СЛУЖБА БЕЗПЕКИ УКРАЇНИ

Інститут Служби безпеки України
Національного юридичного університету
імені Ярослава Мудрого

ВИКОРИСТАННЯ ІНСТРУМЕНТІВ ТА МЕТОДІВ OSINT ДЛЯ ОТРИМАННЯ ПОШУКОВОЇ ІНФОРМАЦІЇ

Практичний порадник
5-те видання, перероблене та доповнене

Харків 2024

УДК 343.3, 004.9 (06)
В43

Рекомендовано до друку Вченою радою
Інституту Служби безпеки України
Національного юридичного університету імені Ярослава Мудрого
(протокол № 30 від 23 квітня 2024 року)

Рецензенти:
Володимир Карастельов,
співробітник Департаменту контррозвідувального захисту
інтересів держави у сфері інформаційної безпеки СБУ, к.ю.н.;
Олександр Жупіна,
співробітник Головного слідчого управління СБУ, к.ю.н.

Авторський колектив:
Дмитро Зоренко, доцент кафедри Інституту;
Людмила Кульчицька, співробітник СБУ;
Роман Лех, заступник директора (з навчальної та наукової роботи)
Навчально-наукового інституту державної безпеки
Національної академії СБУ, к.ю.н.;
Олександр Червяков, начальник Інституту, к.ю.н.

Зоренко Д. С., Кульчицька Л. О., Лех Р. В., Червяков О. І.

В43 **Використання інструментів та методів OSINT для отримання пошукової інформації :** практичний порадник. 5-те вид., переробл. та доповн. / Д. С. Зоренко, Л. О. Кульчицька, Р. В. Лех, О. І. Червяков. – Харків. Видавець: О. А. Мірошниченко, 2024. – 80 с.

ISBN 978-617-8130-64-0.

У практичному порадникові комплексно розглянуто теоретичні й прикладні аспекти використання інструментів та методів OSINT (розвідки з відкритих джерел) для пошуку в мережі «Інтернет» відомостей про осіб, факти чи події з метою задоволення потреб службової діяльності органів і підрозділів СБУ, а також формування відповідних цифрових компетентностей співробітників Служби.

Викладений матеріал розрахований на базові знання й навички користувача та не містить опису шляхів несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

При розгляді інструментів пошуку акцент зроблено на загальнодоступні та безоплатні рішення, а їх наведений перелік не носить вичерпний характер. З часом обсяг функціональності зазначених у порадникові вебресурсів чи програм може змінюватися.

Автори не несуть відповідальності за шкоду або збитки, яких може зазнати користувач (треті особи) в результаті помилкового розуміння та/або застосування наведеної у виданні інформації. Вебдослідник повинен самостійно забезпечувати захист власних персональних даних та іншої конфіденційної інфомації під час пошукової діяльності в мережі «Інтернет».

Будь-які відомості, отримані користувачем із застосуванням викладеного матеріалу, використовуються ним на свій ризик. В оформленні навчального видання використано зображення, взяті з відкритих джерел.

Порадник адресований співробітникам оперативних і слідчих підрозділів СБУ, здобувачам вищої освіти, викладачам й науковцям відомчих навчальних закладів, а також усім, хто цікавиться актуальними питаннями пошуку інформації у відкритих джерелах.

УДК 343.3, 004.9 (06)

ISBN 978-617-8130-64-0

ЗМІСТ

Умовні позначення:
Bellingcat – гіперпосилання на вебресурс;
bot – Telegram-бот;
GitHub – репозиторій проєктів з відкритим вихідним кодом;
free – обсяг безкоштовного функціоналу онлайн-сервісу чи програми;
RU (BY) – інтернет-сайт прямо чи опосередковано пов'язується з рф (рб).

1. Поняття та призначення OSINT

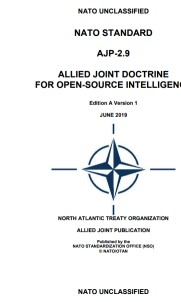
OSINT (*Open Source INTelligence*, розвідка з відкритих джерел) – складова спеціальної діяльності, що передбачає отримання інформації з відкритих джерел (публічно чи комерційно доступних), їх обробку, аналіз та поширення.

OSINT як відокремлена практика зародилася в США у 40-х рр. минулого століття із заснуванням Служби моніторингу закордонних трансляцій. Якщо ж говорити про Україну, то з відновленням державності у 1991 році отримання даних з відкритих джерел також було повсякденною практикою оперативно-службової діяльності, однак без такого структурного виділення як в США. До появи інтернету це було також дослідження друкованих ЗМІ, документів, звітів, матеріалів конференцій, наукових робіт, різноманітних довідників, списків тощо. Після виникнення глобальної мережі зміст OSINT змінився. Тепер часто актуальнішим є не потонути в надмірному обсязі даних і вміти виокремити потрібне.

Сьогодні розвідка з відкритих джерел успішно використовується не тільки органами безпеки та оборони провідних країн світу, а й комерційними компаніями, неурядовими організаціями, аналітичними центрами, журналістами, різного роду розслідувачами, приватними особами тощо.

Найбільш системні описи змісту та процедурного наповнення OSINT викладені фахівцями *НАТО* у збірниках «NATO Open Source Intelligence Handbook» (2001), «NATO Open Source Intelligence Reader» (2002), «NATO Intelligence Exploitation of the Internet» (2002), а також у стандартах «Allied Joint Doctrine for Open-Source Intelligence» (AJP-2.9, 2019) та «Open-Source Intelligence (OSINT) Tactics, Techniques and Procedures» (AIntP-22, 2022).

Зокрема, AJP-2.9 та AIntP-22 визначають сукупність загальнорекомендованих тактик, технік та процедур із провадження на оперативному рівні стандартизованого OSINT-процесу для підтримки операцій НАТО. У них розкривається роль розвідувального циклу як ключової методики збору та аналізу пошукової інформації при реалізації заходів Joint Intelligence, Surveillance and Reconnaissance (розвідки, спостереження та рекогносцировки). Хоча вказані стандарти призначені насамперед як настанови для об'єднаного командування й штабів НАТО, вони можуть використовуватися партнерами, які не є членами Альянсу, а також відігравати роль практичного довідника для цивільного персоналу.


NATO UNCLASSIFIED

NATO STANDARD

AJP-2.9

ALLIED JOINT DOCTRINE FOR OPEN-SOURCE INTELLIGENCE

Edition A Version 1

JUNE 2019

NORTH ATLANTIC TREATY ORGANIZATION

ALLIED JOINT PUBLICATION

Published by the NATO STANDARDIZATION OFFICE (NSO) © NATO/OTAN

NATO UNCLASSIFIED

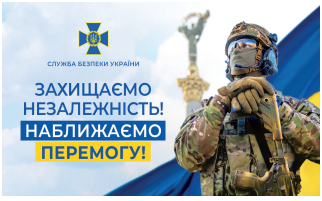
Зі свого боку, громадський сектор та інтернет-ЗМІ наполегливо інтергують OSINT-технології в практику проведення публічних розслідувань резонансних суспільно-політичних подій, корупції високопосадовців, ситуації в зонах збройних конфліктів, порушень прав людини, злочинів проти миру та безпеки. Один із найуспішніших прикладів – діяльність міжнародної команди журналістів проєкту Bellingcat (зокрема кейси щодо збиття авіарейсу MH17, обстрілів території України армією рф у 2014-2015 рр., ідентифікації бойовиків ПВК «Вагнер», причетних до воєнних злочинів тощо).

З огляду на такий потужний поштовх і в українському інформаційному просторі стрімко набрав обертів осінтерський рух – InformNapalm, Molfar, OsintFlow, OSINT Бджоли, Truth Hounds – це далеко неповний перелік OSINT-спільнот, що від початку російської збройної агресії проти України долучилися до допомоги силам оборони, збору доказів воєнних злочинів та протидії ворожій пропаганді. Також, одним із своїх завдань активісти вбачають систематизацію сучасного досвіду OSINT-досліджень для подальшої комплексної імплементації в діяльність зацікавлених державних органів.

Безумовно, збір та аналіз відкритих даних є важливою складовою протидії актуальним викликам і загрозам державній безпеці України – завдяки інструментам та методам OSINT фахівці СБУ виявляють місцезнаходження ворожих військових формувань і техніки, встановлюють особисті дані воєнних злочинців та збирають відповідну доказову базу, викривають зрадників та колаборантів, ініціюють внесення осіб чи організацій до санкційних списків, здійснюють психологічно-інформаційний вплив на противника, розвінчують фейки ворожої пропаганди тощо.

В умовах сьогодення OSINT – це не просто кабінетна робота, а дуже прикладна та результативна дисципліна, що дозволяє отримати відомості про військові об’єкти, плани та документи ворога без ризику для життя співробітників. Натомість вона потребує колосальних ресурсів і часу для аналізу даних та визначення їх впливу на безпеку нашої держави. В цьому процесі СБУ плідно співпрацює з вітчизняними та іноземними партнерами, які надають передові програмні комплекси та інформаційну підтримку.

Оскільки пошукова діяльність із використанням відкритих джерел суттєво збільшує інституційні можливості української спецслужби, OSINT став одним з обов'язкових елементів фахової підготовки співробітників СБУ завдяки вдалому поєднанню кращих світових практик та унікального практичного досвіду, здобутого за час відсічі збройної агресії рф.



2. Етапи пошукової роботи (розвідувальний цикл)

Стандарти НАТО акцентують увагу на необхідності дотримання під час здійснення пошукової роботи певного алгоритму – т.зв. розвідувального циклу (Intelligence Cycle), що складається з наступних **TCPED-етапів**: постановка завдання (Task), збір інформації (Collection), її технічна обробка (Process), подальше опрацювання (Exploit) та поширення результатів (Disseminate).

1) Task (постановка завдання) – формування замовником завдань OSINT-дослідження (приміром, ідентифікація фізичної чи юридичної особи, встановлення окремих аспектів її діяльності, близького оточення чи пов'язаних контактів, компрометуючих матеріалів, місцезнаходження об'єкта або маршруту його переміщення, верифікація наявних даних тощо), визначення необхідних для його виконання сил та засобів, доведення цієї інформації до безпосереднього виконавця.

Останній має проаналізувати такий запит на відповідність критеріям конкретності, вимірюваності, відносності, реалістичності й своєчасності; зрозуміти його обсяг і характер, терміни та форму подання звіту; з'ясувати достатність ресурсів для його виконання; рівень потенційних загроз безпеці збору даних та можливі застереження правового характеру. У разі потреби виконавець може звернутися до замовника з метою уточнення деталей отриманого завдання або надання додаткових вихідних відомостей.

2) Collection (збір інформації) – складається з: 1) формування оптимальної методології збору даних (підготовка плану, визначення необхідних методів, інструментів та ресурсів; формулювання переліку ключових слів для пошукових запитів, ризик-менеджмент тощо); 2) проведення пошуку інформації з використанням відомих та опрацюванням раніше невідомих або альтернативних джерел; 3) безпосередньо цілеспрямованого збору релевантних даних. Водночас дуже важливим є процес оцінки надійності цих джерел та достовірності розміщеної на них інформації, а також їх умовний поділ на *первинні* (повідомлення осіб, які мали безпосередній зв'язок з інформацією) та *похідні* (цитування або використання першоджерела в будь-який інший спосіб).

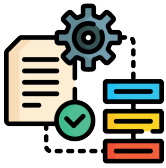
У якості базової моделі планування дослідження можна розглядати *схему 5W+H* (Who *хто*, What *що*, When *коли*, Where *де*, Why *чому* and How *як*) – тоді стає більш зрозумілим, де і в якому вигляді можуть зберігатися необхідні відомості. Процес пошуку нагадує заповнення сегментів мозаїки – кожна нова достовірна одиниця інформації відразу ж задіюється в пошуковій роботі з метою підвищення її результативності. Універсальний набір інструментів і алго-

ритм пошукових дій визначити складно – ключові слова, джерела потенційної інформації, необхідний інструментарій, наявність відомостей та їх достовірність залежать від вихідних даних та кінцевої мети пошуку.

Найпоширеними джерелами інформації про об'єкт зацікавленості є: ***він сам*** (соціальні медіа, канали, блоги, форуми, публікації тощо); ***його оточення*** (родина, друзі, сусіди, роботодавець, колеги, підлеглі, конкуренти); ***держава, органи місцевого самоврядування, підприємства, установи чи організації*** (реєстри, бази даних, судові рішення, борги, офіційне листування, інтернет-ЗМІ та інше).

Збір відомостей може бути ***пасивним*** (без взаємодії з об'єктом зацікавленості, наприклад, за допомогою пошукових систем, сервісів чи Telegram-ботів) та ***активним*** (наприклад, застосування елементів соціальної інженерії при роботі з поштою чи акаунтами особи в соцмережах; отримання доступу до відкритих портів його пристроїв; використання вразливостей встановлених ним програм тощо).

Оскільки дані в мережі «Інтернет» можуть бути видалені власником у будь-який момент, не зайвим кроком стане ***формування офлайн архіву зібраних відомостей*** (приміром, за допомогою скріншотів; створення pdf-файлів з додаванням url-адреси сайту, дати, часу та заголовку; збереження веб-сторінки вцілому чи окремих файлів; архівування сайтів тощо).

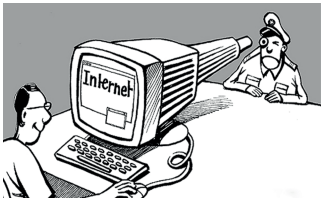


3) Process (технічна обробка) – це аналіз всієї зібраної інформації на релевантність (відповідність меті дослідження) та її сортування за певними критеріями (об’єкт/зміст/джерело/час/достовірність/зв'язок тощо); переклад та адаптація іншомовних матеріалів; додавання до визначених файлів стандартизованих метаданих; зведення інформації у консолідований набір даних шляхом порівняння та групування пов'язаних елементів.

4) Exploit (опрацювання) – верифікація попередньо оброблених відомостей, тобто їх зіставлення з іншими незалежними OSINT-джерелами для підтвердження або спростування достовірності даних. Якщо подібна перевірка неможлива, інформація позначається як «неперевірена». Кінцевий результат роботи формується шляхом поєднання ***якісного*** (поглиблений аналіз предметної області дослідження з можливим додаванням висновків, оцінок, експертних коментарів, роз’яснень та рекомендацій) та ***кількісного*** (використання візуалізації – схем, інтелект-карт, інфографіки, скріншотів/фото; витягів, посиланнь на джерела, додатків) опрацювання інформації з урахуванням релевантності запиту.

5) Disseminate (поширення результатів) – підготовка та передача замовнику підсумкового документу з можливими застереженнями щодо його поширення (обмеження доступу, вміст контенту, викладені погляди або думки, цілі використання, відповідальність тощо). Замовник має оцінити наданий звіт, визначити проблемні моменти дослідження та запропонувати шляхи їх усунення.

3. Анонімізація пошуку в інтернеті

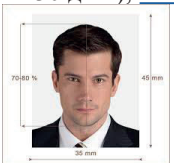


Інтернет – це публічний простір, що знаходиться в постійній динаміці, а тому не існує абсолютно надійних способів залишатися в ньому інкогніто на 100 %. Будь-яка анонімність тут тимчасова, можна лише ускладнити процес ідентифікації користувача. Іншими словами, здійснювати пошук необхідно з усвідомленням того, що ваші дослідницькі дії потенційно можуть фіксуватися та аналізуватися третіми особами з метою подальшої встановлення особи чи спрямованості пошукової роботи.

Виокремлюють *соціальну анонімність* (людина свідомо утримується від розкриття особистої інформації на веб-ресурсах, наприклад, під час реєстрації на платформах соціальних мереж) та *технічну анонімність* (за допомогою спеціальних програмних рішень маскуються/змінюються дані пристрою, з якого здійснюється пошук).Тому, **потрібно розмежовувати свою службову діяльність і приватний серфінг в інтернеті** – особисті облікові записи (операційної системи, браузера й інших програм, акаунти електронної пошти, соцмереж чи месенджерів) та обладнання (ноутбук, планшет, мобільний телефон) не повинні задіюватися під час виконання професійних завдань, і навпаки. Фахівці наголошують – що потрапило у глобальну мережу, залишається там назавжди.

Отже, для кожного програмного продукту, з яким ви працюєте, а також для роботи на веб-ресурсах, месенджерах чи у соціальних медіа, що вимагають від користувача авторизації для доступу до контенту чи певного функціоналу, бажано **використовувати віртуальну особистість** (або декілька), яка має імітувати реальну людину настільки, наскільки це важливо для потреб конкретного дослідження (це може бути нікнейм, стать, вік, регіон, біографія, інтереси та захоплення, коло друзів, світлини тощо). Подібний фейковий профіль (sockpuppet) може складатися з довільного поєднання наступних елементів:

• персональні дані (достатньо поширене ім'я та прізвище, дата народження, країна, місце проживання, стать та ін.), що можна *вигадати* або *згенерувати* – Busines, FakeDetails, FakeInfo, FakeNameGenerator, FakePersonGenerator, Meragor, miniRANDOM, NameFake, OnlineNameGenerator, RandomUserGeneration, Randus (RU, free – 10 запитів на 30 днів), ThisResumeDoesNotExist, uk-osint.com;



• фото – BoredHumans, FaceApp, GeneratedPhotos (free – 3 дні), Meragor (RU), RandomFaceGenerator (присутній водяний знак), ThisPersonDoesNotExist (присутній водяний знак), Unreal Person, WhichFaceIsReal, генератор облич людини, генератор

портретів, Kandinsky (RU, bot); AIFaceswap (створення deepfake фото та відео).

