) — адреса, фото місця та координати, опис тощо, отримання фото квитанції відправлення через «Нову пошту» [66], збут наркотичних засобів, психотропних речовин і прекурсорів через соціальну мережу «Telegram», надсилання інформації про «закладку» (схованку) — адреса, фото місця, координати, опис тощо[1]».

Очевидно, що на момент проведення досудового розслідування та збирання таких доказів лише слідчий, дізнавач та прокурор можуть оцінити належність доказів та їхній зв'язок з кримінальним провадженням, проте в подальшому це може бути предметом дослідження судом, тому сторона обвинувачення повинна мати аргументи, які б реально доводили належність доказів, отриманих в результаті проведеного OSINT розслідування.

У даному випадку більш проблемним є доведення перед стороною захисту не належності доказу, який прямо чи опосередковано доводить чи спростовує обставини, що включаються в предмет доказування, а доведення того, яким чином такі докази були отримані. Тобто мова йде про встановлення всього ланцюга доказів, в результаті яких і була отримана інформація, яка має значення для кримінального провадження. У судовій практиці можна помітити такі формулювання, як «було проведено аналітичне дослідження відкритих джерел інформації

[1] Ратнова А.В. Електронні документи як докази під час розслідування злочинів, пов'язаних з незаконним обігом наркотиків. *Процесуальне та криміналістичне забезпечення досудового розслідування* : тези доповідей учасників науково-практичного семінару (30 жовт. 2020 р.) / упор. А.Я. Хитра. Львів : ЛьвДУВС. 2020. С. 81–83.

методами OSINT»[1] або «було здійснено пошук на основі відкритих джерел (OSINT)»[2]. У даному випадку описуються лише способи збирання доказів, проте у сторони захисту може виникнути цілком логічне питання: «а на підставі яких саме доказів слідством було отримано відомості, які вказують на винуватість обвинуваченого?». Як вже було встановлено і неодноразово наголошено, OSINT — це складний багатоетапний процес, а пошук доказів, які доводять причетність особи до вчиненого кримінального правопорушення, може вимагати від OSINT аналітика вивчення великої кількості даних та формування дуже довгого ланцюга інформації, в результаті якого і будуть отримані докази, які включаються в предмет доказування. У той же час сторона захисту має право бути обізнаною, на підставі яких саме доказів були отримані ті докази, які будуть покладені в основу обвинувачення. Більше того, використовуючи теорію плодів отруєного дерева, сторона захисту може спробувати в подальшому визнати такі докази недопустимими саме через порушення процедури збирання проміжних доказів. Повторюємося, що фактично весь процес OSINT розслідування і передбачає створення ланцюга з інформації, тобто збирання проміжних доказів, які в подальшому дозволять отримати саме ті відомості, які вже напряму будуть стосуватися предмета доказування. З цього можна зробити висновок, що такі проміжні докази також слід вважати належними, адже саме на їхній підставі будуть отримані докази, які дозволяють встановити кінцевий предмет доказування. Уповноважена посадова особа правоохоронного органу повинна бути готова надати всі такі докази на підтвердження того, що OSINT розслідування було проведено законно, а відомості, на яких ґрунтується обвинувачення, були отримані лише з відкритих джерел. Проте така позиція на даний момент також піддається обґрунтованій критиці насамперед у судовій практиці, де досить часто дані, отримані за допомогою OSINT методів, фактично прирівнюються до даних, отриманих оперативним шляхом в тому аспекті, що конкретне джерело їхнього отримання залишається невстановленим.

---

[1] Ухвала слідчого судді Комунарського районного суду міста Запоріжжя від 01.06.2022 року, справа № 333/1938/22. URL: https://reyestr.court.gov.ua/Review/104556752

[2] Ухвала слідчого судді Святошинського районного суду м. Києва від 31.07.2019 року, справа № 759/13808/19. URL: https://reyestr.court.gov.ua/Review/83480188

Тому хоча слідчий, прокурор або інша уповноважена особа повинна бути готова пояснити в суді весь ланцюг отримання таких відомостей, самі судді в силу відносної новизни такого способу отримання інформації задовольняються лише загальними формулюваннями «шляхом проведення OSINT розслідування» чи будь-якого подібного.

Відповідно до ст. 86 КПК України, доказ визнається допустимим у тому випадку, якщо його було отримано у спосіб, передбачений КПК України. Жодних додаткових уточнень щодо специфіки оцінки допустимості електронних доказів КПК не містить, що означає, що необхідно використовувати відносно стандарті критерії оцінки допустимості доказів — належне джерело, належний суб'єкт, належний спосіб збирання та закріплення. Як вже було зазначено, при проведенні OSINT розслідувань переважна більшість доказів буде відповідати такому джерелу, як документи (ст. 99 КПК України), тому оцінка доказів має відбуватися саме як для документів.

І вже при визначенні належного джерела доказу можуть виникнути проблеми, адже основним джерелом інформації для OSINT аналітиків є мережа Інтернет. Очевидно, що сам по собі інтернет не є джерелом, адже будь-яка інформація зберігається на серверах, які і є джерелом відповідної інформації. Відповідно, можна дійти висновку, що будь-яка інформація, отримана з мережі Інтернет, може бути визнана недопустимим доказом, адже слідство вилучало її не з конкретного сервера (що, як правило, або складно, або навіть неможливо). «У такому випадку огляд облікового запису, відеозапису, вебсайту, без вилучення інформації з сервера може бути визнаний недопустимим доказом»[1]. Проте такий висновок видається дещо передчасним.

Специфіка інформації в мережі Інтернет полягає в тому, що її сутність та зміст не буде змінюватися від зміни сервера, на якому знаходиться сама інформація. Інколи в кримінальному провадженні більше значення має сам сайт, де була розміщена інформація (наприклад, загальнодоступна соціальна мережа або закритий форум), ніж фактичне місцезнаходження сервера, яке ніяким чином не впливає на саме кримінальне

[1] Ратнова А.В. Кримінальні процесуальні та криміналістичні основи використання електронних документів в доказуванні : дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 081 «Право». Львів, 2021. 248 с.

правопорушення. Також не можна ототожнювати електронний доказ як засіб доказування та матеріальний носій такого документа, «оскільки характерною рисою електронного документа є відсутність жорсткої прив'язки до конкретного матеріального носія»[1]. Об'єднана палата ВС зазначила, що «для виконання завдань кримінального провадження, з огляду на положення Закону України «Про електронні документи та електронний документообіг», допустимість електронного документа як доказу не можна заперечувати виняткова на підставі того, що він має електронну форму (ч. 2 ст. 8). Відповідно до ст. 7 цього Закону у випадку його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа. Один і той самий електронний документ може існувати на різних носіях. Усі ідентичні за своїм змістом екземпляри електронного документа можуть розглядатися як оригінали та відрізнятися один від одного тільки часом і датою створення. Питання ідентифікації електронного документа до оригіналу можуть бути вирішені уповноваженою особою, яка його створила (за допомогою спеціальних програм порахувати контрольну суму файлу або каталогу з файлами CRC-сума, hash-сума), або за наявності відповідних підстав шляхом проведення спеціальних досліджень»[2].

Загалом вимога щодо належного джерела насамперед стосується «типових» доказів, а не електронних. Дана вимога повинна, крім іншого, забезпечити достовірність доказу та можливість його подальшої перевірки шляхом аналізу самого джерела. Електронні докази, очевидно, працюють дещо за іншими принципами, тому і вимоги оцінки належності джерела мають бути іншими. Як було зазначено, неправильно здійснювати жорстку прив'язку до матеріального носія інформації, коли ведеться мова про електронні документи. До того ж в мережі Інтернет поняття «джерело» є вкрай відносним, адже особа, яка створює онлайн-контент, який в подальшому може бути використаний як доказ, не знає про те, на якому сервері буде розміщена така інформація, адже її більше цікавить сам сайт, ніж сервер. У зв'язку з цим можна дійти висновку, що при оцінці належного джерела електронних доказів,

---

[1] Постанова ККС ВС від 29.03.2021, справа № 554/5090/16-к. URL: https://reyestr.court.gov.ua/Review/96074938

[2] Там само.

отриманих за допомогою OSINT методів, немає підстав робити жорстку прив'язку до належного джерела, як це на противагу відбувається з «типовими» доказами.

Також в якості критеріїв оцінки допустимості доказів необхідно звернути увагу на належного суб'єкта збирання (належний спосіб збирання та фіксації електронних доказів буде досліджено окремо в цій темі). З аналізу судової практики можна дійти висновку, що найбільш популярним способом збирання електронних доказів є проведення огляду вебсайтів (про що детальніше буде написано нижче). У той же час необхідно пам'ятати, що огляд (в тому числі і контенту в мережі Інтернет) є слідчою дією, а тому має проводитися в порядку, передбаченому КПК України. Так, відповідно до ч. 1 ст. 237 КПК України, з метою виявлення та фіксації відомостей щодо обставин вчинення кримінального правопорушення слідчий, прокурор проводять огляд місцевості, приміщення, речей, документів та комп'ютерних даних. Законодавець в абз. 2 ч. 2 ст. 237 КПК України окремо передбачив специфіку огляду комп'ютерних даних, відповідно до якої огляд комп'ютерних даних проводиться слідчим, прокурором шляхом відображення у протоколі огляду інформації, яку вони містять, у формі, придатній для сприйняття їхнього змісту (за допомогою електронних засобів, фотозйомки, відеозапису, зйомки та/або відеозапису екрана тощо або у паперовій формі). Таким чином, слід звернути увагу на те, що законодавець встановив чіткий перелік суб'єктів, які можуть здійснювати огляд комп'ютерних даних — слідчий та прокурор. Насамперед звертаємо увагу, що в даному переліку відсутній дізнавач. Якщо проаналізувати КПК України, то для законодавця це відносно стала практика — не дописувати дізнавача в статті, в яких він, відповідно до його статусу, має бути. У деяких випадках така відсутність має принципове значення. Так, відповідно до ч. 1 ст. 236 КПК України, ухвала про дозвіл на обшук житла чи іншого володіння особи може бути виконана слідчим чи прокурором. Здійснюючи тлумачення даного положення, ВС дійшов досить чіткого висновку, що жодні додаткові особи (в даному випадку — на прикладі оперативних працівників) не можуть проводити обшук. Відповідно, аналогічне тлумачення можна спробувати застосувати і по відношенню до абз. 2 ч. 2 ст. 237 КПК України, тобто що всі електронні докази (в тому

числі проміжні) мають бути отримані під час огляду виключно слідчим або прокурором, проведення таких дій іншими особами (на практиці найчастіше це оперативні працівники) не допускається. На даний момент суди на аргументи про те, що протоколи оглядів «складені оперуповноваженим і сам огляд проводився оперуповноваженим, який відповідно до ст. 237 КПК України не мав на те законних підстав, оскільки такий огляд проводиться лише слідчим або прокурором і будь-яких винятків дана стаття не містить», дотримуються позиції, що «підстав для визнання доказів недопустимими не установлено, оскільки не було з'ясовано факту істотних фундаментальних порушень прав і свобод учасників провадження, регламентованих ст. 87 КПК України»[1].

Загалом необхідно зазначити, що чинний КПК України потребує вдосконалення, адже якщо вести мову про OSINT розслідування, то дані з відкритих джерел будуть збиратися або оперативними працівниками, або аналітиками, які не є представниками правоохоронних органів. Якщо ж підтримувати позицію про те, що проміжні докази також включаються в предмет доказування, то сторона обвинувачення повинна бути в змозі продемонструвати весь шлях, який було пройдено для того, щоб отримати докази, які можуть бути покладені в основу обвинувачення. Жорстка ж прив'язка до нормативних вимог у даному випадку повністю суперечить логіці самого OSINT розслідування, адже всі відомості збираються з відкритих джерел, а тому такі дії не потребують будь-якого санкціонування чи наявності в особи, яка проводить таке розслідування, спеціального статусу. У даному випадку набагато важливішим для суду буде питання не суб'єкта, який отримав проміжні електронні докази, а питання щодо їхньої достовірності.

4.3 ДОСТОВІРНІСТЬ ЕЛЕКТРОННИХ ДОКАЗІВ

Встановлення достовірності існування фактів, яким надається значення доказів, — один з найголовніших елементів дослідження доказів.

[1] Вирок Вінницького міського суду Вінницької області від 20.09.2023, справа № 127/26784/22. URL: https://reyestr.court.gov.ua/Review/113809731

Науковці зазначають, що достовірність доказів є правильністю відображення в них фактів об'єктивної дійсності, яка є предметом досудового розслідування або судового розгляду. Іншими словами — це відповідність доказу дійсності[1]. «Достовірність доказу в кримінальному провадженні є його ознакою, яка характеризується повною відповідністю одержаних відомостей про факти реальним подіям, що відбувалися. Достовірність як ознака доказів виникає, встановлюється та існує в межах системи доказів. Визначення доказу як достовірного відбувається в результаті оцінки доказу для виявлення внутрішніх суперечностей (наприклад, в обстановці на місці події немає слідів, які мали б залишитися під час учинення кримінального правопорушення певним способом, особа під час допиту змінює свої показання стосовно тих чи інших обставин, які є предметом допиту) та супутніх їх одержанню проявів в актах поведінки та показаннях осіб дисимуляції (утаювання чогось), які спостерігаються в ході процесуальних дій як такі, що не узгоджуються із встановленими фактичними даними про конкретну подію і потребують дослідження з метою встановлення їх походження та суті виявлених неузгодженостей; та зовнішніх суперечностей, тобто неузгодженостей з іншими доказами, зібраними у провадженні. Така оцінка кожного доказу повинна розпочинатися з аналізу для виявлення внутрішніх, а далі зовнішніх суперечностей. У випадку виявлення суперечностей не слід автоматично визнавати відомості як недостовірні. Природа (тобто чи є такі дані результатом протидії кримінальному провадженню або ж помилки) та зміст виявлених суперечностей підлягають обов'язковому з'ясуванню й оцінці щодо їх впливу на систему зібраних доказів у кримінальному провадженні»[2].

Існує безліч проблем при оцінці достовірності електронних доказів. По-перше, електронними доказами досить легко маніпулювати та вносити в них зміни. Такі маніпуляції можуть вплинути на всі електронні докази, надані суду, що зменшує їхню надійність. Також можуть

---

1 Докази і доказування. Кримінальний процес : підручник / за ред. В.Я. Тація, Ю.М. Грошевого, О.В. Капліної, О.Г. Шило. Х. : Право, 2013. 824 с.

2 Ратнова А.В. Кримінальні процесуальні та криміналістичні основи використання електронних документів в доказуванні : дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 081 «Право». Львів, 2021. 248 с.

бути технічні помилки під час отримання електронних доказів, які хоча і є відносно рідкісними, проте вони теж послаблюють сприйняття їхньої автентичності. Відповідно, недостовірність електронних доказів може поставити під сумнів законність самого судового рішення. Іншою проблемою також є використання невідповідних інструментів (програм з неправильною специфікацією, з помилками в коді тощо) для доступу та збереження електронних доказів[1].

Оцінка достовірності електронного доказу може відбуватися стандартним способом, тобто шляхом порівняння електронного доказу з іншими, які наявні в кримінальному провадженні. Проте достовірність електронних доказів також має перевірятися у специфічні способи, такі як перевірка контрольної суми (хеш-суми). Контрольна сума — певне значення, обчислене на основі набору даних із застосуванням одного із математичних (криптографічних) алгоритмів (наприклад, CRC32, MD5, SHA-1, SHA-2, SHA-3 або ін.), які використовуються для перевірки цілісності даних при їхній передачі або збереженні. При щонайменшій зміні файлу відразу змінюється і хеш-сума цього файлу. За допомогою такої перевірки забезпечується захист конкретного файлу від зміни.

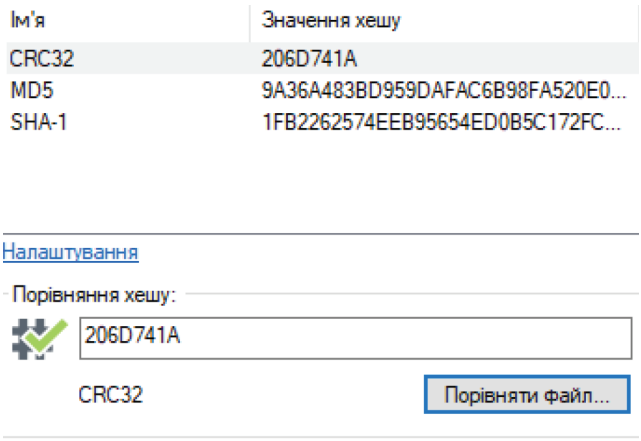
Для прикладу можна взяти довільно створений Word файл, в якому понад 18 тисяч символів. За допомогою програмного забезпечення (вбудованого або зовнішнього, наприклад, відносною популярністю користується безкоштовна програма HashTab) можна переглянути значення хешу файлу, який цікавить OSINT аналітика (CRC32, MD5, SHA-1 тощо — це алгоритми створення хеш-суми. Майже в кожному алгоритмі є свої вразливості, тому доцільно переглядати одразу декілька хеш-сум, як на малюнку) (мал. 4.1).

Ім'я	Значення хешу
CRC32	206D741A
MD5	9A36A483BD959DAFAC6B98FA520E0...
SHA-1	1FB2262574EEB95654ED0B5C172FC...

Мал. 4.1. Приклад хеш-суми файлу документа

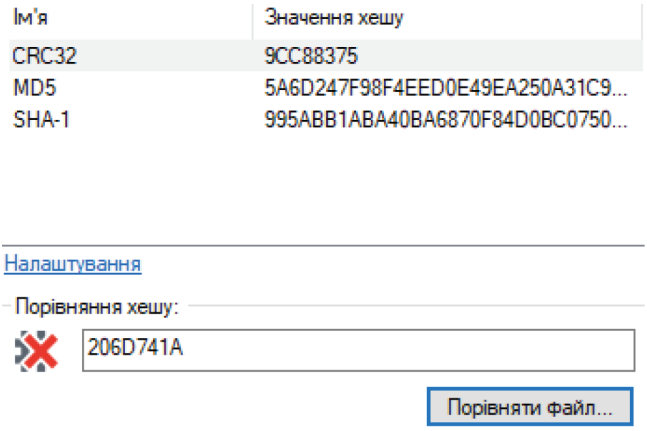
[1] Moussa, A.F. Electronic evidence and its authenticity in forensic evidence. Egypt J Forensic Sci 11, 20 (2021).

Якщо створити копію цього файлу та порівняти хеш-суми, то вони будуть однакові (мал. 4.2).



Мал. 4.2. Порівняння хеш-суми копії файлу документа

Проте якщо в копії файлу змінити хоча б один символ, то жодна з трьох хеш-сум збігатися не буде (мал. 4.3).