Наразі нейромережам найкраще вдаються портретні світлини зблизька, на яких фокус робиться на обличчі, а фон позаду, як правило, розмивається. Основні зони помилок на таких фото – очі, зуби, мочки вух, волосся, елементи одягу чи аксесуарів, написи тощо. Також звертайте увагу на пальці рук, їх може бути більше п'яти та/або вони мають неприродні згини.

Оскільки подібні зображення створюються штучним інтелектом за певними правилами (приміром, очі завжди мають знаходитися на одній паралелі, а відстань між очима та між очима й ротом співпадати), їх бажано перевіряти як візуально, так і за допомогою спеціальних сервісів. А тому перед завантаженням згенерованого фото в соцмережу кращою практикою визнається навіть незначне його корегування за допомогою фоторедактору (наприклад, видозміна рис обличчя, зачіски, одягу, кольору волосся, додавання окулярів тощо);

• електронна пошта (без прив'язки до номеру мобільного телефону чи іншого e-mail) – реєстрація *«постійної» адреси,* наприклад, на ресурсах Addy.io (free – шифрування вихідних листів, функція пересилання пошти, 2 анонімні скриньки та 1 реальна пошта-рецепієнт, місячний поштовий трафік 10 Мб), Gmail (вимога щодо прив'язки телефонного номеру постійно змінюється, наразі вона не є обов'язковою при створенні однієї поштової скриньки через веб-інтерфейс та за відсутності незвичної активності користувача; free – сховище 15 Гб), Mailfence (free – шифрування, сховище 1 Гб), ProtonMail (позитивно сприймається соцмережами під час реєстрації; free – шифрування вмісту листа на відміну від його теми та метаданих, відсутність логування, сховище 1 Гб, безкоштовний VPN), Tuta (пропонує код для відновлення доступу, free – шифрування, видалення IP-адреси з листа, сховище 1 Гб).

Сервіси NameCheckup та NaMint допоможуть підібрати нікнейми для акаунтів пошти та соцмереж (за ім'ям, прізвищем та датою народження).

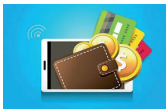
Створені профілі потрібно періодично перевіряти на потрапляння у витоки (приміром, через DeHashed, Have I Been Pwned, Hudson Rock), а в разі необхідності змінювати пароль (бажано не менше 12 символів з числа великих та рядкових літер латиницею, цифр та спецсимволів, або задіювати генератор паролів чи аналоги), увімкнути двофакторну автентифікацію чи зареєструвати новий.

Так само *тимчасова (разова) адреса* має як свої переваги (автоматична генерація випадкової назви скриньки, відсутність прив'язки до будь-якої особистої інформації), так і недоліки (більша частина вебресурсів не приймає її для реєстрації акаунтів; кожна тимчасова адреса унікальна і видається лише раз, по завершенню терміну функціонування всі дані видаляються, тому подальше підтвердження користувача через неї буде неможливе; відсутні гарантії того, що доступ до такої пошти буде тільки у однієї особи – вас).

До найбільш популярних подібних сервісів можна віднести DropMail («цикл життя» – до моменту оновлення веб-сторінки, вбудована функція пересилан-

ня пошти, можливість відновлення скриньки, але не її вмісту), Gmailnator (генератор пошти @gmail.com, «цикл життя» – 10 хв.), Guerrilla Mail («цикл життя» – 60 хв., відправляє листи з вкладеннями до 150 Мб, генератор паролів з можливістю їх зберігання та відновлення за майстер-кодом), mail.tm («цикл життя» – до видалення, тільки приймає пошту, є пароль), Tempr.email («цикл життя» – до 30 днів, приймає та відправляє пошту з вкладеннями, доступ через пароль); Temp-mail та 10minutemail («цикл життя» – 10 хв., подовження до 1 год., можна відповісти на отриманий лист або перенаправити його на іншу поштову скриньку);

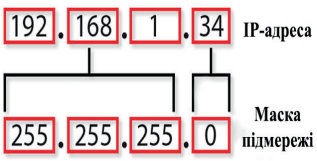
• віртуальний номер телефону (для прийому SMS під час разової реєстрації в соцмережах/месенджерах чи довготривалої оренди) – FreeOnlinePhone, GetFreeSMSNumber, ReceiveSMSOnline, Sellaite.com (обмежена кількість номерів, багаторазове використання, доступність номеру для інших користувачів, SMS-відповіді бачать всі відвідувачі). Але краще використовувати *платні ресурси* GrizzlySms (RU), OnlineSIM (RU), Proovl, Receive-SMS, Sms-Activate (RU), SmsHub (RU), Sms-reg (RU), TempNumber, Twilio або *маркет-плейси готових акаунтів соцмереж, e-mail чи месенджерів* – Accsmarket (RU), AccountsStore (RU), Buyaccs.com (RU), DarkStore (RU), Install-shop (RU), Olimp-shop.net (RU) та ін.



• номер кредитної карти (та пов'язані з ним персональні дані) – CardGeneration, CardGenerator, CardGuru, Fake Credit Card Number Generator, VCCGenerator.

Важливо – оплату акаунтів соцмереж, VPN, Telegram-ботів, мобільних операторів (сервіс Bitrefill) чи будь-якого функціоналу вебсервісів бажано здійснювати через некастодіальний криптогаманець.

Для того, щоб створити ефективну систему технічної безпеки пошукової роботи в мережі «Інтернет», необхідно розуміти потенційні **загрози анонімності** (або вразливості онлайн-середовища) та мати уявлення про засоби їх мінімізації. До основних з них можна віднести:



а) IP-адресу (Internet Protocol Address) – унікальний номер пристрою в комп'ютерній мережі, що використовується для адресації передачі даних. Для версії протоколу IPv4 він являє собою комбінацію з 4-х чисел від 0 до 255, розділених крапками (наприклад, 192.168.0.154 або 203.113.89.134). Коли ви переглядаєте вебсайт або з'єднуєтесь з мережевим комп'ютером, то отримуєте доступ саме до певної IP-адреси. Значуще ім'я того чи іншого інтернет-ресурсу або пристрою (наприклад, rada.gov.ua чи user) – це просто спосіб відобразити таку IP-адресу, щоб людина змогла її простіше запам'ятати.

Прив'язка IP-адреси до значущого імені відбувається за допомогою технології DNS (Domain Name System). Коли користувач вводить в адресному ряд-

ку браузера назву сайту, наприклад google.com, комп'ютер запитує його IP-адресу на спеціальному DNS-сервері та після отримання коректної відповіді відкриває вебсторінку. DNS-сервер – це спеціалізований комп'ютер (або група комп'ютерів), що зберігає IP-адреси сайтів у відповідності до їх значущих імен і обробляє запити користувачів. В інтернеті багато DNS-серверів, вони є й у кожного провайдера для обслуговування абонентів.

IP-адреса пристрою може *статично* визначатися адміністратором мережі (провайдером) або при кожному підключенні надаватися *динамічно* через протокол DHCP (Dynamic Host Configuration Protocol, дозволяє комп'ютеру автоматично отримувати параметри, необхідні для роботи в мережі).

З огляду на діапазон IP-адреси поділяються на *приватні* (т.зв. сірі, використовуються в межах локальної/домашньої мережі або LAN) та *публічні* (т.зв. білі, призначені для адресації у всесвітній мережі або WAN). Наприклад, якщо в помешканні є Wi-Fi-роутер, то кожний пристрій (комп'ютер, смартфон, телевізор тощо) зазвичай динамічно підключається до його приватної мережі та отримує «сіру» IP-адресу для внутрішньої ідентифікації. Дізнатись її можна в налаштуваннях маршрутизатора або в операційній системі (далі – ОС) за допомогою консольної команди *ipconfig /all* (ОС Windows), *ifconfig en0* (MacOS) чи *ifconfig -a* (Unix ОС). Для виходу в інтернет пристрої приватної мережі (з «сірими» IP-адресами) використовують надану провайдером публічну IP-адресу («білу») за допомогою механізму NAT (трансляції мережевих адрес, що замінює приватну IP-адресу на публічну).

За аналогією з поштовим індексом, публічна IP-адреса користувача дозволяє визначити назву провайдера та його місцезнаходження – 2ip.ua, Browserleaks, CentralOps, Deviceinfo, ipapi, ipleak.net, ip-score.com, Whoer (RU), Whois. Водночас відповідному DNS-серверу постійно передаються дані про звернення особи до певного вебресурсу (наприклад, Dnsleak, Dnsleaktest, ViewDns.info). Тому маскування своєї публічної IP-адреси дозволяє уникати відстеження, обходити територіальні обмеження та відвідувати заблоковані сайти. Найбільш поширеними способами такого *приховування* є використання *VPN*, *проксі-серверу*, *Tor-браузеру* або *публічної мережі Wi-Fi*.

VPN (Virtual Private Network) – це віртуальна приватна мережа, що працює усередині наявного інтернет-з'єднання користувача, являючи собою захищений тунель від пристрою до VPN-сервера, який адмініструє цю мережу (надає IP-адресу та DNS-сервер) і пропускає через себе увесь його трафік. Інформація про активність особи в інтернеті спочатку направляється на VPN-сервер, а вже потім у зашифрованому вигляді до провайдера та далі – до зовнішніх ресурсів.

Основні переваги: *анонімність в мережі* (інтернет-трафік повністю шиф-

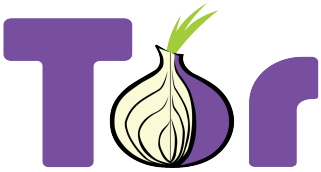
рується та недоступний третім особам, наприклад провайдеру; замість реальної IP-адреси використовується IP-адреса VPN-сервера; аналогічно і DNS), ***обхід блокування*** (змінюючи IP-адресу, ви змінюєте геолокацію, що дозволяє обходити блокування доступу до інтернет-ресурсів певної країни чи з окремої IP-адреси), ***захист від перехоплення і викрадення даних*** (при відвідуванні сумнівних сайтів або підключенні до безкоштовних Wi-Fi-мереж, трафік користувача може бути перехоплений, а його чутливі дані - метадані, паролі, cookie, сесії тощо - викрадені через відсутність шифрування та/або реалізацію сценарію хакерської атаки «людина посередині», Man-in-the-Middle або MITM).

Існують *платні* та *безкоштовні* VPN, у формі *програми на рівні ОС* (це бажаніше, оскільки весь трафік пристрою йде через VPN-сервер) або *плагін для браузера* (захищає тільки підключення конкретного браузера).

Безкоштовність подібних сервісів (наприклад, BrowsecVPN, hide.me, ProtonVPN, TunnelBear, UrbanVPN) досягається за рахунок встановлення обмежень щодо обсягу трафіку чи швидкості роботи, кількості доступних серверів (країн), неможливості завантаження торентів або трансляції потокового відео, і, головне, непрозорості політики щодо конфіденційності.

Доцільно обирати VPN, в якому використовується потужне шифрування (наприклад, AES-256), підтримка надійних протоколів безпеки (OpenVPN, L2TP, IKEv2, WireGuard), захист від витоків через DNS (випадок, коли ваш провайдер відправляє DNS-запити незалежно від увімкненого VPN), технологія TrustedServer/її аналог (видаляє всі ваші дані при кожному перезапуску) та функція Kill Switch/її аналог (розриває з'єднання у разі втрати зв'язку з VPN-сервером, запобігає розкриттю справжньої IP-адреси). Тому платні рішення (зокрема, CyberGhostVPN, ExpressVPN, Mullvad VPN, Private Internet Access, SurfShark VPN) мають набагато кращий рівень захисту, вищу швидкість з'єднання, підтримку більшої кількості локацій чи підключених пристроїв, мультиплатформеність, анонімність оплати та облікових записів, відсутність журналів активності тощо. Але VPN не захищає від трекерів і не впливає на вже завантажені cookie.

Проксі-сервер (приміром, Anonymouse.ws, free-proxy.cz, Kproxy, ProxyScrape, Spys.one) – це пристрій-посередник для обміну даними між користувачем та цільовими вебресурсами. Хоча проксі-сервер підмінює реальну IP-адресу особи на власну, він, на відміну від VPN, не шифрує трафік та не приховує пошукові дії дослідника в глобальній мережі.



Tor Browser (The Onion Router, цибулевий або багатошаровий маршрутизатор) – захищена версія браузера Firefox, що виходить в інтернет за допомогою власної мережі анонімних проксі-серверів і віртуальних тунелів між ними (Tor Network) для забезпечення передачі даних на всіх етапах у зашифрованому вигляді. Аналогія з цибулею ґрунтується на реалізації в Tor наступного механізму.

Кожний пакет інформації, що потрапляє в цю мережу, проходить через три різні проксі-сервери (вузли), які щоразу обираються випадковим чином. Перед відправленням пакет послідовно шифрується трьома ключами: спочатку – для третього вузла, потім – для другого та в кінці – для першого. Коли перший вузол отримує пакет, він розшифровує верхній шар шифру (аналогія з тим, як чистять цибулину) і дізнається куди відправити пакет далі. Другий та третій сервер роблять аналогічним чином. Усередині мережі Tor трафік перенаправляється від одного маршрутизатора до іншого та остаточно досягає точки виходу, з якої чистий (нешифрований) пакет даних уже доходить до початкової адреси одержувача (сервера). У зворотньому напрямку трафік від одержувача спрямовується в точку виходу мережі Tor. До того ж маршрут проходження кожні 10 хв. змінюється випадковим чином. У підсумку жоден посередник не має доступу ані до вмісту, ані до адреси повідомлення. Його повна розшифровка відбувається тільки на сервері одержувача. Недоліком такого підходу є порівняно повільна робота самого браузера.

Найбільший ефект дає *поєднання роботи VPN та Tor*: крім приховування IP-адреси та шифрування трафіку, для забезпечення анонімності браузер не зберігає історію переглядів сайтів, файли cookie та будь-яку інформацію про відвідувані сторінки; всі користувачі мають однакові цифрові відбитки.

При підключенні для виходу в інтернет до публічної мережі Wi-Fi позитивний ефект досягається за рахунок використання «білої» IP-адреси такої мережі (на відміну від IP-адреси, наприклад, домашнього провайдера чи власного смартфона) у поєднанні з одночасною роботою невизначеної кількості інших її абонентів. Водночас вона вважається ризикованою, оскільки не захищає від хакерських атак, вірусів та інших кіберзагроз. Нею краще користуватися у крайньому випадку, попередньо запустивши надійний антивірус.

б) файли cookie – це фрагменти даних для подальшої ідентифікації користувача, які сайт за допомогою браузера зберігає на комп'ютері щоразу, коли він відвідуєте той чи інший ресурс. Після того, як людина вводить адресу певної вебсторінки, браузер шукає на пристрої файл cookie цього сайту та, якщо його знаходить, надсилає на сервер ресурсу. Сайт «впізнає» користувача й автоматично підлаштується – форми реєстрації будуть заповнені, мовні та регіональні вподобання задані. Якщо браузер не знаходить cookie, сайт вважає вас новим відвідувачем і просить дозволу на збереження таких файлів.

Слід наголосити, що cookie, кеш та автозаповнення – доволі різні технології. Кеш – це копії великих за розміром даних сайту, що зберігаються на

пристрої (наприклад, зображення, відео та музика). Під час повторного відвідування сайту браузер не запитуватиме цю інформацію знов, а візьме її з кешу, завдяки чому вебсторінка завантажиться швидше. Автозаповнення – функція браузера. Він запам'ятовує дані, введені користувачем при заповненні форм на сайті (ім'я, номер телефону, пошта тощо), і, якщо потрібно ввести схожий текст на іншому ресурсі, пропонує ці збережені варіанти.

Cookie використовуються для: *управління сеансом* (вхід до облікового запису, IP-адреса та місцезнаходження користувача; дата й час відвідування сайту, версія ОС і браузера), *персоналізації* (мова, валюта, розмір шрифту або масштаб сторінки), *трекінгу поведінки* (кліки та переходи, таймінг знаходження на вебресурсі, переглянутий товар або реклама, обрані фільтри сортування, вподобання, лайки, введений текст – телефон, e-mail, банківська картка, коментарі тощо).