Мал. 4.3. Приклад хеш-суми копії файлу документа,
в якому було змінено один символ

Для мінімізації ризику впливу зловмисників на хеш-суму бажано перевіряти цей показник одразу за декількома алгоритмами, кожен з яких повинен збігатися. Однак використання криптографії для автентифікації цифрових доказів також не є статичним завданням, оскільки галузеві стандарти автентифікації можуть швидко застаріти[1]. Наприклад, Міжнародний кримінальний суд на даний момент активно використовує алгоритм MD5, який на даний час вже може визначити як застарілий, про що неодноразово зазначають науковці[2].

Таким чином, використовуючи хеш-суми, можна гарантувати те, що в оригінальний файл не вносилися зміни, тобто його можна вважати повноцінним дублікатом. А відповідно до ч. 4 ст. 99 КПК України («дублікат документа (документ, виготовлений таким самим способом, як і його оригінал), а також копії інформації, **у тому числі комп'ютерних даних**, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа») та позиції Верховного Суду, яка була озвучена вище, можна дійти висновку, що будь-які копії електронних документів, в яких будуть збігатися хеш-суми, будуть визнаватися в якості оригіналів. При цьому перевірка хеш-сум не вимагає значних технічних вмінь та навичок, достатньо буде лише залучення спеціаліста при проведенні процесуальної дії під час досудового розслідування або судового розгляду, який зможе продемонструвати учасникам таких дій, що хеш-суми збігаються.

У зв'язку з цим уповноважена службова особа, яка проводить огляд комп'ютерних даних відповідно до ст. 237 КПК України з подальшим копіюванням таких даних на електронний носій (наприклад, CD-диск) обов'язково в протоколі такого огляду повинна зазначати хеш-суми файлу (файлів), які були скопійовані на такий носій, з якими в подальшому можна буде порівнювати цілісність копій таких файлів.

---

1 Moriarty, Kathleen. 2021. «Why Are Authentication and Authorization So Difficult?» Center for Internet Security. October 18, 2021.

2 Wang, Xiaoyun, and Hongbo Yu. 2005. «How to Break MD5 and Other Hash Functions». In Advances in Cryptology — EUROCRYPT 2005, edited by Ronald Cramer, 19–35. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer.

Аналізуючи оцінку достовірності електронних доказів в роботі Міжнародного кримінального суду, можна зробити висновок, що на даний момент існує два підходи щодо того, чи мають судді беззастережно приймати висновки експертів щодо таких (та й будь-яких інших) питань. Так, експерт з міжнародного права Юка Фукунага стверджує, що судді ніколи не повинні ухвалювати рішення, які стосуються науки[1]. Як вона справедливо зазначає, наукове дослідження ніколи не може відображати єдину об'єктивну істину. Хоча деякі галузі науки можуть мати загальний науковий консенсус, наукове дослідження за своєю природою є відкритим. На відміну від цього, міжнародне право спрямоване на пошук правди, яке вимагає суворого дотримання стандартів і процедур і, зрештою, остаточного рішення[2]. Враховуючи суперечливі ідеї між науковими дослідженнями та правовими стандартами, Фукунага пропонує застосовувати тест для перевірки узгодженості, об'єктивності та пропорційності методів наукової оцінки для відповідності стандарту доказу поза розумним сумнівом[3]. Заявляючи, що судді насамперед повинні вивчати докази, які надаються сторонами, а не ухвалювати рішення щодо окремої наукової істини, суд може зекономити багато часу, не досліджуючи питання, які не входять до компетенції суду та не можуть судом бути вирішені. Проте такий підхід не звільняє суд від обов'язку аргументації власного рішення на підставі конкретних наукових знань.

Протилежний підхід було розроблено юристом-міжнародником Керолайн Фостер. Вона стверджує, що судді повинні працювати з науковими концепціями, приймати наукову невизначеність і коригувати правила застосування тягаря доказування «поза розумним сумнівом» відповідно до наукової невизначеності. Такий підхід має очевидні переваги у підвищенні рівня грамотності суддів в основних аспектах науки чи техніки. Застосовуючи логіку Фостер до оцінки достовірності електронних доказів, науковці зазначають, що здатність суддів виносити

---

1 Boisson de Chazournes, Laurence. 2012. «Introduction: Courts and Tribunals and the Treatment of Scientific Issues». *Journal of International Dispute Settlement.* 3 (3): 479–81.

2 Wagner, Markus. 2011. «Law Talk v. Science Talk : The Languages of Law and Science in WTO Proceedings». *Fordham International Law Journal.* 35, no 1. 151–200.

3 Boisson de Chazournes, Laurence. 2012. «Introduction : Courts and Tribunals and the Treatment of Scientific Issues». *Journal of International Dispute Settlement.* 3 (3): 479–81.

рішення все більше залежатиме від їхньої здатності оцінювати технологічні та наукові досягнення, покращуватиме їхнє знайомство з цифровими доказами та покращуватиме розуміння нових джерел цифрової інформації[1].

Якщо судді будуть дотримуватися підходу Фукунаги, то основну роль при визначенні достовірності доказів відігравали би аргументи сторін, а не наукові позиції, які стосуються достовірності електронних доказів. Проте такий підхід створює ризики, що судді будуть ухвалювати рішення на добре обґрунтованих, послідовних та об'єктивних аргументах, які не мають достатнього наукового підґрунтя. Застосовуючи цю логіку до оцінки достовірності електронних доказів, судді можуть мимоволі верифікувати дані в повному відриві від оцінки технологічної складової. Підхід Фостер вимагає від суддів значно більш глибоких технічних знань при оцінці доказів. У той же час існує ризик, що судді будуть замість вивчення юридичної сторони доказу досліджувати його технологічну складову, що також має низку негативних аспектів[2]. Очевидно, що найкращим у даному випадку є об'єднання двох підходів та використання всього можливого спектра для оцінки допустимості доказів. Очевидно, що судді не можуть знати всіх технологічних аспектів вилучення, збереження та поширення комп'ютерних даних, тому стандартним буде залучення спеціалістів або проведення експертиз. У той же час самі судді також повинні розбиратися, про що саме буде йтися мова в таких висновках або як, наприклад, перевіряється хеш-сума. З огляду на популярність та поширеність електронних доказів судді повинні постійно оновлювати свої знання щодо електронних доказів, маючи як мінімум базові знання, які в даному випадку є необхідними при дослідженні електронних доказів.

---

1 Freeman, Lindsay, and Raquel Vazquez Llorente. 2021. «Finding the Signal in the Noise: International Criminal Evidence and Procedure in the Digital Age». *Journal of International Criminal Justice.* 19 (1): 163–88.

2 Chelsea Quilling. The Future of Digital Evidence Authentication at the International Criminal Court. The Journal of Public and International Affairs. URL: https://jpia.princeton.edu/news/future-digital-evidence-authentication-international-criminal-court

4.4 ОСОБЛИВОСТІ ЗБИРАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Як вже було зазначено, при оцінці допустимості електронних доказів також має вивчатися належний спосіб їхнього отримання та фіксації. З урахуванням того, що КПК України не оперує таким окремим джерелом доказів, як «електронні докази», на практиці виникають проблеми щодо того, як саме такі докази повинні збиратися. Очевидно, що насамперед все буде залежати від того, які саме завдання ставляться від слідства та якими можливостями наділені уповноважені посадові особи.

Звичайно, що найкращим способом верифікації електронних доказів є фізичний доступ до пристрою, на якому така інформація була згенерована чи опублікована в мережі Інтернет. Непоодинокими є випадки тимчасового доступу до таким комп'ютерів для ознайомлення та вилучення необхідної інформації. Наприклад, була ситуація, коли на адресу Департаменту кіберполіції Національної поліції України надійшла інформація з правоохоронних органів Великої Британії щодо розповсюдження користувачем в анонімному сегменті інтернету протиправного контенту з ознаками дитячої порнографії. «Одночасно з цим на адресу ВПК в Полтавській області Київського управління кіберполіції ДКП НП України надійшло звернення від 22.11.2018 від ОСОБА_4, в якому останній повідомляє про те, що, перебуваючи у себе вдома … де працюючи за своїм власним комп'ютером, 22.11.2018 він скачав з мережі Інтернет на свій комп'ютер «ІНФОРМАЦІЯ_1» та почав його вивчати. … При перегляді даних файлів виявив на них дитячу порнографію, яку скачав на диск, та який у подальшому передав працівникам кіберполіції». У подальшому було проведено огляд такої інформації, за результатами чого, а також за результатами моніторингу анонімного сегмента інтернету виявлено додаткові матеріали, які свідчать про участь у злочинній діяльності трьох невстановлених раніше осіб чоловічої та жіночої статі. «Використовуючи наявні фотографії та методику OSINT щодо пошуку, збору та аналізу інформації, отриманої з відкритих джерел, виявлено соціальні сторінки ІНФОРМАЦІЯ_9 (ОСОБА_6) та ІНФОРМАЦІЯ_10 (ОСОБА_7). При аналізі зазначених профілів встановлено, що на фото зображені одні й ті ж особи, що і на відеоматеріалах

порнографічного характеру за участю зазначених осіб. У подальшому з'ясовані анкетні дані вказаних осіб, якими виявились громадянка України ОСОБА_8, ІНФОРМАЦІЯ_11, проживає за адресою: АДРЕСА_3, яка користується абонентським номером НОМЕР_1, та ОСОБА_9, ІНФОРМАЦІЯ_12, проживає за адресою: АДРЕСА_4, який користується абонентським номером НОМЕР_2»[1]. У подальшому в даному кримінальному провадженні було отримано дозвіл на проведення тимчасового доступу до інформації щодо телефонних дзвінків, смс-повідомлень тощо осіб, які були ідентифіковані слідством.

Даний приклад досить яскраво демонструє специфіку поєднання OSINT розслідування та інших способів збирання інформації у кримінальному провадженні. За допомогою OSINT розслідування була отримана орієнтуюча інформація про осіб, які можуть бути причетними до кримінального правопорушення (були встановлені їхні особи за допомогою пошуку за зображенням), а вже за допомогою тимчасового доступу буде отримана інформація, яка буде доводити (чи спростовувати) їхню винуватість.

Також для отримання відповідної інформації досить часто проводяться обшуки з метою вилучення комп'ютерного обладнання, на якому була згенерована чи розповсюджена інформація, яка цікавить слідство. Наприклад, в одному кримінальному провадженні особа публікувала низку дописів в соціальній мережі «Фейсбук» із закликами до повалення конституційного ладу, хоча в подальшому в судовому засіданні вини своєї не визнала та зазначала, що «до повалення державного ладу він не закликав, такі дописи не поширював та не писав, сторінку свою в соціальній мережі не контролював, хтось інший публікував на його сторінці дописи, можливо, хакери взламали його сторінку»[2]. Звертаємо увагу, що в цьому рішенні Верховний Суд підтвердив позицію, що Фейсбук відноситься до засобів масової інформації — «ОСОБА_8 вирішив використати персональну сторінку користувача соціальної мережі «Facebook» всесвітньої мережі Інтернет з назвою «ОСОБА_9»

---

[1] Ухвала слідчого судді Октябрського районного суду міста Полтави від 15.02.2019, справа № 554/10454/18. URL: https://reyestr.court.gov.ua/Review/79874654

[2] Постанова ККС ВС від 29.11.2023, справа № 595/359/21. URL: https://reyestr.court.gov.ua/Review/115476534#

та електронною адресою: «ІНФОРМАЦІЯ_2», яка у відповідності до вимог абзаців 16, 19 ч. 1 ст. 1 Закону України «Про телекомунікації» і ст. 22 Закону України «Про інформацію», є засобом масової інформації»[1].

Власне, сама інформація про незаконну діяльність була виявлена шляхом моніторингу соціальних мереж уповноваженими посадовими особами, що було відображено в рапорті начальника управління поліції. У даному випадку не обов'язково, щоб така інформація була виявлена безпосередньо начальником управління чи іншою посадовою особою, головне — щоб інформація була загальнодоступною та відповідна уповноважена особа могла з нею ознайомитися. Тобто збір інформації з відкритих джерел може проводитись будь-ким, в тому числі і OSINT аналітиками, а вже первинна «легалізація» такої інформації шляхом її офіційного встановлення буде відбуватися через моніторинг відкритих джерел уповноваженими особами. Для кримінального провадження не має значення, в який саме спосіб уповноважена особа дізналася про таку інформацію — самостійно натрапила на неї в мережі Інтернет чи їй про це повідомили будь-які інші особи, адже в такому випадку не обмежують права та свободи людини, у зв'язку з чим кримінальне процесуальне законодавство не може (і не повинно) регулювати момент отримання інформації з відкритих джерел.

У подальшому, для доведення винуватості особи, в її житлі було проведено обшук, в результаті якого було вилучено комп'ютер, на якому зловмисник заходив у Фейсбук та публікував свої дописи. «Із протоколу обшуку від 16.07.2020 у житловому будинку та господарських приміщеннях за адресою: АДРЕСА_1, де проживають ОСОБА_4 та ОСОБА_20, вбачається, що у спальній кімнаті виявлено блок ПЕОМ. Після його запуску у розділі «історія» браузера за 15.07.2020 встановлено наявність посилання на сторінку профілю «ОСОБА_6», соціальної мережі «Facebook». При відкритті вказаної сторінки у розділі «життєпис» виявлено допис, зокрема за 15.07.2020 о 16 год 12 хв, який розпочинається словами «Мене вже все ваше…» та закінчується словами «повставайте всі вперед знищувати всю ту…» та інші дописи аналогічного змісту.

[1] Постанова ККС ВС від 29.11.2023, справа № 595/359/21. URL: https://reyestr.court.gov.ua/Review/115476534#

У подальшому у програмі «Месенджер» соціальної мережі «Facebook» виявлено листування із ОСОБА_7, якому надіслано повідомлення, яке містить нецензурну лексику. Також у цій же програмі виявлено повідомлення, надіслані ОСОБА_16, датоване 21.03.2020 о 21 год 06 хв, яке містить нецензурну лексику».

Для доведення того, що саме з цього комп'ютера особа публікувала свої дописи, також була проведена експертиза і «відповідно до висновку експерта № 7-223/20 від 28.08.2020 вбачається, що наданий на дослідження системний блок ПЕОМ з процесором «AMD-A4-4020AP4», тактовою частотою 3,2 ГГц, і жорстким диском № WDCWD5000AZRX-00A3KBO, був під'єднаний до мережі Інтернет у період з 02.01.2020 по 16.07.2020. З використанням наданого системного блоку ПЕОМ здійснювався доступ до соціальної мережі «Facebook» (відвідування інтернет-сайту з адресою «ІНФОРМАЦІЯ_2») в період з 13.01.2020 по 16.07.2020. У період з 25.06.2020 по 16.07.2020 з наданого на дослідження системного блоку здійснювався доступ до соціальної мережі «Facebook» з використанням профілю користувача з ID НОМЕР_3 (назва користувача згідно з інтернет-історією «ОСОБА_6»)».

Таким чином, слідство отримало докази того, що дописи були зроблені саме обвинуваченим, адже, відповідно до протоколів допиту, інші особи, які проживали разом з обвинувачем, хоча і користувалися комп'ютером, проте доступу до соціальної мережі «Фейсбук» обвинуваченого не мали. Власне, можна зазначити, що це найкращий спосіб для доведення винуватості особи на підставі інформації, розміщеної у відкритому доступі, — отримати фізичний доступ до комп'ютерного пристрою для того, щоб довести, що саме з цього комп'ютера робились дописи, а фактичне місцезнаходження комп'ютера доводить те, що ним користувалася конкретна особа, що доводить її винуватість поза розумним сумнівом. Проте така ситуація якщо і можлива, то лише на завершальних етапах досудового розслідування, коли визначено місце проживання особи, яка вчиняє кримінальні правопорушення. Очевидно, що OSINT розслідування часто виступає як спосіб збирання орієнтуючої інформації або як проміжний етап при вчиненні інших слідчих (розшукових) дій, які виходять за межі «електронного світу». У той же час самі OSINT аналітики такими можливостями не наділені. Крім того, навіть

у даному кримінальному провадженні критичне значення має той факт, що такі дописи були загальнодоступними, а тому обов'язково необхідно зафіксувати самі допити і в інших доступ.

Конкретно в даному кримінальному провадженні було проведено таку НСРД, як зняття інформації з електронних інформаційних систем: «судом досліджено протокол зняття інформації з електронних інформаційних систем від ІНФОРМАЦІЯ_103, час початку — 16 год 05 хв, час закінчення — 20 год 47 хв та зображення до нього. Із вказаного протоколу вбачається, що у ході процесуальної дії за допомогою службового ноутбука марки «Fujitsu» з використанням браузера «Chrome» було оглянуто профіль «ОСОБА_6» у соціальній інтернет-мережі «Facebook» на вкладці «Життєпис». Інформація профілю є загальнодоступною, доступ до неї необмежений для усіх користувачів соцмережі «Facebook». Крім того, до вказаного протоколу додано зображення дописів, які розміщував ОСОБА_4 у соціальній мережі «Facebook», зокрема, допис від ІНФОРМАЦІЯ_32 за окремою електронною адресою ІНФОРМАЦІЯ_29, який містить графічне зображення тексту «я закликаю до повалення того конституційного ладу в Україні …», та ще 50 зображень дописів з аналогічним змістом на 51 аркуші»[1].

Проте в науковій літературі вже досить давно обговорюється питання щодо доцільності проведення саме НСРД для фіксації інформації з мережі Інтернет, яка знаходиться у відкритому доступі, «оскільки порядок виявлення та фіксації таких відомостей не пов'язаний з подоланням захисту інформації від втручання інших осіб, а тому не відповідає суті негласної слідчої (розшукової) дії. Даний різновид інформації має виявлятися та фіксуватися шляхом проведення такої слідчої (розшукової) дії, як огляд»[2]. Як свідчать матеріали судової практики[3], на даний момент для фіксації інформації, яка міститься у відкритому доступі, проводиться саме огляд.

---

1 Вирок Бучацького районного суду Тернопільської області від 10.03.2023, справа № 595/359/21. URL: https://reyestr.court.gov.ua/Review/109460422

2 Малахова О.В. До питання огляду сторонами кримінального провадження змісту інтернет-сторінок. *Вісник кримінального судочинства*. 2017. № 2. С. 64–69.

3 Постанова ККС ВС від 27.05.2020, справа № 296/2803/16-к. URL: https://reyestr.court.gov.ua/Review/89621215; Вирок Святошинського районного суду м. Києва від 08.08.2023, справа № 759/5413/23. URL: https://reyestr.court.gov.ua/Review/112680427; Ухвала слідчого судді Октябрського районного суду м. Полтави від 09.01.2024, справа № 554/314/24. URL: https://reyestr.court.gov.ua/Review/116260709

Велике значення для цього також має уточнення процедури проведення огляду, а саме доповнення ч. 2 ст. 237 КПК України новим абзацом, відповідно до якого «огляд комп'ютерних даних проводиться слідчим, прокурором шляхом відображення у протоколі огляду інформації, яку вони містять, у формі, придатній для сприйняття їхнього змісту (за допомогою електронних засобів, фотозйомки, відеозапису, зйомки та/або відеозапису екрана тощо або у паперовій формі)». Даним формулюванням законодавець намагався надати працівникам правоохоронних органів досить широкі можливості в частині фіксації електронних доказів, залишаючись у межах даної слідчої дії. Тобто в будь-якому випадку результати огляду мають бути зазначені в протоколі, проте додатком до цього протоколу можуть бути будь-які носії чи форми фіксації інформації, які є «придатними для сприйняття їхнього змісту». Таким чином, уповноважена посадова особа повинна самостійно визначити, в якій формі необхідно здійснювати фіксацію таких відомостей. Головне, щоб були враховані всі вимоги, які були зазначені попередньо (наприклад, зазначена хеш-сума).