Їх умовно поділяють на: *сесійні* (знаходяться в оперативній пам'яті й автоматично видаляються після закриття вкладки браузера) та *постійні* (зберігаються на пристрої до певної дати або впродовж визначеного періоду); *власні* (створюються безпосередньо на сайті, який відкрив користувач) та *сторонні* (на сторінці розміщено клікабельний матеріал інших ресурсів на кшталт банерів або браузерні скрипти, приміром, Google Analytics, Facebook, Google AdSense тощо); *обов'язкові* (необхідні для нормального функціонування сайту); *зомбі-cookie* (флеш-cookie або супер-cookie, це сторонні постійні cookie, які мають унікальну здатність відновлюватися після видалення; за їх допомогою вебресурси можуть блокувати окремих користувачів або поширювати шкідливий програмний код).

Зазвичай файли cookie зберігаються на дисковому накопичувачі комп'ютера в папці відповідного браузера. Здебільшого вони безпечні (це звичайні текстові файли) і не здатні якось вплинути на роботу ОС. Але технологія, що мала б зробити вебсерфінг більш зручним, сьогодні все частіше використовується на шкоду користувачу – проконтролювати, яку саме інформацію збирають про нього cookie, вкрай важко. Так само ніхто не зможе гарантувати повної безпеки процесу обміну цими даними – cookie можуть бути перехоплені або вкрадені, щоб відстежувати попередні дії людини в мережі або мати доступ до її акаунтів. З огляду на це власників сайтів зобов'язали попереджати про використання cookie (наприклад, відповідно до Загального регламенту ЄС щодо захисту даних GDPR або закону Каліфорнії про захист конфіденційності споживачів CCPA). Але поки ви не погодитеся хоча б на мінімальний набір cookie, повноцінний перегляд сайту може виявитися недоступним.

Зі свого боку користувач може тільки заборонити браузеру використовувати певні cookie або час від часу видаляти їх. Наприклад, у Google Chrome для *блокування сторонніх cookie* слід натиснути три крапки в правому верхньому куті й перейти у «Налаштування» → «Конфіденційність і безпека» → «Сторонні файли cookie» та обрати між «Дозволити використання сторонніх файлів cookie», «Блокувати сторонні файли cookie в режимі «Інкогніто»

або «Блокувати сторонні файли cookie»; для *видалення cookie* – «Налаштування» → «Конфіденційність і безпека» → «Очистити історію» та обрати «Файли cookie та інші дані сайтів» (суцільне) або «Налаштування» → «Конфіденційність і безпека» → «Сторонні файли cookie» → «Подивитися всі дозволи та дані сайтів» (вибіркове). Але наразі цей браузер не підтримує опцію «Видаляти файли cookie та дані сайтів при закритті усіх вікон».

Онлайн-сканери 2gdpr, Cookie Compliance Audit Tool (плагін для Chrome), CookieServe, CookieYes, Piwik та ін. дозволяють попередньо перевіряти cookie сайту за посиланням на нього. Захист від різних форм відстеження з використанням cookie здійснюється за допомогою браузерних *антитрекерів* – Bitdefender's Anti-Tracker, Disconnect.me, Ghostery, Privacy Badger, Privacy Possum тощо, а також плагінів для *блокування реклами* – Adblockplus, AdBlocker Stands, Genius PRO, Popup Blocker, uBlock Origin.

Подальшим кроком у розвитку сесійних і постійних cookie для резервування даних стала поява Web Storage (веб-сховище або DOM-сховище). Ця технологія дозволяє сайтам зберігати значний обсяг інформації (до 10 Мб) на пристрої користувача, не пересилаючи їх кожного разу на сервер, та отримувати доступ через спеціальний алгоритм. За аналогією з cookie різновидами Web Storage є *сесійне сховище* (SessionStorage) та *локальне сховище* (LocalStorage). Забезпечити приватність допоможе їх регулярне очищення вручну (див. видалення cookie) чи за допомогою плагінів ClearLocalStorage, Click&Clean, Local Storage, LocalStorage Manager, OneClick Cleaner тощо.

в) цифровий відбиток браузера (Browser Fingerprint) – це унікальний ідентифікатор конфігурацій браузера та ОС користувача, який формується на основі зібраних даних різними технологіями відстеження вебсайтів. При цьому не використовуються традиційні методи ідентифікації, такі як IP-адреса та унікальні файли cookie. Цифровий відбиток браузера має вигляд 32-бітного числа шістнадцяткової системи (приміром, 249821af43932314621f1246618ea8e1), що отримується в результаті обробки всіх прийнятих від браузера даних. Він дозволяє відстежувати користувачів у мережі «Інтернет» із точністю до 94%.

В залежності від налаштувань вебресурсу відбиток формується на основі різної кількості параметрів (в середньому – від 7 до 15, максимально – понад 40), зокрема: *IP-адреса*, *user-agent* (дані про браузер, встановлену ОС та сам пристрій), *налаштування браузера та пристрою* (роздільна здатність екрану, його розміри, глибина кольору; мова браузера, інші встановлені мови; налаштування дати, часу, шрифтів; наявність плагінів та їх характеристики), *графічні технології браузера* (зокрема, відображення графіки та 3D-зображень Canvas та WebGL - на їх

основі алгоритми відстеження генерують ще один унікальний fingerprint), *WebRTC* (плагін для потокової передачі аудіо- та відеоконтенту, через який можна визначити справжню IP-адресу користувача, навіть якщо він використовує VPN), *JavaScript і HTML5* (властивості Document Object Model - те, як вебсторінка інтерпретується браузером; збережені дані LocalStorage і SessionStorage; налаштування параметру «Do not track» – не відслідковувати), *HTTP-заголовки* (відомості для обробки запитів/відповідей між браузером і сервером; наприклад, заголовки Accept-Language вказують на мову, якій користувач надає перевагу), *CSS* (те, як браузер інтерпретує й обробляє запити мови стилю сторінок), *налаштування cookie та supercookie*, *поведінкові фактори* (швидкість набору тексту, патерни рухів мишею, пошукові запити, історія відвідувань) та ін.

Збір відбитка браузера на даний час вважається допустимим і, на відміну від cookie, не потребує формального дозволу від користувача. Cookie більше схожий на інструмент стеження – щойно він опиниться в комп'ютері, сайт знатиме, де особа перебуває та чим займається. Відбиток браузера більш статичний і використовує отримані дані для визначення того, хто ви, але не може стежити за вами. При цьому cookie можна блокувати або видалити, а цифровий відбиток – ні (оскільки більша частина відомостей, які він передає, важлива для інтернет-серфінгу, відключити його майже неможливо). Останній використовується з метою запобігання шахрайству (інтернет-банкінг, накрутка реклами, блокування підозрілих акаунтів), внутрішньої аналітики та оптимізації перегляду вебконтенту, формування профілю особи в маркетингових цілях (стать, вік, сімейний статус, рівень матеріального достатку, інтереси, звички чи навіть персональні дані).

Унікальність цифрового відбитку вашого браузера можна дізнатися за допомогою ресурсів 2ip.ua, AmIUnique, Browserleaks, CoverYourTracks, Creepjs, Deviceinfo, ipleak.net, ip-score.com, Pixelscan, webkay.robinlinus, Whoer (RU) та ін. Чим більше ви намагаєтеся захистити від його зняття, тим більше унікальним стаєте та тим легше вас ідентифікувати (т.зв. інформаційна ентропія). Зміна браузера (або використання декількох одночасно) вже не вирішує цю проблему повністю з огляду на існування крос-браузерної дактилоскопії (Cross-Browser Fingerprinting). Відстеження деяких відбитків браузера можна просто заблокувати й тоді сайти не бачитимуть ваш цифровий профіль. Але подібне приховування стає підозрілим для їх систем моніторингу, що може вплинути на коректний доступ до певних ресурсів.

Основні *заходи протидії*: 1) максимальне *надання браузеру середніх значень* (наприклад, використання налаштувань за замовчуванням, незмінність мови, часового поясу та країни, відсутність плагінів тощо); 2) *ручна зміна* або встановлення *плагінів для приховування окремих складових* цифрового відбитку (приміром, AudioContext Fingerprint Defender, Canvas Fingerprint Defender, Fingerprint Spoofing, Font Fingerprint Defender, NoScript, Random User-Agent (Switcher),

User-Agent Switcher, WebGL Fingerprint Defender, WebRTC Network Limiter, WebRTC Protect). Дійсно, зміна навіть одного елемента відбитку своїм наслідком має автоматичну корекцію всієї хеш-суми ID користувача (формально вона стає іншою). Хоча точність ідентифікації у цьому випадку знижується лише на 0,3%, можуть з'являтися певні невідповідності окремих складових між собою, наприклад, useragent не збігатиметься з ядром браузера та його версією, IP-адреса не відповідатиме такій за WebRTC тощо; 3) *використання антидетект-браузерів* (вони підміняють оригінальний цифровий відбиток фейковим), приміром, AdsPower (free – до 5 профілів), Dolphin-anty (free – до 10 профілів), Ghost Browser (free – до 4 профілів), Incogniton (free – до 10 профілів), Mullvad (як і Tor дозволяє змінювати фейкові відбитки), Switch Antidetect (free – до 5 профілів, доступ через VPN), Undetectable (free – до 10 профілів) та ін.; 4) задіяння *виділеного серверу* (Dedicated Server) – окремого фізичного комп'ютера, що не передає в мережу інформацію про кінцевого користувача та його пристрій. Він порівняно вартісний та потребує фахового налаштування.

Щоб нейтралізувати певні вразливості, які здатні ідентифікувати користувача, можна застосувати віртуальну машину (Virtual Machine), що емулює (імітує) роботу комп'ютера чи смартфона. Ця платформа використовує тільки виділені їй потужності пристрою, на якому працює, у всьому іншому – це ніби окремий фізичний девайс, що дозволяє встановлювати та запускати програмне забезпечення, інколи навіть несумісне з поточною ОС. Тому при роботі в інтернеті він має зовсім інший цифровий відбиток браузера, ніж реальний пристрій та відокремлене від нього середовище, що позитивно позначається на захисті від різного роду кіберзагроз (наприклад, запуск потенційно небезпечних додатків, що можуть пошкодити ОС або вплинути на роботу інших програм; пошук в DarkNet).

Віртуальну машину можна в будь-який момент видалити та знову встановити з бажаними параметрами, налаштувати під окремі види пошукових завдань, тиражувати тощо. Але подібна платформа для своєї роботи потребує певний обсяг оперативної пам'яті, процесорного часу та дискового простору, що може серйозно вплинути на продуктивність усієї системи.

Для початку роботи з нею необхідно: завантажити відповідну програму, приміром KVM, Microsoft Hyper-V (вбудована в ОС Windows), QEMU, VirtualBox, VMware Workstation Player (free – запуск однієї віртуальної машини на ПК з ОС Windows або Linux) та ін.; встановити її відповідно до доданої документації; завантажити ISO-образ бажаної ОС, створити віртуальну машину, визначити їй системні ресурси та запустити; налаштувати гостьову ОС, інсталювати потрібні програмі компоненти для здійснення пошуку.

Отже, яку ОС обрати в якості базової для розвідки з відкритих джерел? Відповідь на це питання залежить від поточних потреб і рівня знань. Зокрема, на базі ОС Linux існує низка OSINT-орієнтованих збірок – CSI Linux, Kali Linux, ParrotOS, Tails, Trace Labs OSINT VM, Tsurugi Linux, Whonix, що пропонують широкий набір пошукових інструментів «з коробки», забезпечують належну анонімізацію процесу збору інформації, дозволяють створювати ізольоване програмне середовище при запуску через віртуальну машину або з портативного носія. Але вони вимагають наявності певних навичок для їх встановлення, налаштування та експлуатації.

Отже, найкращий вибір – це ОС, яку ви вмієте конфігурувати та в інтерфейсі якої почуваєте себе комфортно при повсякденній роботі.

Смартфон (або планшет) зараз являє собою цілу екосистему, що включає браузери, месенджери, соціальні мережі та інші застосунки, які розроблюються спеціально для мобільних ОС. Емулятор мобільної ОС – це інструмент для створення на комп'ютері віртуального пристрою на Android OS чи iOS та запуску відповідної програмної оболонки. Щоб імітувати реальний пристрій, емулятори або використовують власну реалізацію віртуалізації, або працюють із вже готовими варіантами віртуальних машин.

Найбільш популярні *емулятори Android OS*, наприклад BlueStacks, KoPlayer, LDPlayer, MEmu, MuMu Player, NoxPlayer, XePlayer, дозволяють обирати модель смартфону, створювати його IMEI, номер мобільного оператора, встановлювати застосунки з маркету Google Play чи з наявних apk-файлів, активувати Root-права (як правило в безкоштовних версіях присутня реклама у вигляді блоку рекомендованих додатків у нижній частині головного екрану).

Серед *емуляторів iOS* слід назвати Air iPhone, Appetize.io (браузерний застосунок, free – один користувач, два активні пристрої, тривалість сесії – 3 хв., загалом 30 хв. щомісячно), iPadian (free – обмежена кількість застосунків на маркеті App Store, наявність реклами) та Xcode Simulator (входить до складу Xcode – фірмового середовища для розробників від Apple).

Шкідливе програмне забезпечення (Malicious Software або Malware, ШПЗ) – це загальний термін для низки мережевих кіберзагроз, включаючи віруси, шпигунські програми, трояни, рекламні застосунки, хробаки, програми-вимагачі та ін. ШПЗ може потрапити на пристрій внаслідок фішингу, відкриття заражених посилань або листів, завантаження підозрілих

файлів, іншої соціальної інженерії, зі змінних носіїв, через вразливості ОС. Для захисту від ШПЗ, зокрема, використовують антивірусні програми.

Складніше ситуація виглядає з вебресурсами, що перебувають у вільному доступі для невизначеної кількості користувачів з усього світу. *Ознаки зараження сайту*: поява повідомлення браузера з попередженням про небезпечний ресурс під час переходу на нього; перенаправлення на іншу сторінку при спробі зайти на сайт або перейти за внутрішніми посиланнями; поява додаткового контенту на ресурсі, будь-яких оголошень або спливаючих вікон; повільна робота або недоступність вебсторінки тощо.

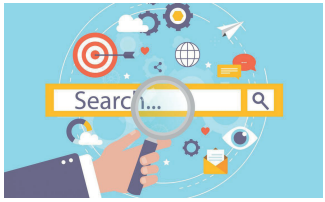
У процесі індексації сайтів пошукові системи перевіряють їх на ознаки зараження, блокують потенційно небезпечний вміст, ведуть і оновлюють «чорні списки» шкідливих ресурсів. Єдине, що не можуть вони гарантувати, – це відсутність ШПЗ у файлах, які доступні для скачування на таких сторінках. Наприклад, результати перевірки сайтів пошуковим сервісом Google можна дізнатися за допомогою Google Safe Browsing.

Також варто користуватися онлайн-сервісами для *виявлення шкідливих програм чи підозрілих посилань* на вебресурсах – Astra Malware Scanner, phish.ly (сканування листів), Quttera, ScamSearch.io (база даних шахраїв та шахрайських сайтів), Sucuri SiteCheck, urlquery, urlscan.io, URLVoid, WhereGoes, *сканування завантажених файлів* – Cuckoo Sandbox, InQuest, Intezer (потребує реєстрації, free – 2 тижні, потім 10 сканувань публічних файлів щомісяця), Recorded Future Triage (потребує реєстрації), Unpacme, Yomi або *універсальними рішеннями* – Any.Run (потребує реєстрації), Hybrid Analysis, Joe Sandbox, malsub (GitHub), OPSWAT, Squarex (потребує реєстрації), VirusTotal, а також для *перевірки за списками спаму* – Blacklistalert.org, DNSChecker, DNSstuff, MultiRBL.valli.org, MXToolbox, RblHostingUkraine, SPAMHaus.org.

Варто наголосити на тому, що забезпечити 100% захист від ШПЗ з використанням лише перерахованих ресурсів практично неможливо. З метою запобігання зараженню та уникненню негативних наслідків бажано використовувати комплексні рішення на основі платних антивірусних програм.

У наш час багато подібних продуктів постачаються не в «чистому» вигляді, а з багатьма додатковими опціями: можливістю резервного копіювання важливих даних, наявністю додатку для безпеки смартфонів чи планшетів, просунутим мережевим екраном (Firewall або брандмауер), функцією «батьківського контролю», одночасним встановленням на кількох пристроях, невідновлювальним знищенням файлів або їх шифруванням, можливістю увімкнення VPN, вебзахистом у режимі реального часу, скануванням електронної пошти та ін.

4. Універсальні пошукові інструменти



Пошукова система (або пошуковик) – це вебсайт, що надає можливість знаходження інформації в інтернеті. Користувач вводить необхідний запит, розпочинаючи процес пошуку, після чого отримує систематизований список посилань, які максимально релевантно йому відповідають. Інформацію зручно шукати за ключовим словом або фразою (набір слів або словосполучень, що найбільш точно відображають зміст необхідних відомостей).