Тема 5

ОСОБЛИВОСТІ OSINT РОЗСЛІДУВАНЬ ЕКОНОМІЧНИХ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

5.1 ПОНЯТТЯ ТА ВИДИ ЕКОНОМІЧНИХ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

Необхідно зазначити, що чинний КК України не містить поняття «економічних злочинів». Цей термін насамперед використовується в правовій доктрині для опису цілого спектра кримінальних правопорушень, які вчиняються у сфері економічних та (або) фінансових відносин. Так, у доктрині також виділяють такі терміни, як «злочини у сфері економіки», «економічні злочини», «тіньова економіка», «кримінальна економіка», «економічна злочинність» та інші. Деякі вчені стверджують, що економічні злочини є майновими і корисливими злочинами, а також злочинами у сфері економіки, які характеризуються сукупністю корисливих зазіхань на власність, порядок управління господарством, що вчиняються особами, які займають певні соціальні позиції в структурі економіки. Інші науковці зазначають, що усі ці поняття мають різний спектр вчинення протиправних діянь. Так, злочини у сфері економіки — це переважно господарські злочини, які вчиняються в різних сферах; економічна злочинність полягає у вчиненні злочинів у сфері господарської діяльності, в тому числі із використанням службового становища. До злочинів економічного характеру слід відносити діяння,

які пов'язані із спричиненням матеріальної шкоди чи отриманням матеріальної вигоди[1].

Власне, до економічних злочинів часто відносять кримінальні правопорушення, які передбачені Розділом VII КК України, тобто кримінальні правопорушення у сфері господарської діяльності: (ст. 199 «Виготовлення, зберігання, придбання, перевезення, пересилання, ввезення в Україну з метою використання при продажу товарів, збуту або збут підроблених грошей, державних цінних паперів, що існують у паперовій формі, білетів державної лотереї, марок акцизного податку чи голографічних захисних елементів», ст. 200 «Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення», ст. 201 «Контрабанда культурних цінностей та зброї», ст. 201[1] «Контрабанда лісоматеріалів та цінних порід дерев», ст. 201[2] «Незаконне використання з метою отримання прибутку гуманітарної допомоги, благодійних пожертв або безоплатної допомоги», ст. 201[3] «Контрабанда товарів», ст. 201[4] «Контрабанда підакцизних товарів», ст. 203[1] «Незаконний обіг дисків для лазерних систем зчитування, матриць, обладнання та сировини для їх виробництва», ст. 203[2] «Незаконна діяльність з організації або проведення азартних ігор, лотерей», ст. 204 «Незаконне виготовлення, зберігання, збут або транспортування з метою збуту підакцизних товарів», ст. 205[1] «Підроблення документів, які подаються для проведення державної реєстрації юридичної особи та фізичних осіб — підприємців», ст. 206 «Протидія законній господарській діяльності», ст. 206[2] «Протиправне заволодіння майном підприємства, установи, організації», ст. 209 «Легалізація (відмивання) майна, одержаного злочинним шляхом», ст. 209[1] «Умисне порушення вимог законодавства про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення», ст. 210 «Нецільове використання бюджетних коштів, здійснення видатків бюджету чи надання кредитів з бюджету без встановлених бюджетних призначень

[1] Кравчук С.Й. Економічна злочинність в Україні. URL: http://westudents.com.ua/knigi/116-ekonomchna-zlochinnst-v-ukran-kravchuk-sy.html

або з їх перевищенням», ст. 211 «Нецільове використання бюджетних коштів, здійснення видатків бюджету чи надання кредитів з бюджету без встановлених бюджетних призначень або з їх перевищенням», ст. 212 «Нецільове використання бюджетних коштів, здійснення видатків бюджету чи надання кредитів з бюджету без встановлених бюджетних призначень або з їх перевищенням», ст. 212^1 «Ухилення від сплати єдиного внеску на загальнообов'язкове державне соціальне страхування та страхових внесків на загальнообов'язкове державне пенсійне страхування», ст. 213 «Порушення порядку здійснення заготівлі металобрухту та операцій з металобрухтом», ст. 218^1 «Доведення банку до неплатоспроможності», ст. 219 «Доведення до банкрутства», ст. 220^1 «Порушення порядку ведення бази даних про вкладників або порядку формування звітності», ст. 220^2 «Фальсифікація фінансових документів та звітності фінансової організації, приховування неплатоспроможності фінансової установи або підстав для відкликання (анулювання) ліцензії фінансової установи», ст. 222 «Шахрайство з фінансовими ресурсами», ст. 222^1 «Маніпулювання на організованих ринках», ст. 222^2 «Маніпулювання на енергетичному ринку», ст. 223^1 «Підроблення документів, які подаються для реєстрації випуску цінних паперів», ст. 224 «Виготовлення, збут та використання підроблених цінних паперів (крім державних цінних паперів)», ст. 227 «Умисне введення в обіг на ринку України (випуск на ринок України) небезпечної продукції», ст. 229 «Незаконне використання знака для товарів і послуг, фірмового найменування, кваліфікованого зазначення походження товару», ст. 231 «Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю», ст. 232 «Розголошення комерційної, банківської таємниці або професійної таємниці на ринках капіталу та організованих товарних ринках», ст. 232^1 «Незаконне використання інсайдерської інформації», ст. 232^2 «Приховування інформації про діяльність емітента», ст. 232^3 «Незаконне використання інсайдерської інформації щодо оптових енергетичних продуктів», ст. 233 «Незаконна приватизація державного, комунального майна»).

Однак при використанні OSINT інструментів уповноважені посадові особи, очевидно, не обмежені лише цим переліком кримінальних правопорушень. У даному випадку насамперед кримінальні

правопорушення доцільно групувати не за об'єктом протиправного посягання, а за можливістю використання відкритих джерел для їхнього розслідування. Відповідно, доцільно в дану умовну групу включити і фінансові кримінальні правопорушення. На думку науковців, фінансові злочини — узагальнене поняття, що поширюється на різні види незаконних дій, пов'язаних з отриманням, використанням та розподілом фінансових ресурсів, а саме: відмивання коштів злочинного походження, шахрайство з фінансовими ресурсами суб'єктів господарювання, підроблення грошових коштів та цінних паперів, порушення податкового та банківського законодавства тощо, які створюють загрозу фінансовій безпеці держави[1].

Крім того, необхідно звернути увагу, що в Україні діє Бюро економічної безпеки, до завдань якого відноситься виявлення зон ризиків у сфері економіки шляхом аналізу структурованих і неструктурованих даних; оцінювання ризиків і загроз економічній безпеці держави, напрацювання способів їхньої мінімізації та усунення; надання пропозицій щодо внесення змін до нормативно-правових актів з питань усунення передумов створення схем протиправної діяльності у сфері економіки; забезпечення економічної безпеки держави шляхом запобігання, виявлення, припинення, розслідування кримінальних правопорушень, що посягають на функціонування економіки держави; збирання та аналіз інформації про правопорушення, що впливають на економічну безпеку держави, та визначення способів запобігання їхньому виникненню в майбутньому; планування заходів у сфері протидії кримінальним правопорушенням, віднесеним законом до його підслідності; виявлення та розслідування правопорушень, пов'язаних з отриманням та використанням міжнародної технічної допомоги; складання аналітичних висновків і рекомендацій для державних органів з метою підвищення ефективності прийняття ними управлінських рішень щодо регулювання відносин у сфері економіки.

З огляду на ці завдання, які передбачені Законом України «Про Бюро економічної безпеки України», а також з огляду на те, що в даному

[1] Комишнюк Ю.О. (2020). Проблеми розслідування фінансових злочинів. *Теоретичні питання юриспруденції і проблеми правозастосування: виклики XXI століття* : тези доп. учасників IV Всеукр. наук.-практ. конф. (Харків, 20 лист. 2020 р.). С. 155–157.

контексті використовується найбільш широке поняття «економічних кримінальних правопорушень», можна зробити висновок, що до таких правопорушень також необхідно відносити ті, які можуть розслідуватися БЕБ. А це, крім кримінальних правопорушень, які передбачені Розділом VII КК України (хоча слід підкреслити, що до підслідності БЕБ відносяться не всі кримінальні правопорушення, які передбачені цим розділом), також ст. 191 «Привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем» та ст. 364 «Зловживання владою або службовим становищем» за дотриманням умов, які передбачені ст. 216 КПК України. Власне, в даному аспекті також можна включити до досліджуваної категорії і корупційні кримінальні правопорушення, які передбачені в примітці до ст. 45 КК України, а також ті правопорушення, які додатково віднесені до підслідності НАБУ та підсудності ВАКС. Загалом необхідно ще раз наголосити, що ключовим при виділенні економічних злочинів, які можуть бути розслідувані за допомогою OSINT технологій, є не об'єкт, на який буде направлене злочинне посягання, а можливість застосування подібних цифрових баз даних, методів вилучення та обробки інформації з них та схожість в аналітичному процесі при виявленні ознак кримінального правопорушення та збирання доказів. Саме тому додатково підкреслюється, що в даній темі досліджуються не кримінальні правопорушення, передбачені КК України, а саме група правопорушень, а методи їхнього розслідування із застосуванням OSINT технологій, які можуть за незначних модифікацій бути використані в аналогічних розслідуваннях.

Крім того, логіка об'єднання таких злочинів в одну категорію пояснюється відсутністю чіткого розмежування аналогічних кримінальних правопорушень у зарубіжних країнах. Досліджуючи нормативно-правові акти інших країн, можна помітити, що там досить часто використовуються саме формулювання «економічні» та «фінансові» злочини, хоча під цю категорію можуть потрапляти абсолютно різні за своїм змістом кримінальні правопорушення.

При цьому навіть поверхневого аналізу нормативного масиву та наукових публікацій достатньо для того, щоб побачити, що на окремі економічні злочини звертається більше уваги. Це пов'язано як зі значною

шкодою, яка може бути завдана такими правопорушеннями суспільним інтересам та економіці держави, так і їх інколи транснаціональним характером. Так, значна увага приділяється проблемі відмивання грошей (легалізації доходів, отриманих незаконним шляхом). На території ЄС було розроблено декілька Директив проти відмивання грошей (Anti-Money Laundering Directives — AMLD), остання з яких (шоста) набрала законної сили 3 грудня 2020 року.

Метою даної Директиви є встановлення мінімальних стандартів нормативного регулювання, узгодження визначення «кримінальні правопорушення» і додавання санкцій відповідно до існуючих норм. У документі формується єдине визначення «правопорушення, пов'язаного з відмиванням грошей», а також надається перелік з двадцяти двох конкретних предикатних злочинів, пов'язаних з відмиванням грошей, до яких включаються злочини в сфері екології, кіберзлочини, прямі та непрямі податкові злочини тощо. Також було розширено коло злочинів, пов'язаних з відмиванням грошей, включивши до нього пособництво, підбурювання та замах на вчинення злочину, пов'язаного з відмиванням грошей. Також була посилена співпраця країн-членів ЄС між собою та з іншими країнами в частині виявлення та припинення злочинів, пов'язаних з відмиванням грошей[1].

Власне, це приклад лише одного нормативного документа ЄС, який напряму пов'язаний з економічними злочинами. Даному типу правопорушень, як вже було зазначено, має приділятися особлива увага, адже лише на одному відмиванні грошей ЄС щорічно втрачає до 1 % ВВП. Через свою значну економічну шкоду OSINT аналітики повинні детально вивчати всі можливі способи вчинення даних кримінальних правопорушень. Одночасно з цим необхідно підкреслити, що значна частина таких правопорушень може бути розкрита саме завдяки інформації з відкритих джерел, що ще більше підкреслює значення проведення такого роду розслідувань. Проте будь-яке якісне OSINT розслідування повинно починатися з вибору правильного джерела отримання інформації.

---

[1] Understanding the Sixth Anti-Money Laundering Directive (6AMLD). Tookitaki : website. URL: https://www.tookitaki.com/compliance-hub/about-6th-money-laundering-directive

5.2 ВИДИ ВІДКРИТИХ ДЖЕРЕЛ ПРИ РОЗСЛІДУВАННІ ЕКОНОМІЧНИХ ЗЛОЧИНІВ

Насамперед необхідно наголосити, що відкритих джерел, з яких можна отримувати інформацію про економічні злочини, є досить багато, і перерахувати їх в одній темі неможливо. У той же час таке завдання і не повинно ставитися на рівні підручника, адже вже неодноразово було підкреслено, що основним завданням даного підручника є формування певного алгоритму роботи з відкритими джерелами, а не створення покрокової інструкції. Крім того, необхідно зазначити, що будь-які відкриті джерела з часом можуть зникнути, а на їхню заміну можуть бути розроблені інші загальнодоступні реєстри чи бази даних. Тому надавати довідник відкритих реєстрів недоцільно також з точки зору їхньої постійної зміни та оновлення. Однак на окремих прикладах необхідно зупинитися детальніше, адже навіть якщо в подальшому такі джерела перестануть існувати, з великою долею вірогідності будуть існувати їхні аналоги.

Ведучи мову про розслідування економічних злочинів насамперед необхідно звернути увагу на загальнодоступні державні реєстри, які прямо чи опосередковано стосуються економічної діяльності. Перелік таких реєстрів можна знайти, наприклад, на сайті ДП «Національні інформаційні системи» (https://nais.gov.ua), на якому є не лише перелік корисних реєстрів, а і нормативно-правова база їхнього функціонування. Власне, в даному переліку є сенс окремо виділити Державний реєстр речових прав на нерухоме майно (https://online.minjust.gov.ua/rrp/), доступ до якого здійснюється за допомогою електронного цифрового підпису, де можна формувати запит і після його оплати отримати необхідну інформацію. Відповідно до ЗУ «Про державну реєстрацію речових прав на нерухоме майно та їх обтяжень» Державний реєстр прав містить відомості про зареєстровані речові права на нерухоме майно, об'єкти незавершеного будівництва, майбутні об'єкти нерухомості та їхнє обтяження, а також про взяття на облік безхазяйного нерухомого майна і ціну (вартість) нерухомого майна, об'єкта незавершеного будівництва, майбутнього об'єкта нерухомості та речових прав на нього чи розмір плати за користування нерухомим майном за відповідними

правочинами, відомості та електронні копії документів, подані у паперовій формі, або документи в електронній формі, на підставі яких проведено реєстраційні дії, а також документи, сформовані за допомогою програмних засобів ведення Державного реєстру прав під час проведення таких реєстраційних дій, та відомості реєстрів (кадастрів), автоматизованих інформаційних систем, отримані державним реєстратором шляхом безпосереднього доступу до них чи в порядку інформаційної взаємодії таких систем з Державним реєстром прав.

Пошук у даному реєстрі можливий за адресою, реєстраційним номером об'єкта нерухомості та за кадастровим номером земельної ділянки. Крім того, можна шукати не сам об'єкт нерухомості, а особу, яка цікавить OSINT аналітика. Для цього можна шукати відомості за ідентифікаційними даними фізичної (РНОКПП або ПІБ) та юридичної (ЄДРПОУ або назва юридичної особи) особи. Необхідно звернути увагу на те, що результативність пошуку може залежати не тільки від якості самого запиту, а і від повноти інформації, яка була внесена державним реєстратором при реєстрації відповідного об'єкта нерухомості. Помилки при внесенні таких відомостей в реєстр трапляються досить часто (наприклад, при внесенні даних про реєстр нерухомості можуть не вказати РНОКПП власника, що зробить неможливим пошук такої нерухомості саме за цим критерієм)[1]. Тому рекомендується здійснювати декілька пошуків за різними критеріями — і за ПІБ власника, і за місцем знаходження нерухомого майна, і за кадастровим номером земельної ділянки тощо в залежності від того, якою інформацією володіє OSINT аналітик.

Вкрай важливим та корисним також є Єдиний державний реєстр декларацій (https://public.nazk.gov.ua). Відповідно до Порядку формування, ведення та оприлюднення (надання) інформації Єдиного державного реєстру декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування, функціональні можливості Реєстру забезпечують: створення, збереження, подання та перегляд електронних

[1] При цьому необхідно наголосити, що відповідно до ЗУ «Про державну реєстрацію речових прав на нерухоме майно та їх обтяжень», відомості, що містяться у Державному реєстрі прав, повинні відповідати відомостям, що містяться в документах, на підставі яких проведені реєстраційні дії. У разі їхньої невідповідності пріоритет мають відомості, що містяться в документах, на підставі яких проведені реєстраційні дії.

документів суб'єктів декларування; пошук за ключовими словами; моніторинг відвідувань та дій з даними Реєстру його користувачами, крім осіб, які здійснюють доступ до публічної частини Реєстру; захист даних (у тому числі персональних даних) від несанкціонованого доступу, знищення, зміни та блокування доступу до них шляхом здійснення організаційних і технічних заходів, впровадження засобів та методів технічного захисту інформації; розмежування та контроль доступу до даних Реєстру згідно з повноваженнями користувачів; наявність зручних інтерфейсів та сервісів, що за ініціативою зареєстрованого у Реєстрі суб'єкта декларування дають йому змогу безоплатно отримувати відомості стосовно себе та членів своєї сім'ї з інформаційно-комунікаційних і довідкових систем, реєстрів, банків даних, у тому числі тих, що містять інформацію з обмеженим доступом, держателем (адміністратором) яких є державні органи або органи місцевого самоврядування, до яких Національне агентство має автоматизований доступ, з метою заповнення декларацій. За ініціативою суб'єкта декларування відомості про членів його сім'ї надаються (за наявності) після підтвердження такими особами належності їх до членів сім'ї суб'єкта декларування, погодження ними збору та передачі суб'єкту декларування таких відомостей, що реалізується за допомогою програмних засобів Реєстру та інших інформаційно-комунікаційних систем, у тому числі засобами Єдиного державного вебпорталу електронних послуг, зокрема з використанням мобільного додатка Порталу «Дія»; електронну ідентифікацію користувачів, крім користувачів публічної частини Реєстру; відповідність електронних документів визначеним правилам; інтеграцію та обмін даними з інформаційно-комунікаційними і довідковими системами, реєстрами, банками даних, у тому числі тими, що містять інформацію з обмеженим доступом, держателем (адміністратором) яких є державні органи або органи місцевого самоврядування; можливість формування статистичних даних Реєстру.