Кожний пошуковик має власний алгоритм роботи, в основу якого покладено наступні етапи: ***сканування*** (спеціальний робот постійно відшукує нові вебсторінки, заносить їх до переліку вже відомих та зберігає розміщений контент); ***індексація*** (відбувається обробка завантажених ресурсів з використанням різних лексичних і морфологічних алгоритмів, структурування та додавання відомостей до «картотеки» пошуковика); ***ранжування*** (програма аналізує запит користувача, відбирає з бази сторінки, що найбільш з ним пов'язані, та виводить результати у вигляді списку посилань, відсортованих відповідно до релевантності цьому запиту).

Вже тривалий час найпопулярнішою пошуковою системою залишається Google (у 2024 році на нього припадає понад 92% всіх запитів у світі), через що дієслово «погуглити» стало синонімом знаходження інформації в інтернеті.

Особливості пошуку за допомогою Google:

– пошуковик читає запит зліва направо, ігнорує регістр букв і знаки пунктуації, вміє відміняти слова, довжина – не більше 32 слів;

– перші за порядком слова більше впливають на релевантність видачі;

– пошук ведеться мовою запиту;

– за замовчуванням між словами стоїть логічний оператор «і»;

– розпізнає текст в документах (файли .pdf, .rtf, .docx, .xlsx, .pptx та ін.);

– результат пошуку персоналізований (залежить від місцезнаходження користувача, типу пристрою, його вподобань, попередніх запитів чи проглянутих сайтів, реклами тощо) та не обов'язково є точним співпадінням запиту (інший відмінок, число або синонім); неперсоналізована видача – за допомогою режиму «Інкогніто» або команди google.com#q=google&pws=0;

– пошуковик рекомендує список корисних, на його думку, форматів контенту – *Google Featured Snippets* (блок з короткими відповідями, що виводиться в окремому вікні та розташовується на нульовій позиції пошукової видачі);

– на формування списку посилань може впливати цензура з огляду на порушення прав певних осіб (авторських прав, права на забуття тощо);

– Google не може індексувати інформацію, доступ до якої можливий лише для авторизованих користувачів чи після заповнення певних форм, а також коректно отримувати дані з відео- та аудіоконтенту.

Google – безумовний лідер у сфері інтернет-пошуку, але далеко не монополіст. Хоча інші пошуковики не настільки відомі, але вони також обробляють мільйони пошукових запитів щодня. Тому під час знаходження певних даних завжди доречно задіювати можливості альтернативних пошукових систем в доповнення до Google, особливо коли останній не дає очікуваних результатів. *Відмінність у кілька посилань може бути важливою, якщо це буде саме те, що ви шукаєте*:

• Microsoft Bing (частка на ринку ~ 3,3%) – за функціоналом Bing та Google доволі схожі, проте пошукові алгоритми все ж трохи відрізняються (Bing відстежує більше взаємозв'язків між окремими вебсайтами, краще опрацьований пошук зображень та відео); у видачі відображається багато додаткових даних у віджетах; для зручності ведеться журнал пошукових запитів, а також колекції (окремі пошукові проєкти для збору різнопланових даних з можливістю їх продовження); інтегровано чат-бот BingAI (на основі OpenAI GPT-4) з метою розширення пошукових можливостей та інтерактивний чат для створення текстового контенту (постів для соціальних мереж, електронних листів, статей тощо);

• Яндекс (RU, частка на ринку ~ 1,5%) – орієнтований на рунет, заблокований в Україні (доступ можливий через VPN), підконтрольний роскомнагляду держави-агресора, дозволяє здійснювати ефективний пошук за фото та відео, а також контентом популярних соцмереж;

• Yahoo! (частка на ринку ~ 1,3%) – у 2009 р. пошуковик купила компанія Microsoft і від тоді всі пошукові запити через Yahoo! виконуються в системі Bing; спеціалізується на пошуку в сфері новин, спорту та фінансів, майже невідомий для більшості користувачів;

• Baidu (частка на ринку ~ 0,9%) – це китайський аналог Google. Платформа відображає результати китайською мовою та вкрай рідко використовується у вітчизняному сегменті інтернету;

• DuckDuckGo (частка на ринку ~ 0,6%) – пошуковик з відкритим вихідним кодом; окрім власного вебкраулеру він також використовує результати інших пошукових систем (у т.ч. Yahoo! та Bing), що дає більш релевантну видачу. Позиціонує себе як анти-Google – не збирає інформацію про користувачів, а тому не персоналізує результати, анонімізує історію пошукових запитів, не відстежує файли cookie та ін. Дозволяє легко шукати інформацію на інших мовах, тоді як Google персоналізує видачу за регіоном. Фільтрує результати пошуку, штучно приховуючи посилання, що вважає «дезінформацією». DuckDuckGo є пошуковою системою за замовчуванням у деяких антидетект-браузерах, зокрема Tor Browser та Vivaldi.

Пошук інформації в українському сегменті інтернету може бути розширений завдяки *вітчизняним сервісам* – i.ua, META, Search, Yep тощо.

Існують команди розширеного пошуку Google (*Google Dorks*), які допомагають уточнити та значно звузити пошукову видачу, зменшивши кількість нерелевантних результатів. Вони також можуть бути використані для пошуку вразливостей вебсторінок (про синтаксис інших пошукових операторів можна дізнатися з цього списку або за допомогою GoogleHackingDatabase):

Запит	*Приклади*
Пошук за прізвищем, ім'ям та по батькові	
Всі слова (опція)	G | новак іван петрович G | іван петрович новак G | novak ivan petrovich
Точне співпадіння	G |«Новак Іван Петрович»
Один з варіантів	G |«Новак Іван Петрович» | «Новак І. П.»
Всі варіанти	G |«Новак Іван Петрович» & «Новак І. П.» & «Н.І.П.»
Групування	G | новак (іван | иван) петрович G | (іван | иван | і.п. | и.п. | і. | и.) новак
За виключенням	G | новак іван петрович -підприємець
З додаванням	G |новак іван петрович +адвокат
Невідома літера, слово, фраза	G |новак * петрович
Діапазон	G |новак іван 2019..2024
Файли певного типу	G |новак іван петрович filetype:pdf (або .xls(x), .doc(x), .ppt(x), .rtf, .txt, .jpeg, .zip, .mp4 тощо)
В локації	G |новак іван петрович loc:харків
На форумах (блогах)	G |новак іван петрович inurl:forum G |новак іван петрович inurl:blog
Пошук профілю в соціальних мережах	
На певному сайті (домені)	G |(іван | иван) новак site:facebook.com (чи на інших – instagram.com, twitter.com, vk.com, ok.ru тощо)
За тегами та хештегам	G |ivannovak@instagram (для X/Twitter, Facebook, Instagram) G |#адвокатихаркова (для Instagram, VK, Facebook, Tumblr, TikTok)
Кеш видаленої вебсторінки*	G |cache:https://www.rada.gov.ua/ G |cache:https://vk.com/id413593960 *з лютого 2024 р. не підтримується, хоча може спрацювати
Пошук електронної пошти за відомим нікнеймом	
Слово в адресі вебсторінки (url)	G |inurl:novak_ivan site:mail.ru (allinurl: - всі слова) (чи на інших – gmail.com, ukr.net, i.ua, meta.ua, yahoo.com, yandex.ru тощо)

Запит	*Приклади*
Пошук контактного телефону особи	
	(новак іван петрович) & (мобильный | мобильник | мобила | моб. | сотовый | сотик | телефон | трубка | труба | мобільний | мобільник)
Пошук інформації щодо особи в публікаціях (новинах)	
Слова в заголовку	allintitle:резюме новак іван (intitle: - перше слово)
Слова в тексті	allintext:адвокат новак іван (intext: - перше слово)
Схожа сторінка	related:https://traditionorder.info (сайт політичного руху)
Інші слова між	новак AROUND (2) адвокат (у дужках - кількість інших слів)
Синоніми	новак іван ~адвокат
Результати до та після певної дати	новак іван before:2022-02-24 новак іван after:2022-02-24
Сайти, що посилаються на url	link:novak.com

Подібні Dorks мають й інші пошукові системи. До того ж в одному запиті можуть використовуватися декілька операторів (наприклад, новак іван site:*.ua filetype:pdf), а функціонал окремих з них продубльовано в інтуїтивно зрозумілому інтерфейсі розширеного пошуку, кнопках «Всі фільтри» та «Інструменти» під пошуковою строкою браузера Google Chrome.

Багато в чому **ефективність пошуку залежить від підходу**:

– *креативність важливіше алгоритмів* – змоделюйте кінцевий результат пошуку, творчо підходьте до вибору ключових слів, комбінуйте варіанти їх написання, додавайте нові, задіюйте синоніми, абревіатури, ставте себе на місце об'єкта зацікавленості тощо;

– підвищити точність пошуку допомагає *використання унікальних ключових слів*, що написані рядковими (малими) літерами потрібною мовою, а також застосування функції браузера «Знайти схожі документи»;

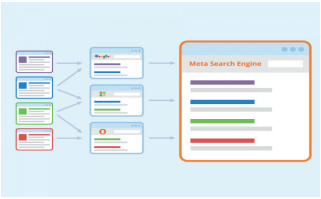
– переглядайте якомога *більшу кількість посилань пошукової видачі* – ви зможете натрапити на менш популярні, проте більш корисні ресурси;

– *шукайте поширені типи файлів на офіційних сайтах* органів місцевого самоврядування, комунальних підприємств, закладів освіти, охорони здоров'я, дошкільних установ, громадсько-політичних утворень тощо. На них можна знайти документи, що містять актуальні персональні дані – списки учнів/студентів, черговості отримання житла чи земельних ділянок, пільгових ліків, платіжні доручення, договори, заяви, скарги, рішення та ін.

Корисним доповненням можуть стати *спеціалізовані сервіси* – De Digger (пошук загальнодоступних файлів на Google-дисках), FilePursuit (агрегує файли з

відкритих вебсерверів), ISearchFrom (пошук з іншого регіону/пристрою, іншою мовою), Keyword Tool (генерує ключові слова за темою), Mark My Search (плагін, підсвічує на сторінці слова з пошукового запиту), Oldest search (починає видачу з найстарішою за датою вебсторінки), 2lingual (одночасний пошук двома обраними мовами), а також *онлайн-перекладачі* – Bing.Translator, Deepl, Google тощо.

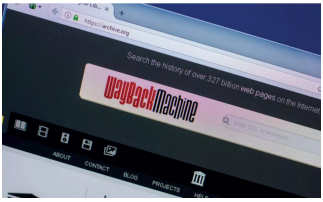
На жаль, жодна з існуючих пошукових систем не може самостійно охопити всі ресурси інтернету, що постійно та динамічно зростають. До того ж алгоритм пошуку різних пошуковиків у вже проіндексованих ними документах має певні відмінності. Потреба розширення їх функціональних можливостей шляхом агрегування в одному місці результатів пошуку найкращих подібних ресурсів зумовила появу метапошукових систем.



Такі вебсайти не мають власних баз даних і пошукового індексу. При опрацюванні запиту паралельно опитується низка «традиційних» пошуковиків та повертаються надані ними результати єдиним списком без дублювання посилань. З одного боку, це скорочує обсяг зусиль та заощаджує час, а з іншого – ранжовані таким чином результати роботи кількох пошуковиків за якістю можуть перевершувати суму видач метапошукових систем. Іншими словами, якщо посилань за запитом багато, то метапошук не потрібен і, можливо, навіть шкідливий, оскільки міксує різні алгоритми ранжування. Але якщо їх мало, то метапошук може бути корисним саме завдяки об'єднанню невеликої видачі окремих пошуковиків.

Найбільш поширеними метапошуковими системами є: BizNar (додатково надає аналітику результатів пошуку; позиціонує роботу з Deep Web – частиною інтернету, що недоступна для звичайних пошуковиків), BoardReader (пошук інформації з онлайн-форумів), Dogpile (презентується як пошуковик з максимально повною видачею; відсутність реклами), Excite, IntelligenceX (дозволяє обирати пошукові інструменти з наявного переліку), Fagan Finder, Gibiru, Izito, MetaCrawler, metaGer, OSINT Helper, searX, Startpage, WebCrawler, Webmii, ZapMeta та ін. Водночас більшість з них має достатньо обмежені синтаксичні можливості для побудови команд розширеного пошуку та роботи з кирилицею.

Вебархів, Internet Archive (The Wayback Machine) – сервіс для збору та збереження копій різних інтернет-сайтів (працює з 1996 р.). За його допомогою можна спробувати віднайти дані, що були з плином часу змінені (попередні версіїпевних вебсторінок) або вже стали недоступні (видалені).



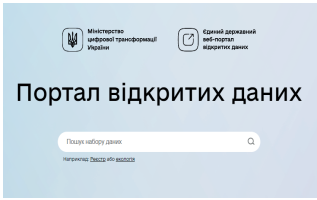
Аналогічно краулерам пошукових систем роботи Вебархіву за певним алгоритмом періодично відвідують і завантажують на свої сервери загаль-

нодоступний контент сайтів (від копіювання вміст можна приховати через пароль або параметри індексування ресурсу) – HTML-код, CSS-стилі та скрипти; зображення, відео та музику, документи тощо. Коли бот Вебархіву «приходить» на сторінку наступного разу, він не видаляє її попередню версію, а зберігає нову. Для початку пошуку необхідно ввести URL- адресу сайту та обрати, за яку дату хочемо подивитися можливо наявну копію. Так само *є можливість архівації ресурсів користувачем* (опція «Save page now» на стартовому вікні).

Сервіс Archive.today (почав роботу у 2012 р.) на відміну від Wayback Machine не використовує боти та архівує сайти *лише за ініціативи відвідувачів*. На головній сторінці є дві форми: верхня (червона) дає змогу архівувати, нижня (синя) допомагає знайти ресурс серед збережених. Сервіс ігнорує стандартне обмеження доступу (за допомогою файлу robots.txt) для пошукових роботів. За рахунок цього зберігає сайти, власники яких заборонили архівацію. Має кілька дзеркал: archive.is, archive.li, archive.ph, archive.fo та ін.

У цьому контексті додатково необхідно назвати ресурси CachedView (пошук в кеші Google, Coral та Internet Archive), Carbon Dating The Web (дата створення вебсторінки), Quick Cache and Archive search (одночасний пошук у 10 пошукових системах та 24 вебархівах), suIP.biz (RU, пошук за декількома вебархівами), Web Archives (плагін для Chrome) та Web-arhive.ru (RU).

Якщо сторінка відсутня у вебархіві, її можна спробувати віднайти за допомогою кешу пошуковика. Це остання відвідана та проіндексована краулером пошукової системи версія сайту – при черговому проході бот перезаписує її на нову, а стару видаляє (частота оновлення коливається від одного до чотирьох тижнів). На відміну від Bing та Яндекс у лютому 2024 р. Google видалив кнопку «cached» для результатів пошуку, хоча відповідний Dork продовжує функціонувати.

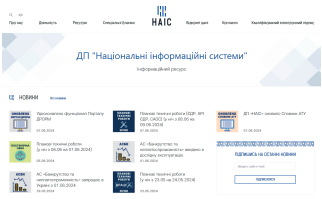


Єдиний державний вебпортал відкритих даних України призначений для вільного доступу та використання публічної інформації органів влади та управління, в т.ч. її автоматизованої обробки електронними засобами. Задекларована мета – забезпечення їх прозорого функціонування.

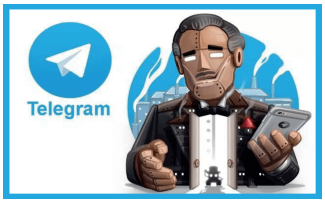
Інформаційно-довідкова документація (реєстри, довідники, договори, звіти, рішення, розпорядження, паспорти тощо) розподілена за 15-ма категоріями (наприклад, держава, економіка та бізнес, регіональний розвиток, юстиція та судочинство), а також за центральними та місцевими розпорядниками. Структура набору відкритих даних включає опис складу його елементів, їх формат (файли .txt, .doc(x), .pdf, .xsd, .json, .csv, .zip та ін.), параметри та призначення. На сьогодні портал містить майже *36 тис. наборів даних* суб'єктів владних повноважень та підтримує наскрізний пошук, а також пошук за групами

чи розпорядниками відповідної інформації.

Спорідненний проєкт Дія.Відкриті дані являє собою опис покрокових інструкцій використання наборів даних та інструментарію OpenDataToolkits для подальшого *посилення громадського контролю* за діяльністю органів державної влади та місцевого самоврядування, суб'єктів господарювання тощо шляхом *виявлення ознак можливих правопорушень чи недоброчесності* з їх боку, викриття корупційних схем.



Основною метою діяльності державного підприємства «Національні інформаційні системи» є технічне, технологічне забезпечення створення та супроводження ведення автоматизованих систем Єдиних та Державних реєстрів, що функціонують відповідно до наказів Міністерства юстиції України, а також інших електронних баз даних (приміром, відкриті дані з реєстрів), надання доступу до них, а також забезпечення збереження й захисту відомостей. Більш детально їх розглянемо у розділах 7 та 8 цього порадника.