Реєстр декларацій є потужним та корисним інструментом в руках OSINT аналітиків, які займаються розслідуванням економічних злочинів. Експерти зазначають, що в процесі аналізу декларацій, які доступні в публічному доступі, необхідно звертати увагу на:

– дату подачі декларації (декларації подаються лише на офіційному вебсайті Національного агентства з питань запобігання

корупції. Паперова копія декларації не надається, а її подання не свідчить про відсутність складу злочину, передбаченого ст. 366-1 КК України);

- місце роботи особи, яка подає декларацію (інформація в цьому розділі декларації зазначається станом на останній день звітного періоду. Це правило не поширюється на осіб, які займають відповідальне та особливо відповідальне становище станом на день початку роботи системи подання й оприлюднення декларацій у 2016 році. Такі суб'єкти декларування зазначають своє місце роботи, посаду, належність до осіб, які займають відповідальне та особливо відповідальне становище, а також до посад, пов'язаних з високим рівнем корупційних ризиків, станом на день початку роботи системи в 2016 році);
- інформацію про членів сім'ї суб'єкта декларування (до декларації включається інформація про членів сім'ї станом на останній день звітного періоду незалежно від тривалості);
- об'єкти нерухомості (нерухомість об'єднання співвласників багатоквартирного будинку (ОСББ) не декларується. Садиба (будинок з прилеглими господарськими будівлями, садом, городом) декларується як один об'єкт з його повним описом або як кілька об'єктів, якщо вони зареєстровані окремо. Користування нерухомістю декларується в розділі «Об'єкти нерухомості» лише, якщо воно обов'язково відбувалося до 31 грудня звітного року, також декларується в розділі «Видатки та правочини», якщо укладався договір користування, вартістю більше 50 прожиткових мінімумів, встановлених для працездатних осіб на 1 січня звітного року (ПМП), об'єкти незавершеного будівництва (у розділі «Об'єкти незавершеного будівництва» у декларації зазначаються: об'єкти незавершеного будівництва; об'єкти, не прийняті в експлуатацію; об'єкти, право власності на які не зареєстроване в установленому законом порядку, якщо вони станом на останній день звітного періоду або: належать пропущений текст? декларанту чи членам його сім'ї на праві власності відповідно до Цивільного кодексу України; розташовані на земельних ділянках, що належать декларанту чи членам

його сім'ї на праві приватної власності, включаючи спільну власність, або передані їм в оренду чи на іншому праві користування, незалежно від правових підстав набуття такого права; повністю або частково побудовані з матеріалів чи за кошти декларанта або членів його сім'ї);

– цінне рухоме майно (рухоме майно декларується в розділі «Цінне рухоме майно (крім транспортних засобів)», якщо його вартість перевищує 100 ПМП. Але у випадку декларування такого майна в цьому розділі з позначкою «Не відомо» у графі «Вартість на дату набуття», вартість об'єкта не визначається на рівні 100 ПМП. Виняток: цінні рухомі речі, що придбані як набір (столовий сервіз, набір меблів, набір ювелірних прикрас тощо) й одночасно, декларуються одним об'єктом. Якщо цінне рухоме майно є подарунком, вартість якого перевищує 5 ПМП, його необхідно зазначити також у розділі «Доходи, у тому числі подарунки»);
– транспортні засоби (у розділі «Цінне рухоме майно — транспортні засоби» декларуються: легкові та вантажні автомобілі, автобуси, самохідні машини, сконструйовані на шасі автомобілів, мотоцикли всіх типів, марок і моделей, причепи, напівпричепи, мотоколяски, інші прирівняні до них транспортні засоби та мопеди, сільськогосподарська техніка, водні та повітряні судна; незалежно від вартості станом на дату набуття) та інші відомості[1].

Існують і інші державні реєстри та бази даних (наприклад, Електронна система публічних закупівель Prozorro (https://prozorro.gov.ua/uk), детально про яку мова піде нижче). OSINT аналітик повинен сам визначити, який саме реєстр йому потрібен з огляду на те, яку інформацію йому необхідно отримати. У даному випадку необхідно лише наголосити, що OSINT розслідування вимагає від аналітика використання одразу декількох різних реєстрів, відомості з яких будуть доповнювати один одного. Наприклад, у результаті моніторингу реєстру декларацій можуть бути виявлені підозрілі дані про об'єкт нерухомого майна, у зв'язку з чим аналітик повинен перевірити таке майно в реєстрі

[1] Волошин О., Панкратова Л. «Реальний» алгоритм перевірки електронних декларацій. URL: https://irrp.org.ua/realniy-algoritm-perevirki-elektronnih-deklaratsiy-vid-yuristiv-irrp/

речових прав на нерухоме майно та підтвердити (чи спростувати) свої підозри. У подальшому, можливо, виникне потреба у перевірці відомостей про власника такого майна в Єдиному державному реєстрі юридичних осіб, фізичних осіб-підприємців та громадських формувань (https://usr.minjust.gov.ua/content/free-search) з подальшим детальним вивченням судових справ, учасником якого була певна юридична особа, в Єдиному державному реєстрі судових рішень (https://reyestr.court.gov.ua). Логіка використання відкритих джерел насамперед має диктуватися необхідністю отримання конкретної інформації та її доступністю в таких джерелах. До того ж в процесі збирання та аналізу інформації OSINT аналітик може виявити ознаки іншого кримінального правопорушення або додаткові докази, про існування яких він не здогадувався. Такий «ланцюговий» процес збирання інформації є вкрай важливим також тому, що в процесі може бути розкрита додаткова інформація, яка не була визначена як мета розслідування в першочерговому плані.

Поряд з цим також необхідно зазначити, що OSINT аналітикам доцільно користуватися не лише українськими відкритими джерелами, а і зарубіжними, які також доступні для наших користувачів. Як вже зазначалося, економічна злочинність може бути транснаціональною, тому існує сенс також досліджувати додаткові джерела, які можуть містити важливу для OSINT аналітиків інформацію.

Очевидно, що перелік таких джерел є ще більшим, тому на первинному етапі необхідно ідентифікувати ті ресурси, які потрібні OSINT аналітику при розслідуванні економічних злочинів. Це можна зробити шляхом формування коректного та чіткого запиту в пошукових сервісах (детальніше про це див. Тему 3). Проте в якості окремих прикладів можна продемонструвати найбільш популярні ресурси, якими користуються аналітики.

Так, на сайті BINLIST.NET (https://binlist.net), ввівши перші 6 або 8 цифр банківської карти, можна отримати інформацію про тип картки, країну, в якій розташований банк, що видав картку, та сам банк. Це можливо завдяки тому, що перші цифри на банківських картках є ідентифікаторами, які дозволяють отримати загальнодоступну інформацію, яка не стосується персональних даних власника карти (мал. 5.1).

Мал. 5.1. Приклад банківської карти

На даному прикладі:

1 — Major Industry Identifier (MII) — ідентифікатор основної галузі. Він вказує, до якої галузі належить ваша картка. Найбільш популярні галузі (1 — Авіакомпанії; 2 — Авіакомпанії та фінансові установи; 3 — Подорожі та розваги, а також American Express; 4–6 — Банківські установи, фінанси та мерчандайзинг (Visa, MasterCard, etc.); 7 — Нафта; 8 — Охорона здоров'я та комунікації; 9 — Уряд. В Україні їх всього 3: 4 — Visa; 5 — MasterCard; 9 — Простір);

2 — ідентифікаційний номер емінента (IIN) або індентифікаційний номер банку (BIN). Цей номер вказує на компанію, що випускає кредитні картки. Кожен постачальник фінансових послуг, що випускає картки, має декілька наборів цифр, які допомагають його ідентифікувати.

В індустрії обслуговування кредитних карток також відбулись значні зміни. З квітня 2022 року всі BIN/IIN розширені з 6 до 8 цифр. Ці зміни необхідні у зв'язку зі збільшенням кількості постачальників фінансових послуг та необхідністю у більшій кількості INN and BIN. Таким чином, більша кількість фінансових установ зможуть випускати картки для свої користувачів.

Наступні 8–10 цифр — ідентифікатори рахунків. Це номер, який фінансова установа надає своєму користувачу. Кожен користувач має свій унікальний ідентифікатор облікового запису.

Остання цифра — перевірка картки на справжність. Остання цифра на картці називається цифра валідатора або контрольна цифра (Check

Digit). Основне призначення цієї цифри — впевнитись, що попередні цифри є дійсними. У кредитних картках вибір цього числа заснований на алгоритмі Луна[1].

Таким чином, маючи інформацію про номер карти особи (навіть в частині, яка не ідентифікує особу), можна вже за допомогою відкритих баз даних отримати певну корисну інформацію про користувача.

На сайті https://opencorporates.com можна отримати відомості про юридичних осіб з усього світу з-понад ніж 220 мільйонів компаній, а на сайті https://www.opensanctions.org можна дізнатися про накладені на юридичні чи фізичні особи санкції або відомості про політичні викриття.

Також важливим при розслідуванні економічних злочинів є ресурс https://offshoreleaks.icij.org — база даних, яка містить інформацію про понад 810 тисяч офшорних компаній, які фігурували в Панамських, Пандорських, Райських паперах та в інших документах, які стали відомі громадськості. Дані пов'язані з людьми та компаніями з-понад 200 країн та територій. Однак самі автори ресурсу зазначають, що «існують законні способи використання офшорних компаній і трастів. Включення фізичної або юридичної особи до цієї бази даних ще не означає, що така особа бере учать у незаконній чи неналежній поведінці. Багато людей та організацій мають однакові або схожі імена. Дані надходять безпосередньо з витоку інформації, пов'язаної з різними розслідуваннями, і кожен набір даних охоплює певній період часу, тобто дана інформація з часом може змінитися».

Очевидно, що це далеко не повний перелік джерел, які можна використовувати при розслідуванні економічних злочинів. Тим більше цей перелік постійно змінюється та еволюціонує. Тому OSINT аналітик повинен насамперед при обранні відповідного джерела відштовхуватися від того, яка конкретно інформація йому потрібна. А це вже буде залежати від того, яке саме кримінальне правопорушення розслідується.

---

[1] Перехід на восьмизначний BIN. Bankera. Blog : вебсайт. URL: https://blog.bankera.com/uk-UA/перехід-на-восьмизначний-BIN/

5.3 ВИКОРИСТАННЯ OSINT ІНСТРУМЕНТІВ ПРИ РОЗСЛІДУВАННІ ПРАВОПОРУШЕНЬ У СФЕРІ ПУБЛІЧНИХ ЗАКУПІВЕЛЬ

Ключовим законом у сфері публічних закупівель є Закон України «Про публічні закупівлі». Відповідно до даного закону необхідність реалізації процедури публічних закупівель відноситься до замовників за умови, що вартість предмета закупівлі товару (товарів), послуги (послуг) дорівнює або перевищує 200 тисяч гривень, а робіт — 1,5 мільйона гривень (щодо окремої категорії замовників застосовуються інші суми — 1 мільйон гривень для товару та 5 мільйонів гривень для робіт). У разі здійснення закупівель товарів, робіт і послуг, вартість яких не перевищує 50 тисяч гривень, замовник повинен дотримуватися принципів здійснення публічних закупівель та може використовувати електронну систему закупівель, у тому числі електронні каталоги для закупівлі товарів. У разі здійснення таких закупівель без використання електронної системи закупівель замовник обов'язково оприлюднює в електронній системі закупівель звіт про договір про закупівлю, укладений без використання електронної системи закупівель. У ч. 5 ст. 3 даного Закону також надається перелік винятків, коли дія ЗУ «Про публічні закупівлі» не застосовується (наприклад, якщо предметом закупівлі є товари, роботи і послуги, закупівля яких здійснюється закордонними дипломатичними установами України або фінансові послуги, що надаються у зв'язку з емісією, купівлею, продажем або передачею цінних паперів чи інших фінансових інструментів тощо).

В усіх інших випадках закупівлі відбуваються через електронну систему закупівель (інформаційно-телекомунікаційна система, яка має комплексну систему захисту інформації з підтвердженою відповідністю згідно з Законом України «Про захист інформації в інформаційно-телекомунікаційних системах», що забезпечує проведення закупівель, створення, розміщення, оприлюднення, обмін інформацією і документами в електронному вигляді, до складу якої входять вебпортал Уповноваженого органу, авторизовані електронні майданчики, між якими забезпечено автоматичний обмін інформацією та документами). Наказом

Мінекономрозвитку від 18.03.2016 № 473 (зі змінами) вебпорталом Уповноваженого органу у складі системи визначено інформаційно-телекомунікаційну систему «Prozorro» за адресою в мережі Інтернет: www.prozorro.gov.ua, а відповідальним за забезпечення функціонування та наповнення вебпорталу — Державне підприємство «ПРОЗОРРО».

Як зазначають науковці, запровадження електронної системи публічних закупівель ProZorro має низку переваг:

- можливість державним підприємствам здійснювати прозорі ефективні й економні закупівлі;
- зменшення корупційних ризиків;
- здійснення процесу моніторингу проведення тендерів відкритим і доступним;
- створення умов для залучення нових учасників процесу державних закупівель.

Відповідно до Закону можна виокремити три узагальнені стадії процесу публічних закупівель:

- ідентифікація потреби, ухвалення рішення щодо того, які товари, роботи або послуги мають бути придбані й коли (планування закупівель);
- процес розміщення оголошення про закупівлю відповідних товарів, робіт або послуг, кваліфікацію постачальника (включаючи аукціон для конкурентних процедур) і підписання договору;
- процес адміністрування договору[1].

Задля того щоб виявляти потенційні кримінальні правопорушення в сфері публічних закупівель, необхідно знати базове законодавство в даній галузі, адже лише шляхом порівняння з ним можна знаходити ті чи інші порушення, які були допущені в процесі публічних закупівель. Метою даного підручника не є глибинний аналіз процедури публічних закупівель, а лише презентація способів використання відкритих джерел при розслідуванні відповідних кримінальних правопорушень. У зв'язку з цим доцільно дослідити саме систему ProZorro як ключове відкрите джерело в даній сфері.

---

[1] Виявлення та розслідування злочинів, пов'язаних із зміною ціни при проведенні державних закупівель : навч. посібник / О.В. Авраменко, І.Б. Висоцька, М.Ю. Ковальська, О.З. Мармура, О.Ф. Пасєка. Львів : ЛьвДУВС, 2018. 104 с.

«Методика аналізу публічних закупівель є взаємопроникненням і взаємодоповненням методики економічного аналізу як науки та методики оцінки конкурсних пропозицій. Це обумовлено тим, що аналіз публічних закупівель неможливий без застосування тих специфічних методів, без яких неможливо було б оцінити подані пропозиції. До таких методів варто віднести балансовий метод оцінки конкурсних пропозицій, економіко-математичні методи, методи рейтингової оцінки, економічної оцінки, багатокритеріальної оптимізації. Актуальність методики аналізу публічних закупівель пов'язана з вибором критеріїв вимірювання досягнутого рівня ефективності, складання системи показників, способу їхнього кількісного вираження і взаємної ув'язки. Незважаючи на те, що витрати на придбання товарів, робіт чи послуг здійснюють зростаючий вплив на економічний (фінансовий) стан підприємства, установи, немає дієвої методики здійснення аналізу публічних закупівель і на рівні підприємства (установи, організації), яка покликана досліджувати раціональне й ефективне використання державних коштів»[1].

Під час розслідування злочинів у сфері публічних закупівель одним із головних завдань є встановлення способу вчинення кримінального правопорушення, залежно від якого здійснюється кримінально-правова кваліфікація цього діяння. Зокрема, замовники конкурсних торгів учиняють злочини з використанням своїх службових повноважень так:

– закупівля товарів, робіт або послуг за завищеними цінами;
– закупівля непридатного до використання або експлуатації устаткування, товарно-матеріальних цінностей;
– оплата фактично не виконаних робіт або послуг (підписання фіктивних актів);
– здійснення держаної закупівлі без проведення процедур, передбачених законодавством (наприклад, якщо сума договору перевищує встановлену законодавством межу) тощо;
– витрата бюджетних коштів на придбання товарів, робіт або послуг в обсягах, які перевищують встановлені граничні суми витрат[2].

---

1 Виявлення та розслідування злочинів, пов'язаних із зміною ціни при проведенні державних закупівель : навч. посібник / О.В. Авраменко, І.Б. Висоцька, М.Ю. Ковальська, О.З. Мармура, О.Ф. Пасєка. Львів : ЛьвДУВС, 2018. 104 с.

2 Там само.

«Основне порушення — це змова на тендерах, за допомогою якої конкуренти, що беруть участь у змові, ефективно підвищують ціни. Така змова може набувати різних форм, але усі вони ґрунтуються на основі однієї базової: якщо учасники торгів можуть погодися не конкурувати один із одним під час торгів, то вони можуть продавати свої товари за вищі ціни. На нашу думку, одним із способів встановлення можливої змови вчинення таких злочинів є спроба виявити схеми у багатьох торгах і укладених контрактах за тривалий період часу чи у визначеній географічній зоні. Розмаїтість схем обмежена творчими здібностями учасників змови. Вивчення таких схем упродовж тривалого часу — це тільки вихідна точка для викриття та подальшого розслідування. Аналіз практики торгів і документів їхніх учасників, навіть за окремим контрактом, може показати, що пропозиції цін необґрунтовано завищені»[1].

Загалом необхідно зазначити, що система ProZorro дозволяє відносно легко виявляти потенційні та реальні порушення в сфері публічних закупівель. Так, експерти[2] виділяють такі найбільш популярні схеми обходу закупівель:

– використання спаринг-партнерів. Схема передбачає, що учасники тендеру домовляються між собою, визначають, хто має бути переможцем, а хто просто бере участь у конкурсі в ролі спаринг-партнера. Ці фірми не є справжніми конкурентами і діють узгоджено під час закупівлі. Юристи Центру протидії корупції помітили, що зазвичай такі компанії готують документацію спільно, припускаються спільних помилок, можуть мати спільні контактні дані — адреси, номери телефонів, e-mail тощо.

  Так, в одному з тендерів брали участь дві різні юридичні особи (мал. 5.2), проте при більш детальному аналізі можна помітити, що ними були подані ідентичні документи (мал. 5.3);

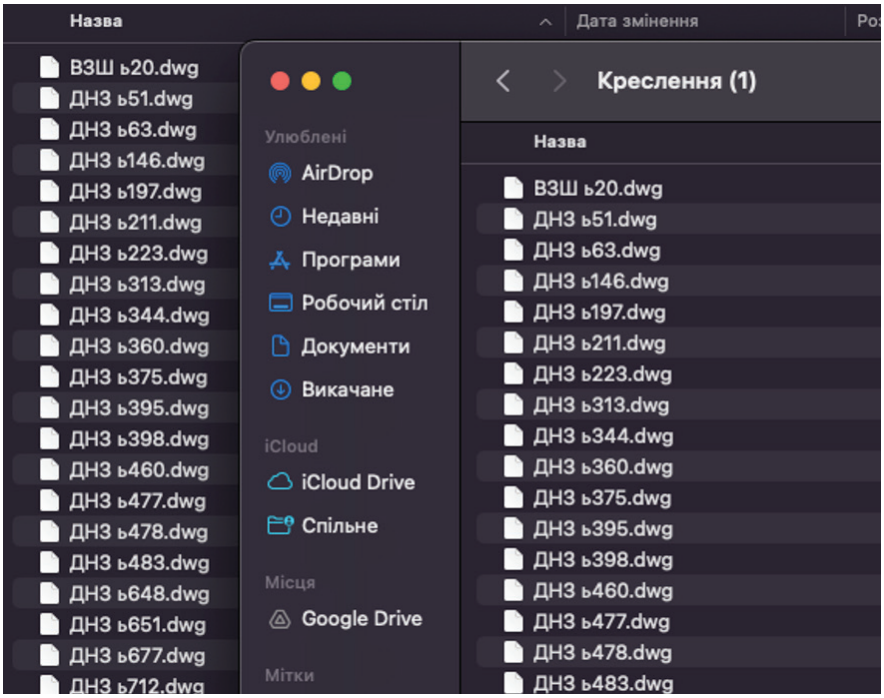
---

1 Доліновський Ю. Виявлення злочинів під час публічних закупівель у сфері охорони здоров'я. *Вісник Національного університету «Львівська політехніка». Серія : Юридичні науки*. 2017. С. 441–448.

2 ProZorro: сім схем обходу — сім методів боротьби з тим. Укрінформ : вебсайт. URL: https://www.ukrinform.ua/rubric-economy/2543102-prozorro-sim-shem-obhodu-sim-metodiv-borotbi-z-tim.html

Учасник	Документи	Рішення
ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ "[redacted] [redacted]	Документи	Допущено до аукціону Документи
ПРИВАТНЕ ПІДПРИЄМСТВО "[redacted]	Документи	Допущено до аукціону Документи

Мал. 5.2. «Різні» учасники торгів

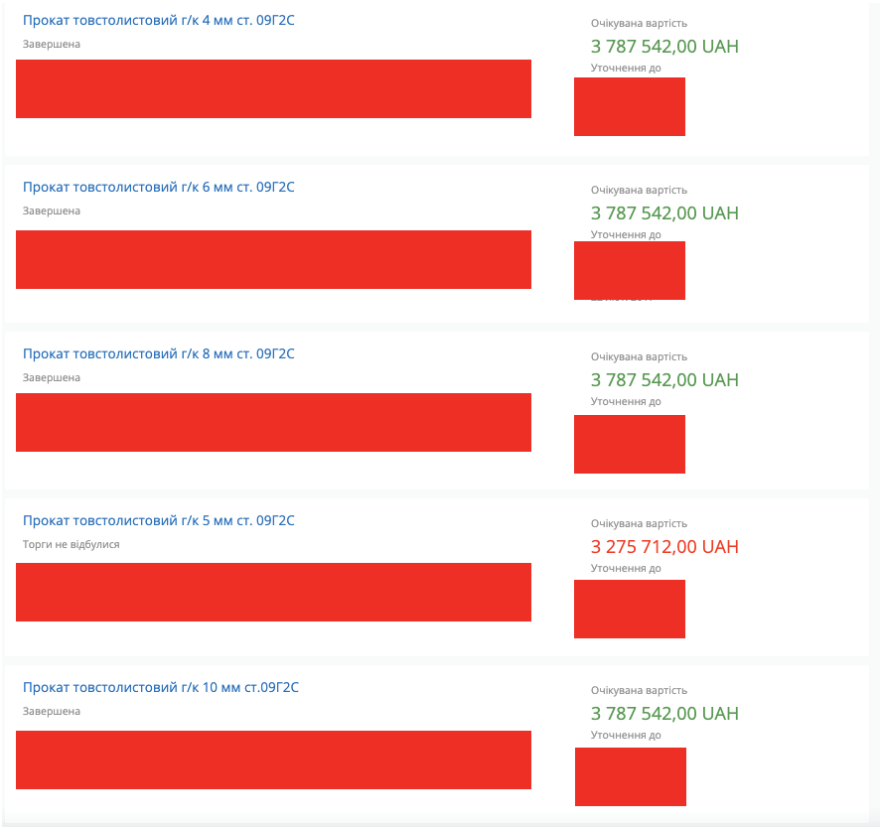


Мал. 5.3. Перелік однакових документів,
які були подані «різними» юридичними особами

– допуск компаній з «чорного списку» Антимонопольного комітету України. «Чорний список» Антимонопольного комітету (АМКУ) — це перелік підприємств, які були оштрафовані комітетом за порушення правил тендерів. З моменту внесення до цього списку компанії не мають права протягом трьох років брати участь

у торгах. Список доступний онлайн. Замовник повинен відхиляти пропозиції компаній-порушників, але трапляється, що він просто не перевіряє наявність учасників тендера в цьому «чорному списку»;

– перемога пов'язаних компаній. Пов'язані компанії належать або одній особі, або близьким родичам, членам однієї сім'ї тощо. Перевірити, чи пов'язані компанії між собою, можна в Єдиному державному реєстрі юридичних осіб. Тендерні пропозиції пов'язаних компаній замовники повинні відхиляти, але чомусь цього не роблять;
– перемога фіктивних підприємств. На тендері «раптом» може перемогти фіктивна фірма. Зазвичай у таких компаніях немає у штаті працівників, немає ніякого обладнання, вони зареєстровані за адресою масової реєстрації, інколи навіть фігурують у кримінальних провадженнях, пов'язаних з тіньовим сектором економіки;
– дроблення закупівель. Згідно із законодавством порядок проведення закупівлі вартістю вище EUR133 тис. є особливим — відбуваються так звані «європейські торги». Вони передбачають участь у тендері іноземних учасників нарівні із українськими, для цього оголошення про закупівлю публікується англійською мовою. Крім того, пропозиції всіх учасників на таких торгах проходять попередню оцінку, а термін подачі пропозицій вдвічі більший, що дає можливість учасникам підготувати необхідний пакет. Щоб удвічі скоротити термін подачі пропозицій учасниками, щоб учасники не проходили перевірку до проведення аукціону, а також щоб у тендері не взяли участь іноземні компанії, замовники «дроблять» тендер (мал. 5.4);
– дискримінації учасників. Це давня схема, в якій замовник встановлює вимоги, «заточені» під конкретного учасника торгів. Таким чином, штучно звужується коло охочих взяти участь у тендері;
– вибірковість при визначенні переможців. Замовник при однакових порушеннях учасників тендерів по-різному оцінює їх: може відхилити одних, в той час як інших, з такими ж порушенням, визнає переможцями.



Мал. 5.4. Приклад дроблення закупівель

5.4 ВИКОРИСТАННЯ OSINT ІНСТРУМЕНТІВ ПРИ РОЗСЛІДУВАННІ ФАКТІВ ШАХРАЙСТВА ТА КОРУПЦІЇ

Не менш корисним може бути OSINT при розслідуванні корупційних правопорушень або будь-яких форм фінансового чи економічного шахрайства. У даному випадку ці категорії кримінальних правопорушень поєднуються тим, що при їхньому розслідуванні можуть застосовуватися однакові відкриті джерела, адже досить часто дані правопорушення доповнюють одне одного.

Власне, складно переоцінити значення OSINT для виявлення такого роду правопорушень. «OSINT дає змогу перевіряти величезний обсяг інформації та виявляти потенційні корупційні ризики (незвичні фінансові операції, зв'язки з політично відомими особами, історія неетичної ділової практики тощо). Інструменти та методи OSINT допомагають виявляти інформацію, пов'язану з корупційними ризиками. До таких інструментів може відноситись аналіз новин, публікацій в соціальних мережах або галузевих звітів про виявлення випадків хабарництва, шахрайства, розкрадання або інших корупційних дій»[1].

Спеціалісти Bellingcat[2] на прикладах демонструють, яким чином можна використовувати відкриті джерела для виявлення прикладів корупції. До таких прикладів відносяться:

– поява політиків на публіці в дороговартісних коштовностях, годинниках тощо (які легко ідентифікувати за зображенням та визначити їхню реальну вартість, в подальшому порівнявши її з деклараціями таких осіб чи іншими даними про їхні статки);
– користування соціальними мережами дітей чи інших родичів корумпованих політиків, які хваляться своїми статками, публікуючи фотографії в дорогих авто чи будинках (наявні численні приклади, коли такі особи, особливо молодшого віку, самі в коментарях на власні дописи відповідають на питання підписників щодо місця чи часу, коли було зроблено фото, чим ще більше полегшують роботу аналітиків);
– пошук за базами даних. Наприклад, на сайті https://id.occrp.org (мал. 5.5) можна знайти посилання на сотні онлайн-реєстрів у залежності від регіону, країни або сфери, яка вас цікавить.

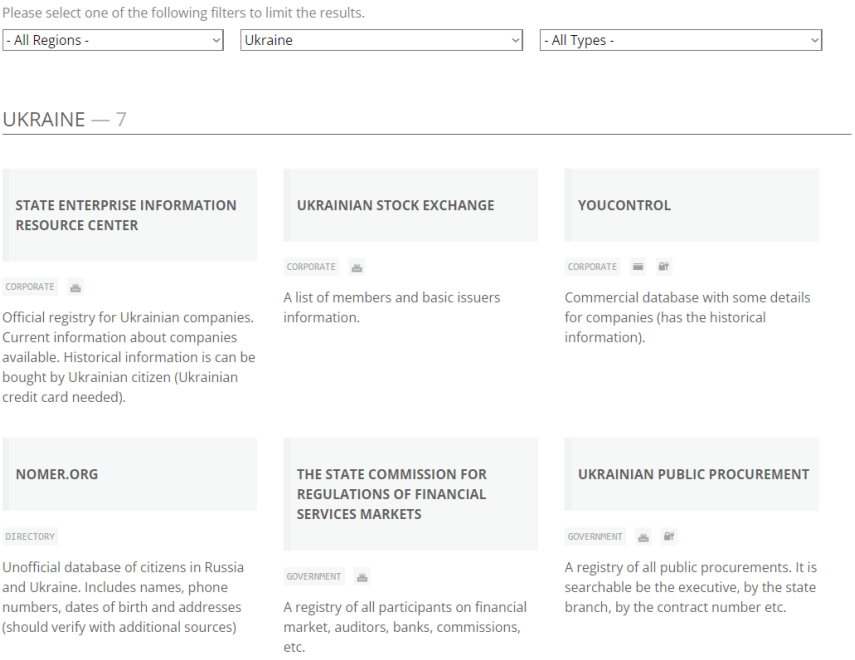
Хоча необхідно повторно наголосити, що об'єднати абсолютно всі відкриті реєстри та бази даних на одному сайті неможливо, тому OSINT аналітик не може покладатися лише на один ресурс та повинен

---

1 Khavanov A. Utilizing OSINT for Enhanced Anti-Corruption Compliance in Third-Party Due Diligence. LinkedIn : website. URL: https://www.linkedin.com/pulse/utilizing-osint-enhanced-anti-corruption-compliance-khavanov-phd-zf5jf?trk=article-ssr-frontend-pulse_more-articles_related-content-card

2 Aric Toler. How to Uncover Corruption Using Open Source Research. Bellingcat : website. URL: https://www.bellingcat.com/resources/2016/09/05/how-to-uncover-corruption-using-open-source-research/

самостійно шукати додаткові відкриті джерела, які можуть допомогти йому в розслідуванні.



Мал. 5.5. Приклад сторінки OCCRP ID

Наприклад, в даному випадку не можна забувати про звичайні пошукові сервіси, які можуть надати навіть більше інформації, адже корупційні правопорушення досить часто стосуються осіб публічних, відомості про яких можна зібрати з новин чи статей у Вікіпедії. «Розслідування корупції може бути ефективним, коли намагаються поєднати докази з різних джерел. Яхта може привести вас до записів компанії та суднових реєстрів, а право власності можна перевірити за допомогою соціальних мереж, таких як Instagram. Потім інформацію з соціальних мереж можна перевірити за допомогою геолокації та спробувати знайти іншу контекстну інформацію про час і місце, де було зроблено фото.

Якщо хтось подорожував узбережжям Італії, щоб сісти на борт яхти, то чи міг він також відвідати місто, яке знаходиться неподалік, в якому проходило якесь свято? Вивчайте людей, які напряму не пов'язані з особою, яка вас цікавить, але все одно знаходяться в сфері його впливу чи інтересів (члени екіпажу, обслуговуючий персонал тощо). Особливо звертайте увагу на соціальні мережі»[1].

Експерти, аналізуючи можливості OSINT при розслідуванні потенційних корупційних дій представниками юридичних осіб, радять аналізувати, крім іншого, структуру відповідної юридичної особи та вивчати аномалії в грошових переказах. Так, при аналізі структури юридичної особи та бенефіціарів бажано звертати увагу на наступні позиції:

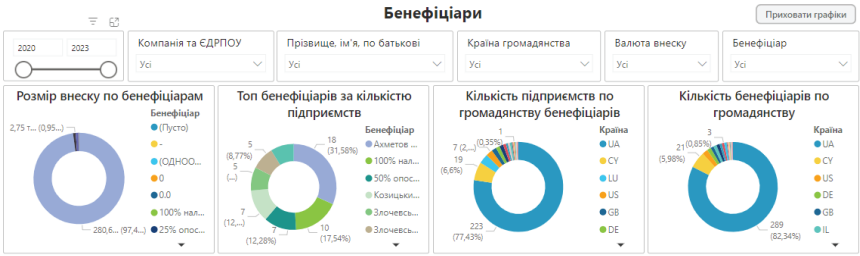
1. Встановлення права власності та специфіки корпоративної структури. Аналіз права власності та корпоративної структури — це процес належної перевірки, метою якого є розуміння ієрархії юридичної особи, визначення ключових зацікавлених осіб тощо.

2. Ідентифікація кінцевих бенефіціарів. Кінцеві бенефіціари — це особи, які в підсумку володіють або контролюють компанію.

Відповідно до ЗУ «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення», кінцевий бенефіціарний власник — будь-яка фізична особа, яка здійснює вирішальний вплив (контроль) на діяльність клієнта та/або фізичну особу, від імені якої проводиться фінансова операція. Кінцевим бенефіціарним власником є: для юридичних осіб — будь-яка фізична особа, яка здійснює вирішальний вплив на діяльність юридичної особи (в тому числі через ланцюг контролю/володіння); для трастів, утворених відповідно до законодавства країни їхнього утворення, — засновник, довірчий власник, захисник (за наявності), вигодоодержувач (вигодонабувач) або група вигодоодержувачів (вигодонабувачів), а також будь-яка інша фізична особа, яка здійснює вирішальний вплив на діяльність трасту (в тому числі через ланцюг контролю/володіння);

[1] Aric Toler. How to Uncover Corruption Using Open Source Research. Bellingcat : website. URL: https://www.bellingcat.com/resources/2016/09/05/how-to-uncover-corruption-using-open-source-research/

для інших подібних правових утворень — особа, яка має статус, еквівалентний або аналогічний особам, зазначеним для трастів.



Мал. 5.6. Статистична інформація про бенефіціарів
на Порталі даних видобувної галузі України
(https://eiti.gov.ua/upravlinnya-vidobuvnim-sektorom/beneficiari/)

Розуміючи доцільність визначення бенефіціарів для забезпечення реального контролю за сферою взаємовідносин з приватним бізнесом, Кабінетом Міністрів України була розроблена Методологія визначення юридичною особою кінцевого бенефіціарного власника, де в якості етапів визначення юридичною особою кінцевого бенефіціарного власника або встановлення факту його відсутності є такі: 1) дослідження ознак, характеру та міри (рівня, ступеня, частки) прямого вирішального впливу на діяльність юридичної особи шляхом безпосереднього володіння фізичною особою ключовою часткою статутного (складеного) капіталу або прав голосу юридичної особи; 2) дослідження ознак, характеру (вигоди, інтересу) та міри (рівня, ступеня, частки) непрямого вирішального впливу (контролю) на діяльність юридичної особи шляхом володіння фізичною особою ключовою часткою статутного (складеного) капіталу або прав голосу юридичної особи через пов'язаних фізичних чи юридичних осіб, трастів або інших подібних правових утворень чи здійснення вирішального впливу на діяльність юридичної особи шляхом реалізації права контролю, володіння, користування або розпорядження всіма активами чи їхньою часткою, права отримання доходів від діяльності юридичної особи, трасту або іншого подібного правового

утворення, права вирішального впливу на формування складу, результати голосування органів управління, а також вчинення правочинів, які дають можливість визначати основні умови господарської діяльності юридичної особи або діяльності трасту або іншого подібного правового утворення, ухвалювати обов'язкові до виконання рішення, що мають вирішальний вплив на діяльність юридичної особи, трасту або іншого подібного правового утворення незалежно від формального володіння; 3) дослідження інформації про засновників, довірчих власників, захисників (у разі наявності), вигодоодержувачів (вигодонабувачів) або групу вигодоодержувачів (вигодонабувачів), а також про будь-яких інших фізичних осіб, які здійснюють вирішальний вплив на діяльність трасту або іншого подібного правового утворення (зокрема через ланцюг контролю/володіння), у випадку їхньої наявності у структурі власності юридичної особи та/або у випадку утворення юридичної особи — правового утворення, подібного до трасту. Щодо трастів та інших подібних правових утворень, вигодоодержувачі (вигодонабувачі) яких характеризуються певними ознаками або класом, встановлюється інформація про таких вигодоодержувачів (вигодонабувачів), яка б надала можливість встановити їхню особу в момент виплати чи реалізації ними належних їм прав; 4) здійснення систематизації, узагальнення, аналізу та документування інформації, отриманої під час дій, визначених підпунктами 1–3 цього пункту; 5) проведення моніторингу та актуалізації (оновлення) інформації про кінцевих бенефіціарних власників.

Проте ще задовго до того, як було розроблено цю методологію, інформація про бенефіціарного власника почала вноситись до Єдиного державного реєстру юридичних осіб, фізичних осіб — підприємців та громадських формувань та доступна в онлайн-режимі на офіційному вебсайті Мін'юсту і Єдиному державному порталі відкритих даних. На цих же ресурсах міститься публічна інформація про учасників (засновників) усіх юридичних осіб, зареєстрованих в Україні, розмір статутного капіталу таких юридичних осіб та відсоток часток у статутному капіталі їхніх учасників (засновників).

Крім того, у 2017 р. Україна зробила важливий крок на шляху підвищення прозорості — приєдналася до Глобального реєстру бенефіціарних власників та стала першою державою, що офіційно заявила

про готовність надати дані про бенефіціарних власників для реєстру[1]. На даний момент така інтеграція ще не відбулася, проте вже можна скористуватися Глобальним реєстром бенефіціарних власників (https://register.openownership.org) для того, щоб перевірити, чи дійсно особа, яка цікавить OSINT аналітика, є бенефіціарним власником в інших країнах.

3. Перевірка моделей володіння акціями, тобто ретельна перевірка загальнодоступної звітності, нормативно-правових документів і інформації про участь на фондових біржах тощо.

4. Афілійовані та пов'язані організації. За допомогою OSINT інструментів можна проводити розслідування щодо пов'язаних юридичних чи фізичних осіб, які були замішані в корупційних скандалах чи неетичній діловій практиці. Розуміння таких зв'язків надасть кращий контекст для оцінки корупційних ризиків.