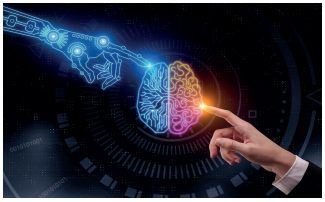
Telegram-бот (чат-бот) – це роботизований акаунт у месенджері Telegram, який запрограмований на автоматичне виконання певних дій: пошук необхідної інформації, продаж товарів, створення контенту тощо. Принцип роботи застосунку доволі простий: він передає повідомлення користувача на сервер, де відбувається обробка запиту, далі сервер надсилає відповідь боту, а той відображає її в месенджері. Як правило, такі утиліти мають інтуїтивно зрозумілий інтерфейс або приклади синтаксису команд.

Більшість Telegram-ботів для пошуку персональних даних осіб (т. зв. пробив) отримують відомості шляхом опрацювання відкритих джерел (пошукові системи та сервіси, соцмережі, форуми, онлайн-оголошення тощо, для чого задіюють API різних сайтів), витоків корпоративних баз даних (державних органів, операторів зв'язку, банків, медустанов, магазинів, страхувальників, служб доставки та ін.) або власних ресурсів (приміром, застосунки для визначення номеру телефону, результати анкетування користувачів або розсилки рекламних повідомлень) і в переважній більшості є платними (в т. ч. за криптовалюту). Безкоштовно інформація надається в обмеженому обсязі. Деякі з них мають реферальну систему (отримання особою внутрішньої валюти боту за залучення нових користувачів) та можливість створення власних пошукових утиліт (т.зв. дзеркал).

До найбільш популярних ботів для *універсального пошуку* можна віднести: BotoDetective (підписка), DataLeakAlert (RU, free – 1 тиждень), EyeGodsBot (RU), HimeraSearch (RU), InfoBazaBot (free – базовий функціонал), LeakOSINT (RU, free – реферальна система), LeakedInfoBot (RU, free – базовий функціонал),

Nemezida2UA (RU, підписка), OpenDataUA (free – базовий функціонал), QuickOSINT (RU, free – 2 запити), SmartSearchBot (RU, free – базовий функціонал), Unamer (RU), TSysBot (RU, підписка), Universal Search (RU, free – 10 запитів, кожні 8 годин вони поновлюються), UsersBox (RU, free – 7 запитів), Zernerda (RU, free – 2 запити), Архангел (RU, підписка) тощо.

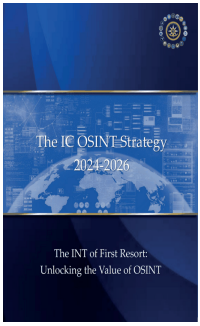
Telegram-боти – це доволі зручний спосіб зібрати потрібні відомості, підказати напрямок пошуку чи розширити набір вихідних даних для нього. Але під час роботи з ними *існують ризики* витоку персональних даних, отримання сторонніми особами доступу до пристрою дослідника, а також зараження ШПЗ через фішингові посилання. Ці застосунки можуть помилятися, видавати неправильні або застарілі дані, пропускати важливі деталі. Тому завжди необхідно дбати про власну безпеку, перевіряти отриману інформацію (використовувати різні джерела), а не повністю покладатися на неї.



Загальновизнаного визначення штучного інтелекту (ШІ) наразі не існує. Однак під ШІ в широкому сенсі розуміють спектр різних технологій, які працюють над підвищенням здатності машин та інтелектуальних систем (а саме комп'ютерів) виконувати дії, які подібні до людського інтелекту.

Щойно подібні системи будуть навчені розробниками, вони зможуть працювати відносно автономно та вдосконалюватись на власних результатах, стаючи все кращими. Зазначене зумовлено тим, що технології ШІ знаходять закономірності в даних, а потім використовують ці закономірності для подальшого прогнозування. Це схоже на те, як люди у себе в мозку на основі нейронних мереж формують свідомість і розуміння того, що відбувається.

Можна виділити такі сучасні технології, що використовують ШІ: машинне навчання, глибоке навчання, нейронні мережі, голосовий пошук, комп'ютерний зір, розпізнавання образів, генерування природної мови (NLG), обробка природної мови (NLP) тощо.



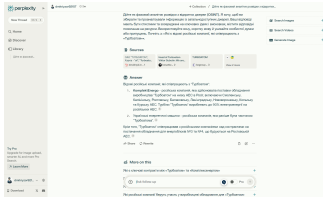
Американське розвідувальне співтовариство, визнаючи критичну важливість і зростаючий обсяг OSINT у своїй діяльності, розробило нову стратегічну ініціативу, спрямовану на вдосконалення збору відомостей, створення й надання результатів такої роботи. Центральне місце в ній посідає застосування ШІ і машинного навчання, що розглядаються як ключові в поліпшенні обробки відкритих даних.

Ці технології обіцяють підвищити ефективність і точність OSINT-досліджень за рахунок автоматизації виявлення та аналізу релевантної інформації з величезної кількості відомостей, наявних у відкритому доступі. Однак у стратегії також визнаються проблеми,

пов'язані із забезпеченням достовірності й достатності відомостей, та підкреслюють важливість розробки надійних механізмів перевірки даних.

Для нас уже давно став звичним *функціонал пошукових систем*, що з'явився завдяки впровадженню ШІ, – розуміння запитів природньою мовою людини, розпізнавання голосу, зворотний пошук зображень та геолокація, релевантне ранжування пошукової видачі, переклад вебсторінок.

Генеративний ШІ привернув увагу громадськості наприкінці 2022 р. із запуском ChatGPT, що став першим широкодоступним та достатньо простим у використанні чат-ботом на його основі. Подібні інструменти здатні імітувати здібності людини до створення текстів, зображень, відео, музики, програмного коду, перекладу та ін. Сьогодні мільйони людей користуються їх можливостями в повсякденному житті й потенціал адаптації певних моделей ШІ до специфічних сфер застосування здається майже безмежним.



З урахуванням змістовного наповнення етапів розвідувального циклу для потреб підвищення ефективності OSINT-досліджень зараз краще підходять **багатофункціональні моделі генеративного ШІ**, приміром ChatGPT, Claude AI, Google Gemini, Microsoft Copilot, Perplexity, You.com (для всіх free – базовий функціонал), основними шляхами **використання** яких є:

– безпосередній *пошук та збір даних з вебсайтів* щодо об'єктів зацікавленості (новини, профілі та публікації в соціальних мережах, дописи на форумах, публічні реєстри й бази даних, різноманітні документи тощо);

– *формулювання ключових слів, ідей* або *переліку ресурсів*, що здатні розширити пошук, *запитів Google Dork* чи для соцмережі *X/Twitter* з метою оптимізації кінцевої видачі, а також *синтаксису команд Github-утилит*;

– *написання та/або оптимізація коду скриптів для парсингу* (автоматизованого збору) даних, *моніторингу ресурсів*, інших періодичних завдань;

– технічний *переклад*, *транскрибація відео-* та *аудіоконтенту*, *обробка неструктурованих даних*, їх *систематизація* (наприклад, згадки про людей, організації, події або місця, статистика; текст, зображення, відео, посилання);

– *аналіз зібраних відомостей, підготовка звітів* (виявлення тенденцій, настроїв, загроз, закономірностей чи взаємозв'язків, формулювання висновків і прогнозів) та *їх візуалізація* (графіки, таблиці, діаграми, карти, схеми).

Використовуючи діалоговий режим, можна просто писати запити до чат-боту на природній мові людини так само, як ви це робите в пошуковиках, але, найімовірніше, це ні до чого корисного не призведе. Щоб отримати більш докладні й точні відповіді, необхідно ставити нейромережі деталізовані та чіткі завдання з використанням підказок (Prompts, промтів) – набору інструкцій для генерації (формування) певного кінцевого результату.

Коли ми не знаємо, як сформулювати промт, – доручіть це ШІ зробити самому. Одним з варіантів його створення є використання *конструкторів* – CHATGPT Prompt Generator, ChatGPT Prompt Generator, Chatgpt prompt generator, Free AI Prompt Generator, Gpt-Prompt (RU, для ChatGPT, YaGPT, GigaChat та Copilot), але краще це зробити *вручну* за певними **правилами**: *визначте роль*, яку має виконувати нейромережа; *чітко сформулюйте запит* (через покрокову інструкцію, опис, список ідей, порівняння підходів до розв'язання певної задачі вкажіть, що саме ви бажаєте отримати); *задайте обов'язкові умови* (для ШІ неухильним для виконання є те, що знаходиться в середині [квадратних дужок]); за потреби *розділіть запит на частини* (лапками, розділами або номерами пунктів, щоб чат-бот міг працювати з великим обсягом тексту або по-різному з кожною складовою); *вкажіть формат відповіді* та *стиль викладу*.

Наприклад, *«Дійте як фаховий аналітик розвідки з відкритих джерел (OSINT). Я хочу, щоб ви зібрали та проаналізували інформацію із загальнодоступних джерел. Ваші відповіді мають бути стислими та зосереджені на ключових ідеях і висновках, містити відповідні посилання на ресурси. Використовуйте ясну, коротку мову й уникайте особистої думки або припущень. Почніть з: «Знайдіть інформацію про співпрацю фірми «ABCDCBA» (м. Харків) з російськими компаніями після 24 лютого 2022 року»*.

Іншими словами, чим більше контексту ви надасте у промті, тим краще чат-бот може зрозуміти, що ви шукаєте, і відповісти більш релевантним чином, а подальші додаткові запитання користувача допоможуть уточнити попередні відповіді та отримати більше корисної інформації. Важливо перевіряти згенеровані(!) чат-ботом відомості, використовуючи критичне мислення та альтернативні джерела для їх підтвердження.

Наприкінці липня п.р. OpenAI оголосила про те, що працює над новим прототипом ШІ-пошуковика під назвою SearchGPT, який має надати користувачам можливість отримувати швидкі та чіткі відповіді з релевантних джерел в інтернеті. Він може стати наступним етапом розвитку іншої достатньо цікавої моделі для дослідників Globe Explorer. До того ж, функціонує магазин плагінів для ChatGPT – GPT Store.

5. Пошук за фото- та відеоконтентом, геолокація

Не завжди отримання необхідної інформації за допомогою текстових запитів є прийнятним. Тому доволі часто виникає потреба пошуку зображень та перевірки їх достовірності, оскільки вони можуть зловмисно або випадково вводити в оману, поширюючи неправдиві відомості. Верифікація фотографії передбачає, головним чином, встановлення першоджерела такої світлини, її автора, місця, дати й часу зйомки, обставин появи в глобальній мережі, наявності модифікованих елементів тощо.

Інструменти для визначення:

1) першоджерела фотоконтенту та його автора (т.зв. зворотний пошук – використання певного зображення як вихідного пошукового запиту; програми сканують картинку, виявляють метадані, визначають мітки та підбирають проіндексовані аналоги, можливі збіги або пов'язані за змістом зображення) через

• *загальні пошукові системи* – Bing, Google Images, Яндекс.Картинки;

• *спеціалізовані пошукові сервіси* – Betaface (аналіз та порівняння облич), Copyseeker, Faceagle, FactCheckTool (дата та час індексації першоджерела), Findclone (пошук для ВКонтакті, потребує реєстрації), Image Search, ImgOps, Lenso, Likelike AI (пошук для Instagram), PhotOSINT (плагін для Chrome, відображає метадані), PhotoSherlock, PhotoTrackerLite (плагін для Chrome), Reverse Image Search, RevEye Reverse Image Search (плагін для Chrome), SauceNAO, Search4faces (RU, пошук серед публічних персон, фото профілів ВКонтакті, аватарок ВКонтакті, Однокласники, Tiktok, ClubHouse), Search by Image (плагін для Firefox), Source search (RU, bot), TinEye, Who stole my pictures? (плагін для Chrome). Ресурси Clearview.ai, FaceCheck.ID та PimEyes є платними, але достатньо потужними інструментами.

Зворотний пошук може дати й негативні результати через налаштування приватності акаунтів соцмереж, непроіндексованість вебсторінок, вади самого зображення (приміром, низька якість, невдалий ракурс, велика часова різниця з датою зйомки) тощо. Тому доцільно знов спробувати відшукати фото після його *технічної обробки* (наприклад, масштабування, корекції кольору, виокремлення ключового фрагменту/обличчя, у дзеркальному відображенні та ін.):

• *комплексні інструменти* – BeFunky, IMGonline, MMagic (GitHub), Online-Fotoshop (RU), OnlineVideoCutter, TinyWow.ImageTools;

• *покращення якості зображень* – Bigjpg, Depix (GitHub, відновлює зображення, що приховано розмиттям або пікселізацією), Ihancer, Image Enlarger (free – 10 кредитів на місяць, зображення 1200x1200 пікселів, до 5 Мб), Image Upscaler Online, Img.Upscaler (free – 10 кредитів на місяць, зображення 2000x2000 пікселів, до 5 Мб), LetsEnhance.io (free – 10 кредитів та водяний знак), MyHeritage

(потребує реєстрації), Upscale.media (free – 3 фото), Waifu2x.net;

• *видалення зайвих об'єктів* – Aiseesoft Free, BGbye, Background Remover, Cleanup.pictures (free – роздільна здатність 720p), Clipdrop, Inpaint (free – низька роздільна здатність), Removebg, Watermark Remover.

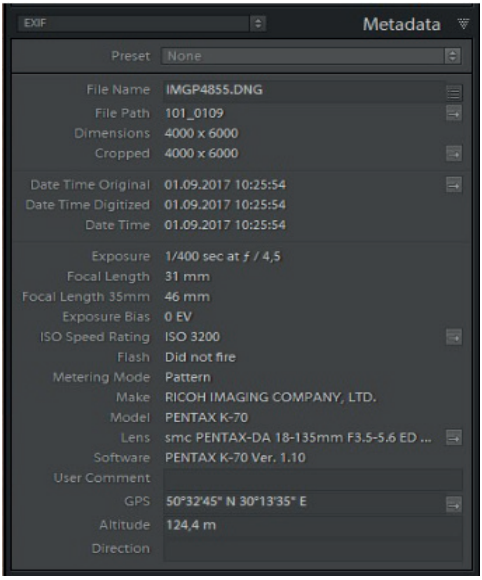
Зазвичай першоджерелом є зображення з найстарішою датою появи в інтернеті або з найбільшою роздільною здатністю.

Перевірка походження фото (дослідження цифрового сліду того, хто та яким чином його виклав) передбачає аналіз джерела, його онлайн-історії чи пов'язаних ресурсів/профілів, часу появи, характеру взаємодії з іншими користувачами, попередньо/додатково розміщеного контенту тощо. Також зображення можуть супроводжувати теги, коментарі або інші фрагмент тексту, що здатні допомогти при ідентифікації – спробуйте «витягнути» з них потенційні ключові слова (приміром, акроніми, назви місць чи їх опис, сленг тощо).

Звертайте увагу на підозрілі моменти – нещодавно створений акаунт, профіль з невеликою кількістю записів/підписників/підписок, раптову зміну географічного розташування автора, чи не є він ботом (наприклад, шляхом порівняння підписників особи з тими, на кого підписаний він сам) та ін;

2) метаданих EXIF (Exchangeable Image File Format) – це додаткова інформація про фотознімок, що зберігається на самому початку такого файлу до даних фактичного зображення (наприклад, марка та модель камери, її налаштування, дата, час і координати зйомки, назва програми, де здійснювалась обробка тощо).

Дізнатися EXIF-відомості можна за допомогою: *вкладки «Властивості»* контекстного меню файла; *софту для перегляду або редагування фото/метаданих* – ExifTool, Exiv2, GIMP, GeoSetter, IrfanView) *вебсервісів* – CameraSummary, Exifdata, Fotor, Get IPTC, GroupDocs, IMGonline, Jimpl, Metadata2go, snapWONDERS (також працює з відео, free – 10 запитів на день), ViewExifData) чи *плагінів для браузера* – EXIF.tools (для Chrome), ExifViewer (для Chrome), xIFr (для Firefox).

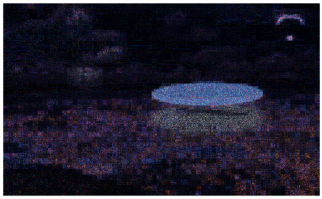


Аналогічну інформацію можна отримати для відео- або pdf-файлів, текстових документів, вебсайтів (тег <meta> в головній частині їх HTML-коду). Бажано використовувати декілька різних джерел для підтвердження правильності отриманих відомостей.

Водночас метадані не є пана-

цією – у вільному доступі існує багато прикладів програмного забезпечення, що дозволяє прибирати їх з файлів зображень або модифікувати. Соціальні мережі та месенджери автоматично видаляють EXIF одразу після завантаження/відправки такого фото;

3) справжньості знімку шляхом пошарового дослідження зображення (фотофорензіка) – Aperi'Solve, Digital Image Forensic Analyzer, Fake News Debunker (плагін для Chrome, також працює з відео), Forensically, FotoForensics, Ghiro (програма для ОС Windows), Image Edited?, Image Verification Assistant, JPEGsnoop (GitHub), Sherlog (GitHub). Для цього переважно використовується *метод ELA* (Error Level Analysis) – це аналіз критеріїв (артефактів) компресії у графічних файлах. Зазвичай вони однорідні для всієї картинки.



Якщо стосовно окремих елементів виявлено принципово інші артефакти компресії (яскраво виражені світлі, темні або райдужні області), це з високою долею ймовірності свідчить про їх чужорідність, тобто про потенційне корегування зображення у фоторедакторі. Вказаний метод також допомагає виявити й зміну яскравості або контрасту (поява білих цяток у таких зонах).

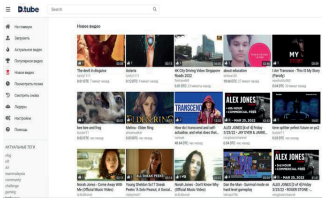
Щоправда, використання подібних сервісів буде вкрай неефективним, якщо фотографію кілька разів зберігали, особливо з використанням компресії. У цьому разі сліди обробки можуть практично зникнути. Саме тому вони не будуть корисними для аналізу зображень із соцмереж, адже їх алгоритми сильно стискають знімки для розміщення на сайтах і видаляють EXIF дані. Хоча сильний шум на ELA (сині та червоні смужки) ознака того, що фото було кілька разів перезбережено.

Метод Hidden Pixels покаже приховані пікселі, тобто умовний прозорий шар, що міг використовуватися під час редагування знімка. Він допомагає побічно ідентифікувати програми, в яких оброблялося зображення. Так, Photoshop забарвлює такі пікселі в білий колір, Gimp і PicMonkey – в чорний.

Пам'ятайте, що тільки один інструмент не може остаточно довести або спростувати маніпуляції з фотографією. Рекомендується використовувати кілька методів та ресурсів для більш повного аналізу.

Зокрема, визначенню достовірності зображення допоможе: *його критичний огляд* (що виглядає дивним – рівномірність освітлення, неприродні тіні, дзеркальне відображення, спотворення по краях об'єктів, зміна кольору тощо); *дослідження сцени з різних ракурсів*; *визначення змін ландшафту* (будівництво, бойові дії, природні катаклізми), *контент-аналіз знімку* (за допомогою збільшення, інверсії кольорів для ідентифікації важкопомітних деталей) разом із

супроводжуючим текстом, іншими світлинами, зробленими раніше/пізніше; *додатковий зворотний пошук оригіналу зображення*; *перевірка використання генеративного ШІ* – AI image Detector, AI or Not (free – 10 запитів на місяць), AmIReal?, Content at Scale, Face Match, Fake Profile Detector (плагін для Chrome), Illuminarty (free – базовий функціонал), Maybe's AI Art Detector, Hive AI Detector (плагін для Chrome), а також Diffchecker (порівняння фотографій), PicTriev (показує стать та вік людини на фото), Stolencamerafinder (визначає камеру за серійним номером та шукає в Інтернеті, які ще фото були нею зроблені).



Щодня в глобальну мережу користувачі викладають величезну кількість відеоконтенту. Але його покадрова індексація пошуковими системами вимагала б значної кількості часу та ресурсів. Саме тому зворотний пошук відео, на відміну від зображень, на цей час не став базовим функціоналом вказаних систем. Bing, DuckDuckGo, Google Video, Yahoo Video Search, Яндекс видео обмежуються відшуканням відео за ключовими словами (назва, опис, імена учасників, місце, особливості тощо) з можливістю фільтрації результатів (за джерелом, датою, тривалістю, обсягом) або з використанням Dorks (наприклад, site:youtube.com українська формула миру). Аналогічна ситуація має місце і в соціальних мережах (Facebook, Instagram, TikTok, ВКонтакті та ін.) – достатньо задати пошуковий запит і перейти на потрібну вкладку.

За своїм змістом **пошук та верифікація відео** дуже схожі на роботу зі світлинами. Переглядаючи ролик, за допомогою скриншотів (для ОС Windows комбінація клавіш Win+Shift+S, для Mac OS – Shift+Cmd+3) виокремлюємо декілька унікальних фрагментів (початок, ключові сцени) та здійснюємо їх зворотний пошук для визначення першоджерела. Автоматизувати цей процес можна через InVID WeVerify (плагін для Chrome) та YouTubeDataViewer.

Безсумнівно, найвідомішим сервісом відеохостингу є YouTube, на якому зберігається найбільший обсяг таких матеріалів. Вбудована система пошуку на цій платформі за якістю своєї роботи не поступається Google (недарма YouTube належить йому). Дуже важливий розділ ресурсу – прямі трансляції (Streams, стріми). Інші популярні безкоштовні відеохостинги – Dailymotion, DTube, RuTube (RU), Дзен (RU), Видео@Mail.Ru (RU).

Корисні сервіси – Altoolskit (пошук серед трендів YouTube), Catchvideo.net (завантаження відео), Filmot (пошук в титрах/субтитрах), Hadzy (статистика коментарів ролику), inPhrase (пошук відео- та аудіофайлів за описом), MW Metadata (перегляд метаданих), Return YouTube Comment Username (плагін для Chrome, нікнейми коментаторів), Selectext (плагін для Chrome, копіювання тексту з відео у

браузері), SnapSave та SSyoutube (завантаження файлу), TurboScribe (формує субтитри/анотацію, free – 3 відео на день), YCF-Comment Finder (пошук коментарів до ролику), YouTube Channel Finder (free – 5 запитів на добу), YouTube location та Youtube-geofind (пошук відео з геотегами), YouTubeScreenshot (скриншоти з відео), YouTube search tool (конструктор пошукових запитів), YouTube Transcript (за наявності субтитрів створює їх анотацію), YT1s.com (завантаження).

Важливо: відмітка часу при додаванні файлу на сервіс YouTube йде за тихоокеанським часом (UTC-8, тобто -10 годин за київським).

Під час визначення достовірності відео необхідно звертати *увагу на деталі* (оскільки програмні алгоритми можна ввести в оману): невідповідність аудіодоріжки зображенню, сліди його монтування («склеювання»), віддзеркалення відео (дивні, «перевернуті» написи), штучне збільшення/зменшення, додавання нових елементів (часу та дати, яскравих логотипів), зміна кольорової схеми на чорно-білу та ін. Контрприйоми – перегляд EXIF, пошук іншого контенту, що фіксує ту саму подію або схожого, яке потенційно можна видати за досліджуване; порівняння орієнтирів у кадрі з супутниковими зображеннями та фото геолокації; аналіз звукового ряду (мова, сленг, імена, події); перевірка погодних умов, покадровий перегляд у відеоредакторі тощо.

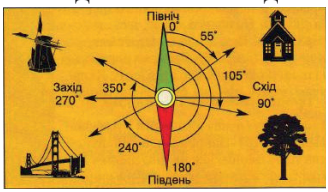
Інструменти для роботи з відео – Anilyzer (покадровий перегляд відео з YouTube), DFSpot-Deepfake-Recognition (GitHub, визначає наявність маніпуляцій з відео та його можливе створення ШІ), FlexClip (набір застосунків, free – роздільна здатність 720p, тривалість роліку 10 хв.), Kapwing (онлайн-відеоредактор, free – роздільна здатність 720p та водяні знаки), TinyWow.VideoTools (набір застосунків), Вільний відеоперекладач (bot, переклад відео з YouTube на українську, анотація).

Геолокаційний аналіз – це встановлення місцезнаходження об'єкта (стаціонарного чи рухомого) на карті, що подано у вигляді географічних координат, поштової адреси або маршруту переміщення. **Визначення локації**, де була зроблена світлина (чи знято відео), зазвичай, відбувається **шляхом**:

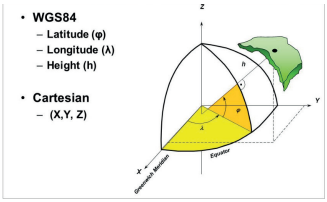
1) перегляду наявності геопросторових метаданих (зокрема, GPS-координат та ступіню їх точності, висоти над рівнем моря, часу, швидкості та азимуту руху GPS-приймача, азимуту захоплення зображення, виду геодезичної системи).

На картах Google, Bing та Яндекс у вікні пошуку в градусах (°) першою зазначається *широта* (від 0° до 90° на північ, від 0° до -90° на південь від екватора), потім *довгота* (від -180° до 0° на захід та від 0° до 180° на схід від Гринвіча) у вигляді десяткового дробу (наприклад, 10.35673009313803, -61.44516182050989). Тоді сервіс вкаже на відповідне місце на поверхні планети. Формати запису координат можна змінювати (приміром, у градуси/хвилини/секунди) – Converting coordinates, Geo Coordinates Parser and Converter, Transform coordinates.

Всесвітній скоординований час (Coordinated Universal Time, UTC) приблизно відповідає сонячному часу на Гринвіцькому меридіані. Запроваджений у 1961 р. Часові пояси навколо земної кулі описуються як додатне або від'ємне зміщення від UTC. Київський час більший від UTC на 2 години взимку (UTC+2) та на 3 – улітку (UTC+3).



Азимут – це кут між напрямом на північ і напрямом на предмет, зазвичай відраховується за годинниковою стрілкою від обраного початкового напрямку та може мати значення від 0 до 360°.



Геодезична система – це система координат, яка використовується для визначення точного місця розташування об'єкта на земній кулі. Стандартом для системи глобального позиціонування (GPS) на даний час є всесвітня система геодезичних параметрів Землі 1984 р. або WGS 84 (World Geodetic System 1984). Як і попередні, вона пов'язана із загальноземним еліпсоїдом, але він має уточнені розміри та орієнтований таким чином, щоб його поверхня найбільш повно співпадала з фізичною поверхнею планети в межах всієї земної кулі. Досі поширена в Україні система Пулково-1942 (СК-42) використовувала еліпсоїд Красовського, який найкращим чином співпадав з фізичною поверхнею Землі лише в межах території колишнього срср.

Ресурси для *геотегування фотографій* за метаданими – GeoImgr (free – 5 фото на день), geOSINT (GitHub), GpsPhoto (RU), Pic2Map, WhereIsThePicture. Якщо є кілька світлин з мітками GPS, то, розмістивши їх на мапі в хронологічному порядку, можна отримати маршрут переміщення об'єкта.

2) здійснення зворотного пошуку за фото (або за скриншотом з відео) для встановлення ймовірного збігу з вже відомими об'єктами чи місцинами, в тому числі за допомогою *спеціалізованих сервісів* – EarthKit (режими «Geoestimation», «Street View», «Satellite»), Geolocation Estimation (ШІ аналізує ландшафт для визначення ймовірної геолокації), GeoSpy, GVision (GitHub, free – 1000 запитів на місяць, потребує Google Cloud Vision API), Landmark Recognition (розпізнавання природних і архітектурних пам'яток), Picarta (ШІ-аналіз, free – 3 запити на день), Wikinearby (популярні місця поблизу вказаних координат).

Гарною практикою є видалення з кадру неважливих елементів, що можуть заважати релевантному пошуку (люди, тварини, транспортні засоби, меблі тощо), або їх пікселізацію або розмиття з метою зосередження роботи алгоритмів пошуковиків на фоні – місцевості чи інтер'єрі. Додатково проаналізуйте назву фото (відео), дописи до нього та іншу супутню інформацію. Якщо зображене на світлині можна описати словами (приміром, готель, гора, церква), спробуйте їх віднайти мовою країни потенційного знаходження;

3) детального вивчення знімку (головна увага до візуальних орієнтирів) – вид з вікна, особливості будинків навколо, їх адреси, помітні елементи, зовнішня реклама, вуличні вивіски та ліхтарі, дорожні знаки та розмітка, лінії

електропередач, конфігурація доріг, написи або малюнки, номерні знаки, маршрути транспорту, характерний рельєф, погодні умови, сонячні тіні, сузір'я, предмети інтер'єру, деталі одягу тощо – Animal.toolpie (ідентифікація тварин), Camopedia (військова уніформа), Geohints та GeoTips (архів геоб'єктів та їх особливостей для різних країн), Geonames (всесвітня географічна база даних), Logo.toolpie (ідентифікація логотипів), Plant.toolpie та Pl@ntNet (ідентифікція рослин), PlatesMania (RU, номерні знаки країн світу), Plate recognizer (розпізнавання номерних знаків, free – 2500 запитів на місяць), Vehicle AI (ідентифікація авто за фото), Worldlicenseplates (номерні знаки країн світу);

4) візуального підтвердження місця геолокації, що відбувається за принципом переходу від глобальних орієнтирів до місцевих (країна → регіон → населений пункт → вулиця → будинок або певна місцевість):

• *супутникові карти* (free – порівняно невисока роздільна здатність) ArcGIS, Bing Maps, CopernicusBrowser, EO Browser, ImageHunter (архів знімків обраної місцевості), Google Earth (у версії для PC Google Earth Pro має більш розширений функціонал та є архів зображень), EOS Land Viewer,

Google Maps, HereWeGo, OpenAerialMap (порівняно невелика кількість знімків), Satellites.pro (містить карти Google, Yandex, OpenStreet, ESRI та Apple), Soar, World Imagery, World Imagery Wayback (архів знімків з 2014 р.), Яндекс.Карти (RU); карти *пожеж* (місця влучань під час бойових дій) – Greenpeace, Firms.NASA, Pogodnik.com, SaveEcoBot, Worldview (архів з 2021 р.);

• *перегляд вулиць, вебкамери, фото з автореєстраторів* – Google Street View (перетягніть іконку у вигляді чоловічка на панелі праворуч унизу), Яндекс.Панорама (RU); Instant Street View та ShowMyStreet (перегляд вулиць в Google Street View); вебкамери – EarthCam, Insecam (RU), Opentopia, Pictimo, RailWebcams (вебкамери, пов'язані із залізницею), Shodan (пошук пристроїв, в т.ч. вебкамер, підключених до інтернету), Skyline, Surveillance under Surveillance, Windy Webcam, WorldCam, WorldCams, World-Cam (RU), YouWebCams (RU), Google Custom Search Engine (пошук за каталогом сервісів вебкамер); KartaView та Mapillary (знімки вулиць з автореєстраторів), WindowSwap (записи видів з усього світу, платний вибір локації), 360cities (панорами);

• *спеціалізовані карти* – Bellingcat OpenStreetMap search (пошук об'єктів за категоріями на заданій території), CellMapper (базові станції мобільних операторів), DualMap (одночасне відображення певного місця через перегляд вулиць, звичайну карту та 3D-проекцію), GpsJam (перешкоди GPS-сигналу на основі звітів навігаційної системи літаків), MapCompare (одночасна робота з декількома картами з понад 250 наявних), OpenCellid (базові станції стільникового зв'язку), OpenInfraMap (лінії електропередач, телекомунікація, сонячна, нафтова, газова та водна інфраструктура світу), OpenStreetMap (межі забудови різного цільового призначення, об'єкти транспорту); Peakery, PeakFinder, PeakVisor (ідентифікація гірського ландшафту), Wikimapia (RU, інтерактивна карта з описом об'єктів), 2ГИС (RU, потребує VPN, карти міст з довідковою інформацією), Візіком (карти міст України з додатковими даними);

• *військова агресія рф* – Bellingcat's map of Ukraine, DeepStateMap, Eyes on Russia Map, Geoconfirmed, LiveUAMap, [WarArchive] Карта війни, мапа російських військових об'єктів Криму;

• *допоміжні сервіси* – Earth Engine Data Catalog (завантаження каталогів Earth Engine), Geofabrik (безкоштовні картографічні дані для OpenStreetMap), GEOINTsearch (пошук посилань на координати Google Maps з X/Twitter, Reddit і 4Chan), MapSwitcher (плагін для Chrome, перемикає електронні карти, конвертує координати), Old maps online (архівні карти), Pastvu (RU, архівні фото населених пунктів), QGIS (ГІС з відкритим вихідним кодом), SearchOnMap (RU, bot, пошук об'єктів на карті – будинків, шляхів, водойм та ін. – за їх параметрами); *вимірювання* – CalcMaps (RU), Free Map Tools, Grid Reference Finder, MapChecking (визначає кількість людей, що може вміститися на певній ділянці), Maps.ie;

5) встановлення приблизної дати та часу (погодних умов) зйомки (хронолокація) через:

• *3D-карти* – F4map (free – споруди та їх тіні в реальному часі), OSM Buildings, Skydb (база хмарочосів та висотних будівель);

• *сонячні/місячні тіні* (відображення траєкторії руху Сонця/Місяця у певний день в будь-якій точці світу для подальшого співставлення тіней на фото/відео з даними сервісу для цього місця) – 3D Sun Path, Gaisma (час сходу і заходу Сонця по всьому світу), MoonCalc, Online Protractor (транспортир), Scale fixereng (вимірювання об'єктів на фото), ShadeMap, ShadowCalculator, Shadowmap (free – вибір місця, тільки для поточної доби), SunCalc;

• *архів погоди* (температури, хмарності, опадів, кута падіння сонячних променів тощо) – Wolfram Alpha (англомовний ресурс, приклад запиту – weather kharkiv 10 april 2024), Ventusky, Windy, Zoom.earth (інтерактивна карта).