5. Ідентифікація фіктивних компаній. OSINT інструменти допомагають ідентифікувати потенційні фіктивні компанії або організації з неоднозначною внутрішньою структурою (наприклад, замала кількість співробітників, дивна адреса реєстрації юридичної особи тощо). Фіктивні юридичні особи часто використовуються саме задля приховування корупційних кримінальних правопорушень, що також має бути враховано OSINT аналітиками.

5.5 ВИКОРИСТАННЯ OSINT ІНСТРУМЕНТІВ ПРИ РОЗСЛІДУВАННІ ФАКТІВ ЛЕГАЛІЗАЦІЇ МАЙНА, ОДЕРЖАНОГО ЗЛОЧИННИМ ШЛЯХОМ

Не менш корисним може бути проведення OSINT розслідування при розкритті злочинів, пов'язаних з відмиванням грошей. Насамперед необхідно наголосити, що в українському законодавстві відсутній термін «відмивання грошей», але в якості його аналога застосовується подібний термін «легалізація (відмивання) майна, одержаного злочинним шляхом». Так, відповідно до ст. 209 КК України, під даним

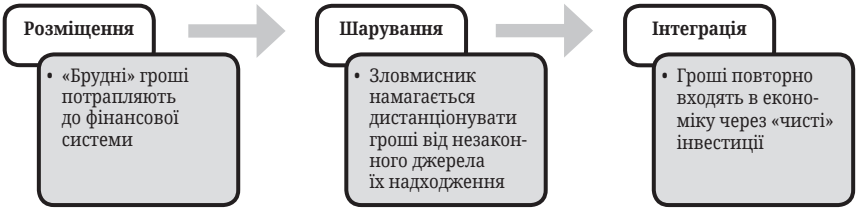
[1] БЕНЕФІЦІАРИ. Портал даних видобувної галузі України : вебсайт. URL: https://eiti.gov.ua/upravlinnya-vidobuvnim-sektorom/beneficiari/

складом злочину розуміється «набуття, володіння, використання, розпорядження майном, щодо якого фактичні обставини свідчать про його одержання злочинним шляхом, у тому числі здійснення фінансової операції, вчинення правочину з таким майном, або переміщення, зміна форми (перетворення) такого майна, або вчинення дій, спрямованих на приховування, маскування походження такого майна або володіння ним, права на таке майно, джерела його походження, місцезнаходження, якщо ці діяння вчинені особою, яка знала або повинна була знати, що таке майно прямо чи опосередковано, повністю чи частково одержано злочинним шляхом». Відповідно до ст. 5 ЗУ «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення», до легалізації (відмивання) доходів, одержаних злочинним шляхом, належать будь-які дії, пов'язані із вчиненням фінансової операції чи правочину з доходами, одержаними злочинним шляхом, а також вчиненням дій, спрямованих на приховання чи маскування незаконного походження таких доходів, чи володіння ними, прав на такі доходи, джерел їхнього походження, місцезнаходження, переміщення, зміну їхньої форми (перетворення), а так само набуттям, володінням або використанням доходів, одержаних злочинним шляхом.

Загалом, аналізуючи дане питання у зарубіжній літературі, можна помітити, що розуміння самої концепції легалізації (відмивання) доходів чи будь-якого іншого майна є відносно стандартизованим, що означає, що для питань, які є релевантними для даного підручника, можна використовувати обидва терміни. Проте в даному аспекті необхідно підкреслити відмінності між такими термінами, як відмивання грошей (Money Laundering) та боротьба з відмиванням грошей (Anti-Money Laundering — AML).

Так, незаконна діяльність (контрабанда, хабарництво, організована злочинність тощо) генерує великі суми незаконних грошей. Однак зловмисники не можуть витрачати ці гроші, не викликаючи підозр у фінансових установ. Відповідно, в даному випадку необхідно здійснити відмивання грошей, щоб зробити їх «чистими», які не будуть викликати підозр. Для відмивання грошей використовується кілька методів, але загалом всі вони передбачають спрямування незаконної грошової

маси в легальний бізнес. Це створює враження, що гроші були зароблені законно. Зазвичай така схема передбачає три етапи: розміщення, шарування та інтеграція (мал. 5.7). Наприклад, злочинець, який незаконно продає наркотичні засоби, купляє автомийку. На стадії розміщення злочинець вкладає незаконні гроші у власний бізнес. Розшарування — це створення враження, що його бізнес дуже успішний шляхом генерації фіктивних рахунків-фактур чи звітів про продаж. Нарешті, інтеграція є кінцевим результатом, ілюзією «чистого» доходу.



Мал. 5.7. Етапи легалізації доходів, отриманих незаконним шляхом

Боротьба з відмиванням грошей (AML) відноситься ж до набору правил і норм, спрямованих на виявлення фактів відмивання грошей. Фінансові установи (страхові компанії, банки тощо) зобов'язані здійснювати ретельний моніторинг будь-яких тіньових угод. Наприклад, якщо хтось раптово вносить велику суму готівки, не пояснюючи джерело надходження таких грошей, то це може викликати певні сумніви.

Зазвичай заходи протидії відмиванню коштів впроваджуються до того, як установи встановлять відносини з клієнтами. Ці процеси включають перевірку «Знай свого клієнта» (Know-Your-Customer — KYC), ретельне вивчення минулих даних і певний рівень обачності. Фінансовий аудит допомагає визначити, чи залучений потенційний клієнт до відмивання грошей[1].

Виділяють наступні складнощі у боротьбі з відмиванням грошей:

1. Неякісний фінансовий моніторинг.

[1] OSINT in Anti-Money Laundering (AML) Investigations : Unmasking Financial Shadows. Social Links : website. URL: https://blog.sociallinks.io/osint-in-anti-money-laundering-aml-investigations-unmasking-financial-shadows/

Якщо фінансові установи неякісно проводять фінансовий моніторинг, вони можуть випадково обслуговувати клієнтів, метою яких є відмивання грошей. Такі помилки можуть призвести до суттєвої шкоди діловій репутації чи великих штрафів. Наприклад, у 2022 році Міністерство юстиції США оштрафувало естонську філію Danske Bank на 2 мільярди доларів. За словами прокурорів, програма протидії відмиванню грошей банку була недостатньо якісною, що дозволило використовувати дану фінансову установу в незаконних цілях.

2. Технологічний розвиток.

Коли з'являється нова технологія, як правило, саме зловмисники першими знаходять способи, як можна такі технології використовувати для власної вигоди. Не є винятком у даному випадку і відмивання грошей. Наприклад, у популярній відеогрі «Fortnite» шахраї купували ігрову валюту за рахунок незаконного прибутку, а в подальшому перепродавали профілі користувачів на аукціонах, щоб відмити такі гроші.

Крім того, відносно недавно з'явилися токени NFT. Ці цифрові активи набули популярності приблизно у 2021 році та стали новим інструментом для відмивання грошей. До кінця 2021 року платформи NFT отримали 1,4 мільйона доларів із гаманців, пов'язаних із країнами, які перебувають під санкціями. Це стає можливим завдяки тому, що платформи, на яких продаються токени, не проходять перевірку «Знай свого клієнта» (KYC). Через недостатньо чіткі правила шахраї можуть володіти кількома обліковими записами та продавати токени самим собі, щоб підвищувати ціну («відмивання торгівлею»).

3. Труднощі у відстеженні коштів терористів.

Терористичні угруповання використовують різні методи, щоб приховати джерело, переміщення та призначення коштів. По суті, відмивання грошей тісно пов'язане з екстремістською діяльністю. Такі групи можуть переказувати гроші через кордони, не викликаючи підозр, використовуючи благодійні організації, беручи участь у відмиванні грошей через торгівлю тощо.

Хоча такі організації, як, наприклад, Група розробки фінансових заходів боротьби з відмиванням грошей (Financial Action Task Force — FATF), активно розслідують і намагаються зробити більш жорсткими

правила боротьби з відмиванням коштів, щоб припинити фінансування тероризму, в цьому процесі перемогти фактично неможливо. Згідно із заявою FATF, незважаючи на зусилля робочої групи, екстремістські організації, такі як ІДІЛ і Аль-Каїда, отримують постійне фінансування за рахунок пожертвувань своїх прихильників і незаконних схем відмивання грошей, що підкреслює значення боротьби з відмиванням грошей.

4. Dark Net.

Dark Net становить серйозну загрозу саме через високий ступінь анонімності, який він пропонує своїм користувачам. Транзакції зазвичай відбуваються через безпечні канали та псевдоніми, що ускладнює ідентифікацію залучених до цього процесу осіб.

5. Складність платіжних потоків.

Цифрові фінанси здійснили революцію в сфері обміну грошей, що призвело до різкого зростання популярності електронної комерції. Однак разом із цим з'явилися нові виклики. Фінансові установи зіткнулися з труднощами при дослідженні сучасних методів оплати (наприклад, криптовалюта). Так, популярним методом легалізації незаконних коштів є послуги криптомікшерів, які стягують комісію за розбиття переказу на тисячі (іноді мільйони) менших транзакцій для шифрування їхнього походження[1].

При аналізі потенційних ризиків відмивання грошей необхідно, на думку авторів Fraud Examination 2012, звертати увагу на компанії, які:

- створені без очевидної комерційної мети;
- отримують великі суми грошей з-за кордону, які співпадають з сумами виплати компаній з інших країн;
- купують товари та послуги за цінами, значно вищими або нижчими від ринкових;
- виплачують заробітну плату своїм працівникам, яка не відповідає середній заробітній платі у відповідному бізнес-секторі;
- мають відносно високий оборот коштів у порівнянні з масштабом свого бізнесу;

[1] OSINT in Anti-Money Laundering (AML) Investigations : Unmasking Financial Shadows. Social Links : website. URL: https://blog.sociallinks.io/osint-in-anti-money-laundering-aml-investigations-unmasking-financial-shadows/

– мають надмірно складну бізнес-структуру, яка в даній ситуації є нелогічною[1].

Інструменти OSINT розвідки допомагають аналітикам виявляти такі факти відмивання грошей. Так, до найбільш популярних методів ідентифікації відносять наступні:

1. Цифрові сліди.

Цифрові сліди є невід'ємною частиною інтернету, де аналітики можуть відстежити фактично будь-кого. Інструменти OSINT можуть ідентифікувати підключення до облікових записів у соціальних мережах, геолокаційні дані з тегами та списки друзів і партнерів за іменами, адресами електронної пошти, номерами телефонів та іншими відкритими даними. Ці відомості дозволяють аналітикам створювати профіль дій суб'єкта, що може дозволити ідентифікувати факт відмивання грошей.

2. Сканування месенджерів.

Злочинці, які беруть участь у схемах відмивання грошей, часто використовують такий месенджер, як Telegram, через його анонімність. Однак, аналіз месенджерів за допомогою інструментів з відкритих джерел дозволяє розширити сферу розслідування. Цього можна досягти за допомогою пошуку за певними ключовими словами, псевдонімом, номером телефону або ідентифікатором Telegram; виявлення посилань на закриті групи; аналізу діяльності адміністраторів; або доступу до видаленого вмісту. Усі отримані дані можуть допомогти розкриттю схем відмивання грошей.

3. Відстеження транзакцій.

Неважливо, наскільки складними є грошові перекази, адже всі їх можна відслідкувати тим чи іншим способом. OSINT дозволяє аналітикам відслідковувати такі перекази шляхом аналізу перехресних посилань на публічні записи, фінансові вебсайти та записи внутрішніх організацій. Крім того, OSINT може стати життєво важливим для виявлення неоднозначних переказів коштів і порушень, візуалізації ключової інформації, яка може виявити неочевидні зв'язки між зловмисними обліковими записами та особами.

[1] W. Steve Albrecht, Chad O. Albrecht, Conan C. Albrecht, Mark F. Zimbelman. Fraud Examination. Cengage Learning, 2015. 696 p.

4. Моніторинг тіньової мережі.

Жодне шифрування не може ефективно приховати злочинну діяльність. OSINT інструменти дозволяють слідчим відстежувати схеми відмивання грошей через Dark Net, скануючи джерела даних, підпільні ринки та форуми для збору корисної інформації проти зловмисників. Крім того, можна деанонімізувати приховані профілі шляхом перехресного посилання на інформацію з публікацій в поверхневому та тіньовому інтернеті (навіть видалених) і проводити пошук на основі імен користувачів і адрес криптогаманців, що створює можливості для отримання корисної інформації.

5. Відображення корпоративної мережі.

Розуміння того, як конкретні особи пов'язані з компаніями, може стати важливою інформацією в процесі боротьби з відмиванням грошей. OSINT дозволяє слідчим візуалізувати організаційну структуру компаній шляхом сканування корпоративних реєстрів. У багатьох випадках таке розуміння може стати надзвичайно цінним, оскільки OSINT інструменти дозволяють об'єднувати бази даних санкцій у процес дослідження та аналізу того, чи є якась особа політично відомою, що дозволяє виявляти приховані зв'язки[1].

[1] OSINT in Anti-Money Laundering (AML) Investigations : Unmasking Financial Shadows. Social Links : website. URL: https://blog.sociallinks.io/osint-in-anti-money-laundering-aml-investigations-unmasking-financial-shadows/

Тема 6

ОСОБЛИВОСТІ OSINT РОЗСЛІДУВАНЬ ВОЄННИХ ЗЛОЧИНІВ

6.1 ПОНЯТТЯ ВОЄННИХ ЗЛОЧИНІВ

Перш ніж розпочати аналіз способів використання OSINT інструментів при розслідуванні воєнних злочинів, необхідно встановити, які саме правопорушення до них відносяться. Офіційно в законодавстві України поняття «воєнні злочини» не існує, у зв'язку з чим дану категорію кримінальних правопорушень досить часто плутають з іншими — військовими злочинами. Військові злочини — це насамперед кримінальні правопорушення, направлені проти встановленого порядку несення військової служби, які передбачені Розділом 19 КК України. Так, відповідно до ст. 401 КК України, військовими кримінальними правопорушеннями визнаються кримінальні правопорушення проти встановленого законодавством порядку несення або проходження військової служби, вчинені військовослужбовцями, а також військовозобов'язаними та резервістами під час проходження зборів. Таку відповідальність несуть військовослужбовці Збройних сил України, Служби безпеки України, Державної прикордонної служби України, Національної гвардії України та інших військових формувань, утворених відповідно до законів України, Державної спеціальної служби транспорту, Державної служби спеціального зв'язку та захисту інформації України, а також інші особи, визначені законом.

Воєнні ж злочини — це порушення законів та звичаїв війни, які визначаються міжнародним кримінальним правом, «свідоме, грубе,

порушення законів та звичаїв війни, за який винуватці (учасники бойових дій та особи, які віддають їм накази) несуть кримінальну відповідальність, визначену рішенням міжнародних воєнних трибуналів»[1].

Так, відповідно до Римського Статуту Міжнародного Кримінального Суду під воєнними злочинами розуміються

1) грубі порушення Женевських конвенцій від 12 серпня 1949 року, а саме будь-яке з таких діянь проти осіб або майна, що охороняються згідно з положеннями відповідної Женевської конвенції:
   – умисне вбивство;
   – катування або нелюдське поводження, у тому числі біологічні експерименти;
   – умисне заподіяння сильних страждань або тяжких тілесних ушкоджень чи шкоди здоров'ю;
   – широкомасштабне знищення і привласнення майна, що не викликане військовою необхідністю і вчинене незаконно та безглуздо;
   – примушення військовополоненого або іншої особи, що перебуває під захистом, до служби у збройних силах ворожої держави;
   – умисне позбавлення військовополоненого або іншої особи, що перебуває під захистом, права на справедливий і звичайний суд;
   – незаконна депортація або переміщення чи незаконне позбавлення волі;
   – взяття заручників;
2) інші серйозні порушення законів і звичаїв, що застосовуються в міжнародних збройних конфліктах у встановлених рамках міжнародного права, а саме будь-яке з таких діянь:
   – умисне спрямування нападів на цивільне населення як таке або на окремих цивільних осіб, що не беруть безпосередньої участі у воєнних діях;
   – умисне спрямування нападів на цивільні об'єкти, тобто об'єкти, що не є військовими цілями;

[1] Воєнні злочини та їх документування. Безоплатна правнича допомога : вебсайт. URL: https://legalaid.gov.ua/publikatsiyi/voyenni-zlochyny-ta-yih-dokumentuvannya/

- умисне спрямування нападів на персонал, об'єкти, матеріали, підрозділи або транспортні засоби, задіяні в наданні гуманітарної допомоги чи в місії з підтримання миру відповідно до Статуту Організації Об'єднаних Націй, доки вони мають право на захист, яким користуються цивільні особи або цивільні об'єкти згідно з міжнародним правом збройних конфліктів;
- умисне вчинення нападу з усвідомленням того, що такий напад призведе до випадкової загибелі чи поранення цивільних осіб або заподіє шкоди цивільним об'єктам чи масштабної, довготривалої та серйозної шкоди навколишньому природному середовищу, яка буде явно надмірною в порівнянні з конкретною та безпосередньо очікуваною загальною військовою перевагою;
- напад на незахищені й такі, що не є військовими цілями, міста, села, помешкання або будівлі чи їхній обстріл із застосуванням будь-яких засобів;
- вбивство або поранення комбатанта, який, склавши зброю чи не маючи більше засобів захисту, беззастережно здався;
- неналежне використання прапора парламентера, прапора чи військових знаків розрізнення та форми ворога або Організації Об'єднаних Націй, а також розпізнавальних емблем, встановлених Женевськими конвенціями, наслідком чого є смерть або заподіяння особі серйозних ушкоджень;
- переміщення, прямо чи опосередковано, окупаційною державою частини її власного цивільного населення на окуповану нею територію чи депортація або переміщення всього або частини населення окупованої території у межах чи за межі цієї території;
- умисне спрямування нападів на будівлі, призначені для релігійних, освітніх, мистецьких, наукових чи благодійних цілей, на історичні пам'ятники, госпіталі та місця зосередження хворих і поранених за умови, що вони не є військовими цілями;
- заподіяння особам, які перебувають під владою ворожої сторони, фізичного каліцтва або здійснення над ними медичних чи наукових експериментів будь-якого характеру, які не обґрунтовані необхідністю медичного, стоматологічного або лікарняного лікування відповідної особи і здійснюються не в її

інтересах та які призводять до смерті або серйозно загрожують здоров'ю такої особи чи осіб;
- віроломне вбивство або поранення осіб, що належать до ворожої нації чи армії;
- заява про те, що пощади не буде;
- знищення або захоплення майна ворога, крім випадків, коли таке знищення або захоплення настійно вимагаються воєнною необхідністю;
- оголошення скасованими, призупиненими або недопустимими в суді прав і позовів громадян ворожої сторони;
- примушення громадян ворожої сторони до участі у воєнних діях проти їхньої власної країни, навіть якщо вони перебували на службі воюючої сторони до початку війни;
- розграбування міста або населеного пункту, навіть якщо його захоплено штурмом;
- застосування отрути або отруєної зброї;
- застосування задушливих, отруйних або інших газів та всіх аналогічних рідин, матеріалів чи засобів;
- застосування куль, що легко розгортаються або сплющуються в тілі людини, таких, як кулі з твердою оболонкою, яка не повністю покриває осердя або має надрізи;
- застосування зброї, боєприпасів і матеріалів, а також методів ведення війни такого характеру, які спричиняють надмірні ушкодження чи непотрібні страждання або які за своєю суттю є невибірковими в порушення норм міжнародного права збройних конфліктів, за умови, що така зброя, такі боєприпаси і матеріали та методи ведення війни є предметом всеохоплюючої заборони і включені до додатка до цього Статуту шляхом внесення поправки згідно з відповідними положеннями, викладеними у статтях 121 і 123;
- посягання на людську гідність, зокрема образливе і принизливе поводження;
- зґвалтування, сексуальне рабство, примушення до проституції, примусова вагітність, як вона визначена в пункті 2 (f) статті 7, примусова стерилізація чи будь-яка інша форма сексуального

насильства, яка також становить грубе порушення Женевських конвенцій;
- використання присутності цивільної особи або іншої особи, яка перебуває під захистом, для захисту певних пунктів, районів або збройних сил від військових операцій;
- умисне спрямування нападів на будівлі, матеріали, медичні установи й транспортні засоби, а також на персонал, що використовує згідно з міжнародним правом розпізнавальні емблеми, передбачені Женевськими конвенціями;
- умисне використання голодування цивільного населення як методу ведення війни шляхом позбавлення його предметів, необхідних для виживання, у тому числі умисне створення перешкод для надання допомоги, як це передбачено відповідно до Женевських конвенцій;
- набір або вербування дітей віком до п'ятнадцяти років до складу національних збройних сил або використання їх для активної участі в бойових діях;

3) інші серйозні порушення законів і звичаїв, що застосовуються у збройних конфліктах неміжнародного характеру в установлених рамках міжнародного права, а саме будь-яке з таких діянь:
- умисне спрямування нападів на цивільне населення як таке або на окремих цивільних осіб, які не беруть безпосередньої участі у бойових діях;
- умисне спрямування нападів на будівлі, матеріали, медичні установи й транспортні засоби, а також персонал, що використовує згідно з міжнародним правом розпізнавальні емблеми, передбачені Женевськими конвенціями;
- умисне спрямування нападів на персонал, об'єкти, матеріали, підрозділи або транспортні засоби, задіяні в наданні гуманітарної допомоги чи в місії з підтримання миру відповідно до Статуту Організації Об'єднаних Націй, доки вони мають право на захист, яким користуються цивільні особи або цивільні об'єкти згідно з міжнародним правом збройних конфліктів;
- умисне спрямування нападів на будівлі, призначені для релігійних, освітніх, мистецьких, наукових чи благодійних цілей, на

історичні пам'ятники, госпіталі та місця зосередження хворих і поранених за умови, що вони не є військовими цілями;
- розграбування міста або населеного пункту, навіть якщо його захоплено штурмом;
- зґвалтування, сексуальне рабство, примушення до проституції, примусова вагітність, як вона визначена в пункті 2 (f) статті 7, примусова стерилізація та будь-яка інша форма сексуального насильства, яка також становить грубе порушення статті 3, спільної для чотирьох Женевських конвенцій;
- набір або вербування дітей віком до п'ятнадцятих років до складу збройних сил чи груп або використання їх для активної участі в бойових діях;
- віддання розпоряджень про переміщення цивільного населення з причин, пов'язаних з конфліктом, якщо тільки цього не вимагають міркування безпеки відповідного цивільного населення або настійна необхідність військового характеру;
- віроломне вбивство або поранення комбатанта ворога;
- заява про те, що пощади не буде;
- заподіяння особам, які перебувають під владою іншої сторони конфлікту, фізичного каліцтва або здійснення над ними медичних чи наукових експериментів будь-якого характеру, що не обґрунтовані необхідністю медичного, стоматологічного або лікарняного лікування відповідної особи і здійснюються не в її інтересах та які призводять до смерті або серйозно загрожують здоров'ю такої особи чи осіб;
- знищення або захоплення майна ворога, крім випадків, коли таке знищення або захоплення настійно вимагаються обставинами конфлікту, та інші воєнні злочини, які передбачені міжнародним гуманітарним правом.

Якщо вести мову про законодавство України, то тут насамперед необхідно звернути увагу на ст. 438 КК України («Порушення законів та звичаїв війни»), а також інші подібні кримінальні правопорушення, наприклад ст. 432 («Мародерство»), ст. 433 («Насильство над населенням у районі воєнних дій») тощо. Особливістю даних кримінальних правопорушень є необхідність застосування при кваліфікації відповідних

злочинних діянь також норм міжнародного гуманітарного права, тому OSINT аналітик також має володіти хоча б базовими знаннями у сфері МГП для правильної оцінки такого роду правопорушень.

6.2 ВИКОРИСТАННЯ OSINT ІНСТРУМЕНТАРІЮ ПРИ РОЗСЛІДУВАННІ ВОЄННИХ ЗЛОЧИНІВ

Напевно, можливості OSINT найяскравіше проявляються саме в процесі ідентифікації та розслідування воєнних злочинів, адже значна кількість порушень МГП, які в подальшому кваліфікуються як воєнні злочини, зачіпають невизначене або дуже широке коло осіб, а їхні наслідки дуже складно приховати. При цьому необхідно зазначити, що не існує окремих спеціальних методів розслідування з використанням відкритих джерел, які б стосувалися виключно воєнних злочинів. У процесі розслідування такого роду правопорушень будуть корисними всі раніше здобуті знання та навички, які в тій чи іншій мірі дозволяють користуватися відкритими джерелами задля, наприклад, ідентифікації місцевості чи осіб, які зображені на фото чи фігурують у відео.

Власне, розрізняють пасивні та активні методи проведення розслідування воєнних злочинів з допомогою відкритих джерел.

1. Пасивні методи дозволяють отримувати загальну інформацію про об'єкт. Вона збирається вручну або за допомогою спеціальних сервісів та інструментів, що спрощують збір, систематизацію та аналіз даних. Наприклад, програм для парсингу сайтів. По суті, пасивною веброзвідкою можуть займатися абсолютно всі, хто має комп'ютер і доступ в інтернет, — від простого користувача до співробітника аналітичного або маркетингового відділу.

До пасивних методів можна віднести:

- збирання інформації (у тому числі за фотографіями) з відкритих пошукових систем;
- аналіз активності користувача в соціальних мережах і блогах, на форумах, інших віртуальних платформах;
- пошук відкритих персональних даних користувачів у соціальних мережах, месенджерах;

– перегляд збережених копій сайтів у пошукових системах, інтернет-архіві;
– отримання геолокаційних даних за допомогою загальнодоступних ресурсів, таких як Google Maps.

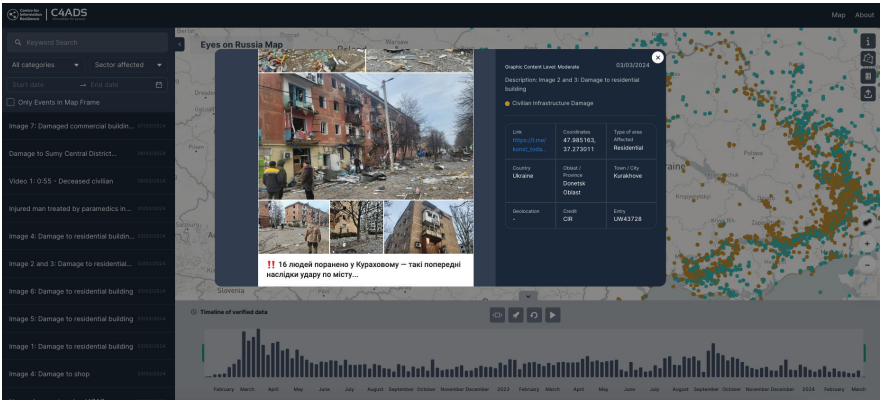
2. Активні методи. Такі методи мають на увазі безпосередній вплив аналітика на досліджуваний об'єкт, використання спеціалізованих засобів отримання даних або здійснення дій, що вимагають певних зусиль, наприклад:

– збір даних на закритих ресурсах, доступ до яких можливий лише за передплатою;
– застосування спеціалізованих сервісів та програм, які активно впливають на досліджуваний об'єкт — наприклад, автоматично реєструються на сайті;
– використання сервісів, що сканують програми, файли чи сайти на наявність шкідливого коду;
– створення підроблених вебресурсів, каналів у месенджерах, які збирають дані користувачів, конфіденційні чи секретні відомості.

У логіці OSINT пасивні методи, спрямовані на збір загальної інформації з доступних джерел, передують застосуванню активних способів, призначених для збору конкретних даних про об'єкт[1].

Вже зараз можна оцінити масштаби OSINT розслідувань воєнних злочинів, вчинених на території України, що підтверджує значення розслідування з відкритих джерел. Більше того, на даний момент існують ресурси, на яких систематизується такого роду інформація. Наприклад, незалежна некомерційна організація Центр інформаційної стійкості (The Centre for Information Resilience — CIR) у січні 2022 року запустила проєкт Eyes on Russia (https://eyesonrussia.org) для збору та перевірки відео, фотографій, супутникових зображень тощо, які пов'язані з вторгненням рф в Україну. «Відтоді проєкт Eyes on Russia координує дослідження ширшої спільноти OSINT (Open Source Intelligence), включаючи Bellingcat і GeoConfirmed, за підтримки Advance Democracy, Inc. База даних перевіреної інформації є колективним продуктом цієї спільноти».

[1] Як OSINT впливає на війну в Україні? Itedu : вебсайт. URL: https://itedu.center/ua/blog/articles/osint/



Мал. 6.1. Eyes on Russia

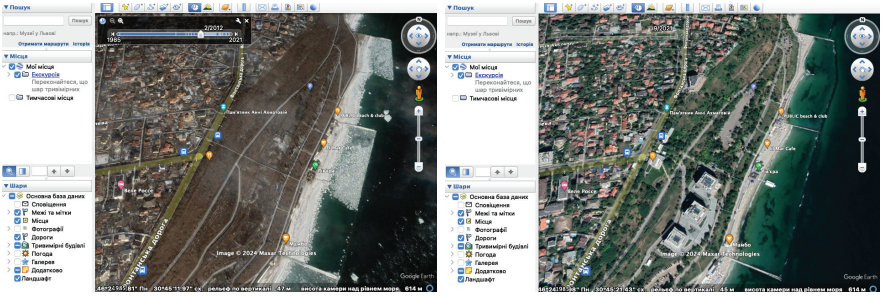
Власне, при розслідуванні воєнних злочинів застосовуються аналогічні або подібні інструменти, які вже були проаналізовані в даному підручнику. Як правило, насамперед необхідно провести ідентифікацію місцевості, де були виявлені ознаки таких правопорушень або де знаходились особи, які можуть бути причетними до воєнних злочинів. У зв'язку з цим переважна більшість OSINT аналітиків, які пов'язані з розслідуванням воєнних злочинів, часто в своїй практиці здійснюють аналітику супутникових зображень, які знаходять у відкритому доступі та які відносно часто оновлюються.

«Переваги супутникових зображень — саме у зафіксованій історії змін. Тобто можна відмотати знімки назад і подивитись, хто звідки рухався, яку зброю встановили, де розташовані військові сили тощо. За словами спеціалістів, супутникові знімки допомагають побачити випромінювання РЕБ, яке свідчить про те, що поряд перебуває ворожа армія. Воно може бути встановлене далеко від людей, й інших доказів, окрім супутникових даних, може і не бути»[1].

[1] Як аналітики використовують OSINT, щоб розкривати воєнні злочини росіян : супутникові зображення, аналіз соцмереж та ШІ. Книга пам'яті : вебсайт. URL: https://bookofmemory.com.ua/uk/analytics/how-analysts-use-osint-uncover-russian-war-crimes-satellite-imagery-social-media-analysis-and-ai

Наприклад, дуже показовим у даному випадку є розслідування фахівців OSINT аґенції Molfar причин техногенної катастрофи на Каховській ГЕС[1]. Так, експерти, крім іншого, проаналізували супутникові знімки Каховської ГЕС до та після її знищення, дійшовши висновку, що це не було часткове саморуйнування, що призвело до детонації раніше замінованої греблі.

Для аналізу динаміки змін місцевості можна, наприклад, використовувати Google Earth Pro, де можна дослідити такі зміни в часових діапазонах, які цікавлять аналітика (мал. 6.2). Саме за допомогою даного програмного забезпечення експерти Bellingcat, наприклад, змогли спростувати позицію росії щодо причетності України до збиття боїнгу MH17, де в якості доказів використовувалися супутникові знімки. OSINT аналітики змогли довести, що надані знімки були зроблені в інший час, ніж той, на якому наполягали представники росії, шляхом аналізу рельєфу місцевості на знімках, які були отримані з Google Earth Pro.



Мал. 6.2. Приклад зміни місцевості за майже 10 років в Google Earth Pro

Крім того, велике значення відіграє в процесі проведення OSINT розслідувань ідентифікація осіб, які зображені на фото чи відео. Так, експерти[2] розробили інструкцію, як можна ідентифікувати країну,

[1] Техногенна катастрофа на Каховській ГЕС : причини, хронологія та винуватці — аналітика Molfar. Molfar : вебсайт. URL: https://molfar.com/blog/tehnogenna-katastrofa-na-kakhovskiy-ges-prichini-hronologiya-ta-vinuvatci-analitika-molfar

[2] Rao Komar. How to Digitally Verify Combatant Affiliation in Middle East Conflicts. Bellingcat : website. URL: https://www.bellingcat.com/resources/how-tos/2018/07/09/digitally-verify-middle-east-conflicts/

до якої відноситься військовослужбовець, лише за фотографією такого військовослужбовця

1. Військова форма.

«Військова форма може дати підказки про те, хто такий комбатант і до якої групи він належить. Наприклад, камуфляжні візерунки на військовій формі часто пов'язані з певною країною, збройними силами чи навіть недержавним суб'єктом»[1]. Так, існує сайт Camopedia (https://www.camopedia.org), на якому можна переглянути візерунки військової та іншої уніформи різних країн. При цьому в якості прикладів надаються також зразки уніформ недержавних або неофіційних військових формувань, наприклад приватних військових компаній чи добровольчих корпусів.

Так, експерти Bellingcat зробили висновок, що даний комбатант (мал. 6.3), який тренується на острові Файлака (Кувейт), служить в Турецьких збройних силах, виходячи з візерунку його камуфляжа.

Мал. 6.3. Фото військовослужбовця та зразок камуфляжа з сайту https://www.camopedia.org

2. Нашивки та знаки розрізнення.

«Військові нашивки та знаки розрізнення, що позначають звання або приналежність до підрозділу, є чудовим способом перевірити або

[1] Rao Komar. How to Digitally Verify Combatant Affiliation in Middle East Conflicts. Bellingcat : website. URL: https://www.bellingcat.com/resources/how-tos/2018/07/09/digitally-verify-middle-east-conflicts/

ідентифікувати приналежність комбатанта. Найбільш очевидним першим кроком було б пошукати в Google будь-які слова чи фрази, знайдені на символіці». Також існують спеціальні сайти, такі як International Encyclopedia of Uniform Insignia (https://www.uniforminsignia.net) чи відповідна сторінка на Вікіпедії (https://en.wikipedia.org/wiki/List_of_comparative_military_ranks) (мал. 6.4), де також можна пошукати таку інформацію.

Мал. 6.4. Приклади погонів військовослужбовців ЗСУ відповідно до Вікіпедії

3. Озброєння та спорядження.

«Ідентифікація зброї чи обладнання, якими користувався комбатант, може багато чого розповісти про його приналежність. Певні системи зброї, швидше за все, можна знайти в конкретній країні та серед військових сил цієї країни. Стрілецька зброя — гвинтівки, автомати та пістолети — часто вказує не лише на те, до якої армії належить комбатант, іноді вона навіть може визначити, до складу якого підрозділу він входить».

Загалом необхідно наголосити, що сучасні онлайн-технології та бази даних надають змогу OSINT аналітикам проводити повні та якісні розслідування воєнних злочинів. У будь-якому випадку результативність такого розслідування в значній мірі буде залежати від того, наскільки якісно та ефективно OSINT аналітик зможе комбінувати всі доступні інструменти для отримання необхідного результату. Проте в будь-якому випадку будь-яке збирання доказів має завершуватися їхньою фіксацією, тому питанню документування воєнних злочинів необхідно приділити

окрему увагу, особливо з огляду на специфіку даної категорії кримінальних правопорушень та складності у доведенні винуватості осіб під час судового розгляду.

6.3 ДОКУМЕНТУВАННЯ ВОЄННИХ ЗЛОЧИНІВ, ВІДОМОСТІ ПРО ЯКІ БУЛИ ОТРИМАНІ ЗА ДОПОМОГОЮ OSINT ІНСТРУМЕНТІВ

Ведучи мову про документування воєнних злочинів, не можна обмежуватися лише фактом фіксації відомостей про такі правопорушення. Дійсно, вже функціонують інтерактивні мапи воєнних злочинів, які були вчинені на території України, такі як вже згадувана eyesonrussia.org чи мапа, розроблена спеціалістами Bellingcat (ukraine.bellingcat.com). Хоча такі ресурси є вкрай корисними як для OSINT аналітиків, так і для інших осіб (насамперед для журналістів), таке документування є лише спробою поєднання графічних, просторових та хронологічних даних. За допомогою цих та інших подібних сервісів можна візуалізувати масштаби воєнних злочинів та їхню інтенсивність в залежності від місця, де відбуваються бойові зіткнення. Проте такі способи фіксації насамперед застосовуються для інформування громадськості щодо таких правопорушень. У кримінальному ж процесі документування будь-яких злочинів має відбуватися відповідно до процедури, встановленої кримінальним процесуальним законодавством.

У Темі 4 досліджувалась специфіка фіксації відомостей, отриманих в результаті OSINT розслідування, та їхнє подальше використання в доказуванні у кримінальному провадженні. Очевидно, що такий саме порядок буде стосуватися і документування воєнних злочинів, адже докази в кримінальному процесі будуть досліджуватися однаково незалежно від того, для доведення яких саме кримінальних правопорушень вони будуть використовуватися. Відповідно, ці ж правила будуть застосовуватися і в процесі документування воєнних злочинів. У той же час окремі особливості документування все ж існують.

Насамперед така специфіка проявляється в тому, що держава в силу кількості воєнних злочинів, які вчиняються на території

України, з урахуванням того, що невчасне їхнє документування може призвести до того, що такі докази в подальшому зникнуть або будуть суттєво змінені, намагається залучати до документування воєнних злочинів журналістів, представників громадських організацій, волонтерів. «Ми не можемо розраховувати на те, що коли скінчиться війна, то ми тоді займемося розслідуванням злочинів, які були вчинені під час військового конфлікту, бо докази зникають. Це властивість доказів. А це означає, що багато воєнних злочинців уникнуть відповідальності, багато жертв не отримають ані компенсації, ані навіть певної справедливості бачити злочинців засудженими. Тому ми не можемо чекати»[1]. Очевидно, що під час проведення активних бойових дій питання документування воєнних злочинів відходить «на другий план», проте це не означає, що їх не потрібно фіксувати. «Жертви воєнних злочинів заслуговують на правосуддя. Специфіка даної категорії злочинів, а також складності в їхньому розслідуванні означають, що в окремих випадках особи, відповідальні за злочинні дії, постануть перед правосуддям через багато років, можливо, навіть після смерті основних потерпілих. Проте правосуддя має здійснитися незалежно від тривалості розслідування. І ефективність такого розслідування насамперед буде залежати від якості документування фактів воєнних злочинів, адже саме такі відомості в подальшому будуть використані для розслідування воєнних злочинів»[2].