6. Соціально-орієнтовані платформи

Соціальна мережа – це вебсайт або застосунок, де користувачі можуть створювати особисті профілі, підтримувати контакти з іншими учасниками спільноти та формувати нові знайомства, віртуально обмінюватися інформацією. Вони прагнуть ділитися досвідом, емоціями, поглядами та новинами, товарами або просто спілкуватися, оскільки залежать один від одного для схвалення, визнання та соціалізації, ведення бізнесу.

Враховуючи це, соціальні мережі зберігають великі масиви даних про своїх користувачів, включно з їхніми загальнодоступними постами, фотографіями, відео, колом спілкування, історією взаємодії, що перетворює подібні платформи на ідеальне поле для проведення OSINT-досліджень. Їх опрацювання вимагає використання віртуальних акаунтів. Але соцмережі постійно вдосконалюють власні протоколи безпеки задля захисту приватності авторизованих учасників, що подекуди ускладнює роботу осінтерів.

Наявність у особи профілю в соцмережах можна визначити через:

• ***пошукові системи та їх оператори*** – наприклад, site:linkedin.com/in «НЮУ» (виведе список акаунтів на LinkedIn, що пов'язані з Національним юридичним університетом імені Ярослава Мудрого), site:(https://www.facebook.com/ | https://vk.com/) «Новак Иван» (шукатиме користувача Новака Івана серед профілів Facebook та ВКонтакті) тощо. Водночас значна частина інформації на цих платформах розміщується в Deep Web, а тому недостатньо проіндексована, що робить пошуковики не завжди ефективним інструментом;

• ***спеціалізовані сервіси*** (базовий пошук йде за нікнеймом) – Alfred (GitHub), Blackbird, Check Usernames, DetectDee (GitHub, пошук за e-mail та телефоном), EagleEye (GitHub, пошук за фото), Google Social Search, Enola (GitHub), Holehe (GitHub, пошук за e-mail), Maigret (GitHub), Maryam (GitHub, модуль social_nets), Mr.Holmes (GitHub), NameCheckup та NaMint (використовується у зворотному порядку – платформи, де певний нікнейм недоступний, це показник того, що особа може мати там обліковий запис), OSINT Tools (пошук за e-mail або номером телефону), Predictasearch (пошук за e-mail або номером телефону, free – базовий функціонал), Seon (пошук за e-mail або номером телефону), Sherlock (GitHub), Sherlockeye, Snoop (GitHub), Social Analyzer (GitHub), Social Mapper (GitHub, пошук за ПІБ, e-mail, номером телефону, фото), SocialRecon (GitHub), Social Searcher (free – 100 запитів на день), Username Lookup, Usersearch.org (free – базовий функціонал), WhatsMyNameWeb;

• *зворотний пошук зображень*;

• ***Telegram-боти*** – як для універсального пошуку, так і вузькопрофільні – GetFB (RU, пошук за номером телефону), Maigret OSINT (RU, пошук за

нікнеймом);

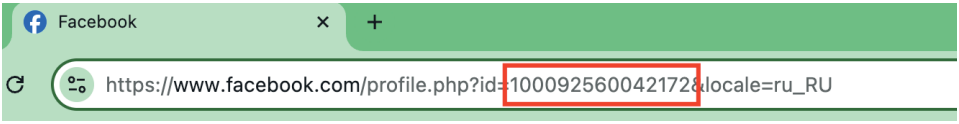
• ***пошукові можливості соцмереж*** – *за ніком чи ПІБ* (в т.ч. у різних варіантах їх написання), *за номером телефону* (через його додавання до списку контактів, а особи – до друзів), *за відомим профілем в іншій соцмережі* (через список друзів, резюме), *через підписки* (спільні знайомі), *за відмітками на фото* (участь у спільних заходах); *за хештегами* (професія, характер занять або інтересів, місця народження, проживання, навчання, роботи, відпочинку тощо; сторонні ресурси – Kribrum.io (RU, потребує реєстрації та VPN), Quick hashtags and keywords search, Storyful Multisearch (плагін для Chrome)) та *геотегами* (додатково – geOSINT (GitHub, шукає в соцмережах фотографії з геотегами та наносить їх на карту), OSINT Geolocation Databases Search (пошук за базами Bellingcat, Cen4InfoRes та ін.), Social Geo Lens, xHunt (free – 7 днів, потребує реєстрації)).

Досить часто в якості нікнейму особа може використовувати варіації з ПІБ чи ініціалів з додаванням дати (року) народження, культурного, політичного чи історичного персонажу, інформації про неї (місце роботи чи професія, світогляд/психологія, вподобання) або «щоб ніхто не здогадався» – слово навпаки, кирилицею в англійській розкладці, латинською тощо;

• ***комерційні рішення*** – Artellence, Tangles тощо.

За результатами пошуку важливо переконатися, що знайдена сторінка дійсно належить саме об'єкту зацікавленості. Профіль користувача – візуальне відображення персональних даних, пов'язаних з конкретною особою та характеристикою його унікального середовища в соціальній мережі. Він належить до цифрового представлення особистості людини. Але існує ризик того, що під час авторизації вводилися завідомо неправдиві або неповні дані.

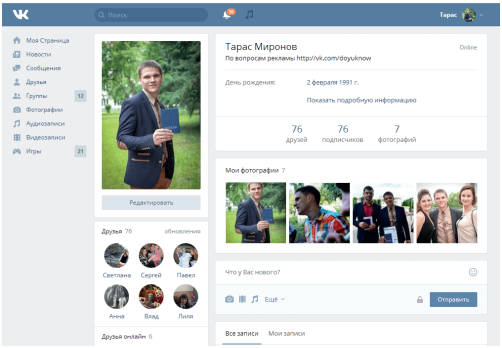
ID користувача – унікальний незмінний номер, що присвоюється акаунту, спільноті, каналу чи групі під час реєстрації у певній соціальній мережі (кожна з них має свої правила побудови ID). Цей ідентифікатор допомагає однозначно авторизувати власника облікового запису незалежно від його прізвища та імені або нікнейму. Наприклад, для Facebook – це п'ятнадцять цифр, що йдуть після символів «id=» в позначенні URL-адреси (Uniform Resource Locator, уніфікований локатор ресурсу) сторінки користувача.



Також існує можливість змінювати цей ідентифікатор на ім'я латинськими літерами, воно знаходиться після назви домену в адресному рядку браузера (https://facebook.com/yourname). У будь-якому разі для визначення ID можна скористатися пошуком серед HTML-коду сторінки (через виклик контекстного меню правою клавішею миші чи комбінацією клавіш) або функціоналом нижченаведених спеціалізованих ресурсів.

За встановленим ID можна знайти відповідний профіль об'єкта зацікавленості та переглянути всі загальнодоступні відомості (хоча користувач у налаштуваннях безпеки може обирати, яку інформацію зробити загальнодоступною).

Дізнатися більше про особу допомагають **індикатори** – профіль (аватарка, статус, персональні дані); список друзів; стрічка новин, пости/репости, публікації; частота розміщення матеріалів; фотографії, музика, відео, локації; участь в групах, спільнотах, підписки; ведення власних блогів, зокрема професійних, суспільно-політичних тощо.



З цією метою варто використовувати *як універсальні* для більшості соцмереж *колекції інструментів* – Comment Picker, OnePlus OSINT Toolkit, Shreateh Social Media Tools чи *окремі ресурси* – 4K Video Downloader (завантаження відео), CrowdTangle (плагін для Chrome, показує, хто ділився посиланням та як часто), ExportComments (експорт коментарів до постів, free – 100 коментарів на день), NetSocOSINT (GitHub, збір інформації з акаунту в Instagram, TikTok, X/Twitter, Twitch, Telegram, GitHub), Phantom Buster (збір даних з акаунтів, free – 14 днів, обмежений функціонал), Popsters (RU, аналітика акаунтів, потребує VPN, free – 7 днів, 10 завантажень), SaveFrom.net (завантаження відео), Social Blade (статистика акаунтів), Social Searcher (моніторинг згадувань у соцмережах), Tagdef (вказує на значення хештегів), Tonetizer (аналізатор тону постів, українська відсутня), VideoDownloader (завантаження відео), Video DownloadHelper (плагін для Chrome, завантаження відео), VideoGrabber, *так і вузькопрофільні:*

Facebook:

- *ID* – Codeofaninja, Find Facebook ID, Lookup-id.com, Randomtools.io;
- *альтернатива внутрішньому пошуку* – Facebook Hashtag Search, FacebookMatrix, Facebook Search, Facebook Search CSE, Graph.tips, IntelligenceX, IntelTechniques, Search is Back, Socmint Tool, SowSearch, WhoPostedWhat;
- *аналіз профілю* – StalkFace;
- *завантаження контенту* – DumpItBlue+ (плагін для Chrome), Fdown.net;
- *інше* – Facebook Data Breach Checker (перевірка використання номеру телефону для реєстрації), Facebook Live Map (пошук прямих трансляцій), Facebook Recover Lookup (відновлення акаунту).

Instagram:

- *ID* – Codeofaninja, Find Instagram User ID;
- *альтернатива внутрішньому пошуку* – Aware Online, Instagram Explorer (пошук фото), IntelTechniques;

- *аналіз профілю* – Instagram-scraper (GitHub), Modash, Not Just Analytics, Osintgram (GitHub), SolG (GitHub), Toutatis (GitHub, через API отримує дані з акаунту – e-mail, телефон тощо), Unseen (GitHub), Webstagram;
- *перегляд профілю та завантаження контенту* – DownloadGram, Dumpoir, ExportGram, GreatFon, iGram, Imginn, IMGinn.io, Inflact, Instafollowers, INDownloader, InstaFreeView, Instaloader (GitHub), InstaNavigation, InstaDP, Pixwox, Picuki, PokoInsta, SaveInsta, Snapinsta.app, StoriesIG, StorySaver.net.

LinkedIn:

- *альтернатива внутрішньому пошуку* – CrossLinked (GitHub, дані про співробітників), CSE, Free people search, IntelligenceX, IntelTechniques, LinkedIn Boolean Search Tool (free – 7 днів), LinkedIn Guest Browser (плагін для Firefox, перегляд акаунтів без реєстрації), LinkedInt (GitHub), Programmable Search Engine, Recruit'em, Recruitment Geek, RocketReach (потребує реєстрації);
- *аналіз профілю* – InSpy (GitHub);
- *завантаження контенту* – Linkedin Video Downloader;
- *інше* – LinkedIn Overlay Remover (плагін для Firefox, видаляє накладку, що відображається поверх профілю LinkedIn).

X (Twitter):

- *ID* – Codeofaninja, Find Twitter ID, TweeterID;
- *альтернатива внутрішньому пошуку* – Aware Online, FollowerWonk, Free people search, IntelligenceX, IntelTechniques, Network Tool (шляхи поширення твітів), One Million Tweet Map (твіти з геотегами), Socialbearing (є аналітика), Synapsint, Tweet Archiver (плагін для Chrome), Twint (GitHub, скрейпер), Twitter Advanced Search, Twitter List search, Twitter search tool, twXplorer;
- *аналіз профілю* – Foller, Lolarchiver (історія профілю), memory.lol (історичні дані), Tinfoleak, Twitonomy, TwitterAudit (автентичність підписників);
- *завантаження контенту* – Download Twitter Data, TwitterVideoDownloader;
- *інше* – Botometre (визначення бот-акаунту), Deleted Tweet Finder (пошук видалених твітів), SimpleScraper OSINT (моніторинг твітів з координатами), Wayback Tweets (GitHub, архівні твіти), Wayback Tweets (архівні твіти).

TikTok:

- *ID* – Find Tiktok ID;
- *альтернатива внутрішньому пошуку* – Aware Online, TikTok Quick Search, UrleBird, Vidnice;
- *аналіз профілю* – Exolyt (free – базовий функціонал), MaveKite (free – базовий функціонал), TikTok hashtag analysis (GitHub, аналіз хештегів);
- *завантаження контенту* – Ssstik, SnapTik, Tiker, TikTok Scraper (GitHub), TikTok Downloader, Tiktok Video Downloader, Ttdown, TTSave;
- *інше* – TikTok-Timestamp (дата та час завантаження відео).

ВКонтакті (RU):

- *ID* – ForVk (RU), Prozavr (RU);
- *альтернатива внутрішньому пошуку* – BigBookName (RU), Custom search engine Google, Photo-Map (RU, пошук постів з геотегами), Vk.barkov.net (RU), VK.watch (RU, додатково – пошук за фото);
- *аналіз профілю та його зв'язків* – 220vk (RU), FindNameVk (RU, bot), InfoApp (RU, потребує профіль у соцмережі), Social Graph Bot (RU, bot, графовий аналіз сторінок), UseVk (RU), VKCity4Me (RU), VKUserInfo (RU, bot);
- *інше* – ForVk, Nebaz та Vkdia (RU, відстеження користувачів), Regvk (RU, дата реєстрації акаунту), VKHistoryRobot (RU, bot, архів профілю).

Одноклассники (RU):

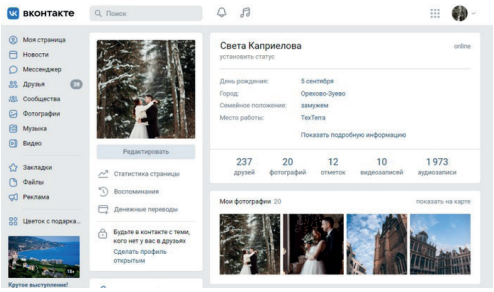
- *альтернатива внутрішньому пошуку* – poisk-cheloveka (RU), Vk.barkov.net (RU, додатково – аналіз профілю).

Discord:

- *ID* – Discord.name, Disserv (GitHub), Lookupguru, Unofficial Discord Lookup;
- *альтернатива внутрішньому пошуку (сервери та боти)* – Disboard, Discordbots.gg, Discordbotlist, Discord center, Discord discadia, Discord.me, Discord official server search, Top.gg;
- *інше* – Discord Client Encyclopedia (GitHub, набір сторонніх клієнтів та модів).

У разі своєї достовірності отримані за допомогою вказаних інструментів відомості можуть *вказувати на:* психологічний портрет, психотип, характер, відкритість особи; її цінності, моральні установки, рівень культури та виховання, сприйняття світу, мотивацію, пріоритети; хобі, захоплення та інтереси, дозвілля, ритм і спосіб життя, коло спілкування; емоційний стан, настрій; рівень агресії, конфліктності; публічну активність, громадянську позицію, політичні погляди, відношення до певних подій чи людей; професійні навички, досягнення, репутацію; симпатії/антипатії тощо.

Шукаючи людину в соціальній мережі, **необхідно враховувати всю її вхідну та вихідну взаємодію** – згадування про неї в постах близьких або знайомих, колег, роботодавців; наявність спільних фотографій, постів чи коментарів; участь у заходах; події, подорожі, місця перебування тощо. Якщо



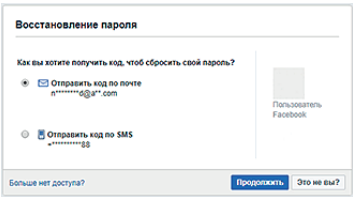
профіль особи «мовчить» або він закритий чи навіть відсутній у соцмережі, акаунти його рідних чи друзів можуть бути більш інформативними. Наприклад, в LinkedIn/Facebook шукаємо колег об'єкта з унікальними іменами (бажано жінок – вони часто не закривають акаунт і не

приховують справжніх імен), а потім його самого – у підписках, постах, коментарях, на фото корпоративів, у відеороліках чи інших документах тощо.

Фото в соціальних мережах та дописи під ними здатні розповісти про місця, що відвідувала особа (робота/відпочинок, відеоекскурсії офісом, квартирою, маєтком, подорожі, вид з вікна, групові знімки, фото в ліфті, позначки про геолокацію та ін.) та окреслити коло її близьких контактів. Тому одним з варіантів пошуку *фото людини або її потенційних знайомих* є формування переліку локацій, де вони можуть часто/періодично знаходитися (навчання, робота, салони краси, спортзали, автосервіси, розважальні заклади, публічні/урочисті заходи тощо) та аналіз опублікованих звідти світлин і акаунтів їх авторів.

У якості *аватарки профілю* для різних соцмереж особа доволі часто може задіювати одне й те ж саме фото або малюнок. З метою знаходження таких облікових записів використовуйте зворотний пошук зображень чи Dorks (наприклад, ivan novak imagesize:170x170 site:http://facebook.com, в залежності від мережі розміри зображень диференціюються). У разі потреби варто покращити світлину чи визначити її достовірність.