У зв'язку з цим і держава, і громадські організації зіштовхнулися з новою і доволі специфічною проблемою — забезпечити документування воєнних злочинів шляхом залучення до цього процесу населення, насамперед — жертв таких воєнних злочинів. Очевидно, що такий підхід має низку недоліків, адже особи, які не мають юридичної освіти, не можуть якісно здійснювати фіксування кримінальних правопорушень. У той же час це єдиний спосіб убезпечити доказову інформацію, яка в подальшому буде використана як докази воєнних злочинів. «Минає час, спогади згасають, а інформація зникає, але необхідність

---

1 Документування воєнних злочинів та порушень прав людини як національний обов'язок. Українська Гельсінська спілка з прав людини. 31.06.2016. URL: https://helsinki.org.ua/articles/dokumentuvannya-vojennyh-zlochyniv-ta-porushen-prav-lyudyny-yak-natsionalnyj-obov-yazok/

2 Paul Williams, Jessica Levy. Documentation for Accountability. CaseWestern Reserve Journalof InternationalLaw 52 (2020). P. 451–465.

у притягненні винуватих осіб за грубі порушення міжнародного кримінального права не зникає. Оскільки процес притягнення таких осіб до відповідальності дуже часто затягується, вкрай важливо, щоб докази звірств були зібрані, підготовлені та доступні для використання як тільки з'явиться відповідний судових механізм»[1]. У таких умовах спроби організації фіксування воєнних злочинів не спеціалістами виглядають не як спроба перекласти цей обов'язок на громадян, а як єдиний дієвий механізм фіксування наслідків воєнних злочині, який вже неодноразово демонстрував свою ефективність в інших країнах.

«Так, Офісом Генерального прокурора було створено онлайн-ресурс https://warcrimes.gov.ua, в якому будь-хто може надати інформацію про будь-які воєнні злочини. Вся інформація, яка надається на сайті, поділена на чотири блоки: відомості про особу, яка надає інформацію; коли сталася подія; де сталася подія (з можливістю визначення місця на інтерактивній мапі України); який саме воєнний злочин було вчинено. При цьому громадян не змушують детально описувати подію, дозволяючи вибрати вид воєнного злочину з переліку запропонованих, що значно спрощує первинну кваліфікацію такого правопорушення. Також на сайті пропонується надати особисту інформацію ворога та будь-які додаткові відомості, які стосуються воєнного злочину. При цьому бажано додатково завантажити фото чи відеозапис відповідної події.

Можна зазначити, що такий спосіб фіксації воєнних злочинів є найбільш вдалим, адже, по-перше, він у максимально зручній формі дозволяє повідомити найважливішу інформацію про кримінальне припорошення; і по-друге, такі відомості напряму потрапляють до правоохоронних органів, що дозволяє проводити розслідування максимально оперативно. При цьому сайт зроблено максимально зручно саме задля того, щоб ним могли скористуватися максимально широкі верстви населення.

У той же час така форма фіксації має і деякі недоліки. Так, такий спосіб передачі інформації залежить від наявності доступу до мережі Інтернет. Крім того, ворог продовжує створювати фішингові сайти, які ззовні є подібними до справжніх сайтів для збирання інформації, проте

[1] Paul Williams, Jessica Levy. Documentation for Accountability. CaseWestern Reserve Journalof InternationalLaw 52 (2020). P. 451–465.

з фішингових сайтів інформація передається напряму ворогу. Також далеко не всі громадяни (а особливо це стосується людей похилого віку — найбільш уразливої категорії населення) можуть самостійно зайти в інтернет та повідомити про воєнний злочин»[1].

Експертами фонду Global Rights Compliance у травні 2023 року було опубліковано Керівництво з базових стандартів розслідування для документування міжнародних злочинів в Україні, де було надано низку порад, в тому числі які стосуються специфіки документування воєнних злочинів, відомості про які були отримані за допомогою OSINT інструментів. Так, у даному Керівництві, крім іншого, були надані практичні поради, які стосуються збереження інформації, яка має використовуватися в подальшому як доказ. «Інформація може зберігатися на місцях, наприклад, на зашифрованому паролем жорсткому диску, що зберігається в замкненій шафі, на мережевому диску, який є частиною локальної мережі або віддаленого сервера, або на хмарному сховищі. Спосіб зберігання інформації залежить від: чутливості цифрового контенту і відносної безпеки різних варіантів; вартості; ємності сховища; доступності; довгострокової стійкості; і відповідних законів, включно із законодавством про захист даних. Це слід враховувати при складанні вашого плану документування. Для відстеження того, що зберігається, де і які елементи були верифіковані або вимагають верифікації, слід використовувати стандартизовану систему збору даних (наприклад, деталізовану електронну таблицю). Тут виникає етичне міркування щодо самої людини, яка першою поділилась інформацією в інтернеті, і чи дала вона вам свою інформовану згоду на зберігання і використання цієї частини інформації. Там, де це можливо, слід вжити заходів для отримання інформованої згоди, якщо тільки це не піддасть ризику того, хто завантажив інформацію.

Наприклад, Єменський проєкт (https://yemeniarchive.org) розробив протокол, за допомогою якого URL-адреса будь-якого матеріалу, який слідчі хочуть зберегти, може бути скопійована в електронну таблицю, хешована цифровим способом і збережена в цілісності. Крім того, Сирійський центр

[1] Ващук Л.П, Торбас О.О. Кримінальні процесуальні та криміналістичні особливості документування воєнних злочинів. Правова система України в умовах воєнного стану : збірник наукових праць / за загальною редакцією О.О. Кота, А.Б. Гриняка, Н.В. Міловської, М.М. Хоменка. Одеса : Видавничий дім «Гельветика», 2022. С. 484–494.

правосуддя і підзвітності (https://syriaaccountability.org) розробив власне програмне забезпечення для створення реляційних баз даних, відоме як «Баянат» (Bayanat), за допомогою якого організація успішно зберегла понад 1,8 мільйона файлів даних, включно з понад 350 000 відеозаписів.

Нестабільне підключення до інтернету може стати перешкодою для фахівців, які проводять розслідування з відкритих джерел в зонах конфліктів, особливо при спробі зберегти інформацію. Щоб пом'якшити цю проблему, Myanmar Witness, місцева ОГС, яка займається збором інформації з відкритих джерел про порушення прав людини в М'янмі, співпрацює і ділиться інформацією з незалежним механізмом ООН з розслідування в М'янмі, який потім може зберігати і перевіряти матеріали»[1].

Загалом необхідно ще раз наголосити, що незалежно від виду кримінального правопорушення, документування доказів, отриманих з відкритих джерел, буде проводитись відносно стандартизовано, адже воно повинно відповідати загальним вимогам, які визначені кримінальним процесуальним законодавством України. Особливістю документування воєнних злочинів є лише те, що в подальшому такі відомості можуть досліджуватися поза кримінальним процесом України, наприклад, в Міжнародному кримінальному суді.

6.4 ВИКОРИСТАННЯ ДОКАЗІВ, ОТРИМАНИХ ЗА ДОПОМОГОЮ OSINT ІНСТРУМЕНТІВ, МІЖНАРОДНИМ КРИМІНАЛЬНИМ СУДОМ

У зв'язку з тим, що воєнні злочини порушують базові права, які підтримуються майже всіма державами світу, увага до таких правопорушень завжди є максимально серйозною. Тому цілком логічним є те, що 17 липня 1998 року було засновано Міжнародний кримінальний суд (далі — МКС) шляхом підписання Римського статуту. Необхідно зазначити, що Україна підписала, проте не ратифікувала Римський статут. Однак це не означає, що Україна взагалі не визнає юрисдикцію МКС. Міністерство

[1] Керівництво з базових стандартів розслідування для документування міжнародних злочинів в Україні. Global Rights Compliance. 2023. URL: https://www.asser.nl/media/796421/manual-керівництво-з-базових-стандартів-розслідування-для-документування-міжнародних-злочинів-в-украі-ні.pdf

закордонних справ України заявило, що наша держава визнає юрисдикцію МКС з двох питань — справа щодо Майдану (заява від 17 квітня 2014 року) та щодо злочинів проти людяності та воєнних злочинів, що вчинені на території України (заява від 8 вересня 2015 року). Через повномасштабне вторгнення 2022 року в кримінальному процесуальному законодавстві відбулися суттєві зміни, однією з яких є введення нового розділу в КПК України, присвяченого особливостям співробітництва з МКС.

Таким чином, на даний момент як ніколи критично важливим є забезпечення правильного документування воєнних злочинів на національному рівні, адже в подальшому такі відомості можуть бути передані до МКС. У той же час необхідно розуміти, що хоча загальна логіка здійснення кримінального провадження (а отже, і фіксування доказів) є універсальною, в діяльності МКС є свої особливості, які необхідно враховувати в процесі організації відповідної взаємодії.

Якщо ж вести мову про можливості використання OSINT Міжнародним кримінальним судом, то можна зазначити, що МКС вже досить давно та активно використовує в якості доказів відомості, отримані з відкритих джерел. Насамперед це пояснюється тим, що воєнні злочини вже відносно давно розслідуються саме завдяки відомостям, отриманим з відкритих джерел. Власне, Протокол Берклі було розроблено насамперед задля розслідування порушень МГП та суміжних правопорушень. Тому не дивно, що уповноважені особи МКС не лише застосовують докази з відкритих джерел, а і активно пропагують інших осіб долучатися до їхнього збору. Так, в 2023 році прокурор МКС оголосив про запуск розширеної платформи для надання доказів OTPLink (https://otplink.icc-cpi.int). OTPLink дозволяє уніфікувати збір інформації від осіб відповідно до ст. 15 Римського статуту. «Ця інноваційна програма поєднує передові сучасні технології та міжнародне право і надає користувачам безпечний метод подання потенційних доказів в режимі реального часу з будь-якого пристрою, який має доступ до інтернету. Платформа забезпечує швидкий, безпечний і надійний збір інформації. OTPLink спрощує традиційний процес перевірки доказів, дозволяючи офісу обробляти більші обсяги інформації за допомогою штучного інтелекту і машинного навчання, щоб забезпечити краще розуміння отриманої інформації, значно скорочуючи час, необхідний для її аналізу

та вжиття відповідних заходів. Платформа підтримує міжнародні стандарти обробки доказів, використовуючи цифровий ланцюг збереження інформації, що гарантує цілісність доказів»[1].

«OTPLink зробить значний внесок у збір доказів та обмін інформацією з метою запобігання безкарності за найтяжчі міжнародні злочини. OTPLink також збільшить пряму взаємодію зовнішніх зацікавлених сторін з ОП МКС, підвищить доступність для потенційних жертв і свідків, а також надасть інструмент для збору доказів та інформації, які в іншому випадку були б неможливими для слідчих ОП МКС. Такий інструмент надасть жертвам і свідкам найтяжчих міжнародних злочинів, включаючи зґвалтування, тортури, вбивства і обернення в рабство, безпрецедентні можливості. Однак мета OTPLink не буде повністю досягнута, якщо ОП МКС не інвестуватиме в інформаційно-просвітницьку діяльність та послуги з перекладу, щоб платформа та її ефективне використання охопили всі зацікавлені сторони — включаючи постраждалі громади та потенційних жертв і свідків — у всіх ситуаціях, що перебувають на стадії досудового розслідування та слідства»[2].

У той же час така увага уповноважених осіб до доказів з відкритих джерел ще не означає, що МКС беззаперечно визнає такі докази. Більше того, прийнятність таких доказів на рівні МКС почала визнаватися відносно не так давно. Насамперед необхідно зазначити, що відповідно до Статуту і Правил процедури та доказування Міжнародного кримінального суду (Statute and Rules of Procedure and Evidence), суддям надаються досить широкі дискреційні повноваження щодо оцінки доказів. Однак у міру розвитку прецедентного права в МКС відбулися помітні тенденції до більш суворого підходу до використання показань з чужих слів та відомостей, отриманих з відкритих джерел. Хоча на початку судді дозволяли використовувати різноманітні відомості, що надходили від громадських організацій чи ЗМІ, надмірне використання прокурором таких відомостей в якості прямих доказів призвело до того, що судді, починаючи з 2013 року,

---

1 ICC Prosecutor Karim A.A. Khan KC announces launch of advanced evidence submission platform : OTPLink. International Criminal Court : website. URL: https://www.icc-cpi.int/news/icc-prosecutor-karim-aa-khan-kc-announces-launch-advanced-evidence-submission-platform-otplink

2 Збір цифрових доказів у Міжнародному кримінальному суді : Обіцянки та підводні камені. Just Security : вебсайт. URL: https://www.justsecurity.org/87731/digital-evidence-collection-at-the-intl-criminal-court-promises-and-pitfalls-ua/

почали обмежувати відповідну практику, зазначаючи, що відомості з відкритих джерел насамперед мають використовуватися як орієнтуюча інформація або разом з іншими доказами. Так, в справі Прокурор проти Гбагбо суд зробив наступний висновок: «[Палата] із серйозним занепокоєнням зазначає, що в цій справі прокурор значною мірою покладався на звіти громадських організацій і статті в пресі щодо ключових аспектів справи, включаючи контекстуальні елементи злочинів проти людяності. Такі докази жодним чином не можуть бути представлені як результат повного та належного розслідування, проведеного Прокурором відповідно до статті 54(l)(a) Статуту. Незважаючи на те, що звіти громадських організацій та статті в пресі можуть бути корисним для розуміння історичного контексту конфлікту, вони, як правило, не можуть замінити той тип доказів, який необхідний для забезпечення стандарту доказування щодо відповідних обвинувачень»[1]. Відтоді МКС суттєво обмежив вагу та обсяг відомостей з відкритих джерел, які можна використовувати для доведення обставин.

«Аналізуючи різні судові рішення, можна зробити декілька висновків щодо того, як саме судді МКС оцінюють докази з відкритих джерел. По-перше, судді більш поблажливо ставляться до використання прокурором доказів з відкритих джерел на ранніх стадіях провадження і більш суворо підходять до їхньої оцінки під час судового розгляду. По-друге, у суддів існує чітка ієрархія відкритих джерел, яка заснована на сприйнятності їхній легітимності: офіційні звіти ООН — звіти агентств ООН — звіти відомих неурядових організацій (наприклад, Human Rights Watch і Amnesty International) — звіти менш відомих неурядових організацій — повідомлення в ЗМІ від авторитетних інформаційних агентств (наприклад, BBC і New York Times) — інші ЗМІ. Також судді при оцінці можливості використання відомостей з відкритих джерел враховують прозорість використаних методів при збиранні такої інформації та ідентифікацію самого автора, особливо якщо автор буде давати показання в суді»[2].

---

1 Gbagbo and Blé Goudé Case. International Criminal Court : website. URL: https://www.icc-cpi.int/cdi/gbagbo-goude

2 Lindsay Freeman. Prosecuting Atrocity Crimes with Open Source Evidence. Lessons from the International Criminal Court. Digital Witness : Using Open Source Information for Human Rights Investigation, Documentation, and Accountability. URL: https://www.academia.edu/95425352/Prosecuting_Atrocity_Crimes_with_Open_Source_Evidence_Lessons_from_the_International_Criminal_Court

Проте в подальшому Суд стикнувся з новим викликом, адже на заміну звітам з відкритих джерел почали приходити електронні докази з відкритих джерел. У 2016 році, коли прокурор порушив справу за знищення культурних цінностей у Тімбукту проти Ахмада Аль-Факі Аль-Махді як безпосереднього виконавця, понад 600 доказів було передано до суду, включаючи відеозаписи, на яких були зображені обвинувачені і те, як вони брали участь у знищенні мечетей або пояснювали свої наміри їх знищити. Аль-Махді визнав себе винним, тому ці докази в суді не досліджувалися, проте це була перша справа, в яких в якості доказів була надана інформація з інтернету у вигляді скріншотів або відеозаписів.

Через рік, у 2017 році, МКС видав ордер на арешт Аль-Верфаллі, вказуючи на його причетність до вбивств під час неміжнародного збройного конфлікту в Лівії. Ордер ґрунтувався в більшій мірі на семи відеозаписах, які були розміщені в соціальних мережах. Щодо кожного злочину в ордері на арешт містився короткий опис вмісту відео, а потім зазначалося, що відео було опубліковано в соціальних мережах в певний конкретний день. Лише в першому випадку ордер вказував на Facebook як на платформу, де були розміщені відео, але в ордері не було конкретних посилань або вказівок на профілі користувачів, де були розміщені такі відео. Деякі вчені вважають таку практику помилковою, адже це демонструє, що МКС розглядає соціальні мережі як одне-єдине універсальне джерело інформації[1].

У будь-якому випадку можна помітити, що судді МКС почали частіше використовувати докази, отримані з відкритих джерел, у своїй практиці. Очевидно, що насамперед це пояснюється швидким розвитком цифрових технологій та неможливістю ігнорування відомостей, які можуть бути опубліковані в соціальних мережах чи блогах. У той же час судді МКС досліджують такі докази з певною долею скептицизму, що загалом ще раз підтверджує думку про те, наскільки якісною має бути документування таких злочинів ще на національному рівні.

---

[1] Lindsay Freeman. Prosecuting Atrocity Crimes with Open Source Evidence. Lessons from the International Criminal Court. Digital Witness : Using Open Source Information for Human Rights Investigation, Documentation, and Accountability. URL: https://www.academia.edu/95425352/Prosecuting_Atrocity_Crimes_with_Open_Source_Evidence_Lessons_from_the_International_Criminal_Court

НОТАТКИ

Наукове видання

Торбас Олександр Олександрович

OSINT ПРИ РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

Підручник

Обкладинка	*В. Савєльєва*
Верстка	*Н. Ковальчук*
Технічне редагування	*О. Гринюк*

ЮРИДИКА
ВИДАВНИЦТВО

Підписано до друку 08.03.2024 р. Формат 60x84/16.
Папір офсетний. Гарнітура Droid. Цифровий друк.
Ум. друк. арк. 10,46. Наклад 100.
Замовлення № 022п/0324.
Віддруковано з готового оригінал-макета.

Видавництво і друкарня – Видавництво «Юридика»
65101, Україна, м. Одеса, вул. Інглезі, 6/1
Телефони: +38 (095) 934 48 28, +38 (097) 723 06 08
E-mail: mailbox@juridica.od.ua
Свідоцтво суб'єкта видавничої справи
ДК № 7653 від 18.08.2022 р.