Певні дані можна отримати через *функцію «Відновлення облікових записів»* соцмережі. Якщо в такий спосіб, наприклад у ВКонтакті, ввести відомий номер телефону або e-mail, а у відповідь отримати відсутність результату, це означатиме, що на них акаунт не реєструвався. В позитивному випадку вас запитають щодо зміни пароля і висвітяться частина адреси поштової скриньки або номеру, що можуть допомогти в подальшому пошуку (наприклад, для валідації інших акаунтів користувача). На даний час працює в X/Twitter, Facebook, Instagram, ВКонтакті, Однокласники.



Враховуючи мету створення віртуального акаунту, в деяких випадках актуальноє стає потреба його *подальшого наповнення та просування* хоча б на рівні активності середньостатистичного користувача (раз на кілька днів опублікувати щось у себе на сторінці, додати нейтральний коментар під постом у групі або поставити вподобайку певній публікації; час від часу додаватись до тематичних груп залежно від задекларованих інтересів чи місцезнаходження, підписуватися на відповідні пабліки тощо). Не зайвою буде й наявність оптимальної кількості друзів та/або підписників (необхідно періодично розсилати запити на додавання до друзів учасникам груп, до яких приєдналися), а також поширення цільового, послідовного, пов'язаного між собою та позбавленого унікальності контенту (повідомлення, тематична картинка, мем або репост якогось допису). Тут можуть допомогти сервіси для генерації фейкового листування – FakeChatMaker, FakeDetails, Pranx, Simitator, Zeoob або задіяння можливостей ШІ.

Кращою практикою є створення віртуального акаунту мовою, якою ко-

ристувач вільно володіє, оскільки перекладені тексти можуть одразу кинутися в око та викликати непотрібні сумніви (як варіант – максимально обмежити текстову інформацію або задіювати допомогу фахівців). Чим більше даних додано до профілю, тим легше перевірити його справжність – він має спиратись на реально існуючі прототипи. У якості аватарки можна використовувати знеособлене зображення (предмет, абстракцію, персонаж чи малюнок), хоча ми підсвідомо більше довіряємо співрозмовнику з фото реальної людини.

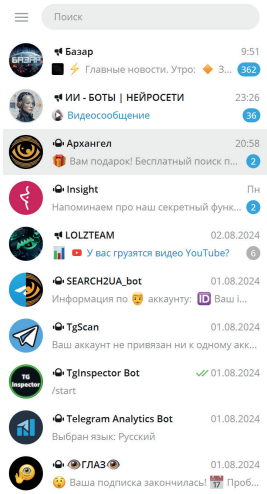
Соцмережі часто об'єднують в одну групу з месенджерами: і ті, й інші створюють умови для спілкування великому колу людей. Основна відмінність у тому, що соціальні мережі дають доступ до масової комунікації. Наприклад, ваш пост у Facebook побачать одразу всі друзі, а може й інші учасники. Тоді як месенджери дозволяють людям спілкуватися один на один або створювати невеликі ком'юніті, наприклад сімейний чат або чат для колег. Межа між цими поняттями доволі розмита: у багатьох соцмережах є вбудовані месенджери, а в деяких месенджерах є можливість публікувати пости на широкий загал. Зазвичай месенджери підтримують наскрізні зашифровані чати, відеодзвінки, VoIP, обмін файлами та деякі інші функції.

Telegram (RU) давно став більшим, ніж просто месенджером – для багатьох людей це основне джерело новин, корисного чи розважального контенту. Він дає змогу спілкуватися з іншими користувачами, створювати групи, канали, боти та чимало іншого. Найпоширеніший спосіб дізнатись, чи представлена певна особа в Telegram (за наявності встановленого застосунку й її номеру телефону): в адресному рядку браузера ввести https://t.me/+XXXXXXXXXXX та в разі підтвердження перейти у відповідний чат й переглянути його. Альтернативні варіанти – додати цей номер до телефонної книги та проаналізувати результат або задіяти telegram-phone-number-checker (GitHub).

Telegram ID – це набір цифр, який ідентифікує профіль (username) у месенджері. Він не залежить від імені користувача, номера телефону, фотографії або інших даних, його не можна змінити або видалити. У стандартному функціоналі Telegram не передбачена функція, за допомогою якої можна дізнатися свій/чужий ID. Для цього, переважно, використовуються можливості ботів – GetMyID та UserInfoBot (RU, ID користувача, поточний ID чату, ID відправника повідомлення в публічній групі або ID чату пересланого повідомлення з такої групи), usinfobot, Userbox , Telerecon (комплексне OSINT-рішення), а також боти для універсального пошуку.

Слід пам'ятати, що при зміні телефонного номера не обов'язково створювати новий акаунт у Telegram, оскільки цей месенджер має функцію перенесення облікового запису на інший номер. При цьому зберігається історія

повідомлень, контакти, медіа та інші дані, пов'язані з обліковим записом.



Канали та групи самої різної спрямованості збирають величезні аудиторії. *Канал* схожий на тематичний блог або сторінку в соціальній мережі, на яку можна підписатися та слідкувати за її життям, оновленням інформації, переглядати публікації й реагувати на них, але жодним чином не впливати на функціонування. У той же час як *група* в Telegram – це спільнота, де ви можете самостійно оприлюднювати контент, брати участь в обговоренні, відповідати учасникам тощо. Іноді в таких спільнотах є адміністратори, які стежать за порушеннями правил тієї чи іншої групи.

Канали та групи мають схожу рису – різновиди відкритості (публічні та приватні). Приміром, *публічні* канали доступні всім користувачам месенджера через його загальний пошук. *Приватні* канали не можна знайти в такий спосіб. Посилання для них створюються адміністратором – і тільки за таким запрошенням користувачі отримують можливість перейти на канал та підписатися нього. Але ці типи групового спілкування також відрізняються за особливостями адмініструванням, функціоналом й іншими параметрами.

Telegram-канал не обмежений кількістю підписників. У ньому тільки адміністратор може надсилати повідомлення. Для того, щоб учасники мали змогу спілкуватися між собою, він має дозволити коментувати ці публікації. Обмін думками в коментарях відбувається як окрема гілка обговорення, що відноситься до конкретного повідомлення. На публікації підписники каналу також можуть реагувати (як ставити вподобайки в соціальних мережах, тільки тут дещо ширший список емодзі для реакцій). Функції модератора полягають у видаленні учасників, які порушили правила, накладенні постійних або тимчасових обмежень. Учасники каналу можуть переглядати історію повідомлень від самого початку – нові підписники мають змогу дізнатися про попередні публікації та навіть завантажити їх собі. Важливим елементом підписки на канал є конфіденційність учасників – ви можете бачити тільки їх загальну кількість і не матимете доступу до відповідних профілів (особистих даних та номерів телефону, лише аватар та нікнейм). Ця опція доступна лише в коментарях (адже тут ідеться про окрему спеціально створену для комунікації групу).

Під час вступу до групи інколи неможливо переглянути історію повідомлень через обмеження, що накладені адміністратором. Але в більшості випадків нові користувачі можуть ознайомитися з архівними публікаціями та постами. На початку становлення месенджера до групи могли приєднатися не більше 200 осіб, зараз чисельність супергрупи обмежена 200 000

учасниками. Групову активність можна вивчати тільки за кількістю користувачів, які перебувають у групі або залишають коментарі. А в каналах адміністратор може дізнатися про кількість переглядів кожної публікації.

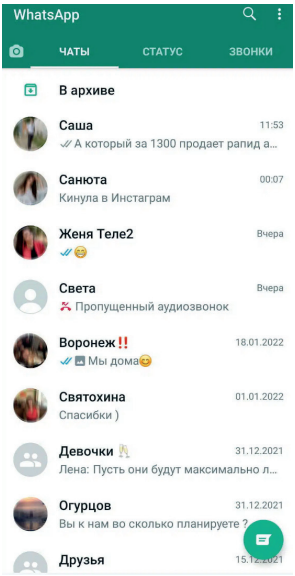
Таким чином, групи в Telegram є способом комунікації, вони дають змогу об'єднувати велику кількість людей в одному діалозі. У той час як канали призначені для отримання інформації з певного джерела без можливості безпосередньо впливати на нього. Отже, виокремимо *інструменти для*:

• ***пошуку каналів, груп і ботів*** – DirectoryTG, Lyzem, Telegogo Google CSE (публічні повідомлення), Telegram Channels, Telegram Channels Search, TelegramDB, TelegramGroup, Telemetr.io (free – базовий функціонал, потребує реєстрації, відображає видалені пости у вкладці «Дописи»), Telemetr.me (RU), TeleScan (RU, bot, шукає групи, вивантажує повідомлення), Telemetry (шукає повідомлення, free – 5 запитів на день по 25 результатів у видачі), TeleSINT (RU, bot, шукає групи, в яких перебуває користувач), TGInspector (RU, bot, шукає групи, вивантажує повідомлення), TGScan, TGStat (RU), xTea;

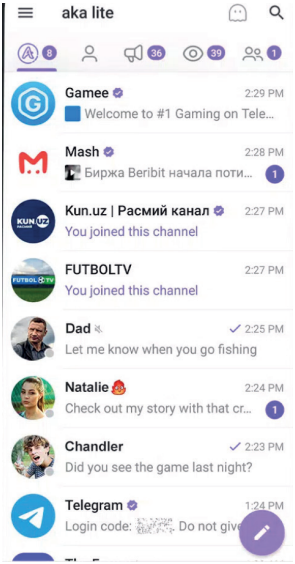
• ***дослідження профілю користувача/групи/каналу*** – CCTV (GitHub, відстеження місцезнаходження, потребує API), CommentGram (пошук коментарів), FunStat (RU, bot, різноманітна статистика), Geogramint (GitHub, пошук через API користувачів та груп, які активували функцію «Поруч»; за стандартними налаштуваннями вона відключена), informer (GitHub, інформація про канали, групи та користувачів), IntelligenceX (пошук та аналіз даних Telegram), Insight (RU, bot, інтереси користувача на основі його активності в групах), LinkGrabber (збирає розміщені на вебсторінці посилання – друзів, авторів коментарів чи вподобайок), Save Telegram Chat History (GitHub, плагін для Chrome, збереження переписки чату), Telegra.ph (RU, пошуковик Telegram), Telegram Message Analyzer (GitHub, аналітика збереженої в html-файлі історії чату), Telegram Nearby Map (GitHub, визначення місцезнаходження користувачів поруч), Telegram Scraper (GitHub, інформація про членів групи), Telegram Sender (плагін для Chrome, збір нікнеймів користувачів групи), Telegram Tracker (GitHub, генерує json-файли з інформацією про Telegram-канали та пости, потребує API), Telepathy-Community (GitHub, дозволяє архівувати чати Telegram, включаючи відповіді, медіа-контент, коментарі та реакції, збирати списки учасників, шукати користувачів за заданим місцем розташування, аналізувати найпопулярніші повідомлення в чаті, складати карту переадресованих повідомлень тощо), TgDev (RU, пошук постів Telegram-каналів), TeleTracker (дослідження каналів), TlgGeoEarthBot (bot, відображає активні Telegram-акаунти з увімкненою геолокацією навколо заданої точки; free – 3 запити на день), Tosint (дослідження ботів, пов'язаних з Telegram-каналом).

У Telegram функція наскрізного шифрування не працює, поки не створено секретний чат з іншими учасниками групи. На відміну від нього WhatsApp за замовчанням забезпечують наскрізне шифрування чатів та дзвінків, що накладає певні обмеження на функціонал *пошукових ресурсів*:

• ***перевірка статусу реєстрації/підключення*** – WATools.IO (free – 8 годин для трекінгу статусів особи, повідомлень про використання ним WhatsApp, моніторингу його активності, а також дослідження вірогідності чату між двома номерами), подібний функціонал у Chatwatch (потребує реєстрації, free – 3 дні), Whapi (додатково – Automatic warm-up of WhatsApp accounts, Chat Link Generator, Products, Profile picture, QR Code Generator, Text Formatter; free – 5 розмов на місяць, 150 повідомлень та 30 запитів на день, 1000 викликів API на місяць), Whatsapp Mobile Tools, WhatsappMonitor (GitHub, моніторинг активності), WhatsApp-Monitor (GitHub, трекер, сповіщення), WhatsApp OSINT (додатково – дані про користувача, часовий пояс), WhatsApp OSINT Tool (GitHub, тривалість сесії);



• ***інше*** – Email2WhatsApp (GitHub, за електронною поштою шукає номери, що зареєстровані в WhatsApp), Fake WhatsApp Chat Generator (фейковий чат), Whatsapp-GroupContacts-Scraper (GitHub, вивантаження контактів з групових чатів WhatsApp), WhatsFoto (GitHub, плагін для Chrome, завантаження фото профілю користувача), WhatScraper (GitHub, вивантаження інформації про учасників групи).



Viber, як і будь-який інший популярний месенджер, має багато переваг, однією з яких є зручність для ведення бізнесу. Однак він майже не захищений від здійснення небажаних інформаційних розсилок. Завдячуючи поширеності месенджера, таке поєднання привертає велику увагу спамерів і створює певні проблеми для користування ним. Для того, щоб додати людину до спам-розсилки, достатньо знати номер її телефону, тому в його мережі щодня поширюються мільйони нав'язливих рекламних повідомлень. Крім цього, користувачі, які не входять до списку контактів, можут переглядати фото вашого профілю, IP-адресу та інші особисті дані.

Не варто забувати, що окремі дата-центри компанії зберігаються в росії. І хоча там стверджують, що на них знаходяться тільки відомості щодо російських користувачів, цю інформацію не можна жодним чином перевірити.

Корисний інструмент – Viber Osint (GitHub, перевірка реєстрації номера телефону в Viber).

7. Формування профілю фізичної особи

Відправною точкою для пошуку може стати будь-яка наявна інформація – прізвище та ім'я особи, номер її мобільного телефону чи адреса електронної пошти, профіль в соціальній мережі, місце роботи/характер занять, сфера громадської активності, фотографія або відеофрагмент тощо.

Іншими словами, формування **профілю (досьє) особи** починається з певних вихідних відомостей, що за допомогою пошукових інструментів потрібно пов'язати з іншими відкритими даними (за наявності), розподіливши в звітньому документі отриману інформацію за функціональними блоками:

Прізвище, ім'я та по батькові
(можливі зміни ПІБ, псевдонім/нік, позивний)

Фото

Установчі дані (дата та місце народження, місце реєстрації (проживання), паспорт громадянина України (закордонний паспорт, громадянство інших країн), реєстраційний номер облікової картки платника податків, водійське посвідчення), **контактна інформація** (мобільний телефон, електронна пошта, Skype, месенджери), **акаунти в соцмережах** тощо:

- ***пошукові та метапошукові системи***;
- ***Telegram-боти*** для універсального пошуку;
- ***соціально-орієнтовані платформи***;
- ***спеціалізовані сервіси*** – Castrick (free – базовий функціонал), DarkGPT (GitHub, інструмент на базі ChatGPT-4 для пошуку у витоках даних), Epieos (пошук за e-mail або номером телефону, потребує реєстрації, free – Google, Email Checker & Skype, Clickable links, водяний знак), Hive (GitHub, автоматизує збір даних через Truecaller, Shodan, IntelX, Email Verifier, Sherlock та ін.), Phunter (GitHub, пошук за номером телефону), PrivacyWatch (free – базовий функціонал), Pipl (free – 5-тиденний доступ, потрібна реєстрація), SpiderFoot (GitHub, пошук за IP-адресою, доменем, e-mail або номером телефону), Spokeo (оплатна видача результатів), Uscrapper Vanta (GitHub, збирає та вивантажує з цільового сайту адреси електронних пошт, посилання на соцмережі, геолокацію, номери телефонів, нікнейми користувачів; може фільтрувати видачу за ключовими словами), Webmii (інформація з соцмереж, вебсайтів та онлайн-документів), X-Ray (free – 2 кредити, потребує реєстрації, пошук росіян на час збройної агресії безкоштовний);
- ***телефонні номери*** – Moriarty Project (GitHub); мобільні *застосунки для ідентифікації номерів абонентів* CallApp, CheckerUA, Eyecon, Getcontact, NumBuster, TrueCaller, WhoCalls (за замовчанням вивантажують записи телефонної книги користувача; для безпечної роботи необхідний окремий телефон з імітаційними контактами); *бази телефонних*

номерів – Spravkaru.net (RU), spravochnik109 (RU), Довідник міських телефонних номерів (RU, росія, Україна, білорусь, Молдова, Латвія, Казахстан), Хто Дзвонив?; *інше* – IMEI.info (пошук за IMEI, International Mobile Equipment Identity, міжнародний ідентифікатор мобільного обладнання), email2phonenumber (пошук за e-mail), PhoneInfoga (GitHub, інформація про номер телефону);

- ***електронна пошта*** – GHunt (GitHub, збір різнопланової інформації про користувачів Google; є онлайн версія, що потребує реєстрації), H8Mail (GitHub, сканує вказану поштову скриньку та видає перелік можливих паролів від неї), PasswordSearchBot (bot, шукає електронну пошту та видає «злиті» паролі, free – 10 запитів на день), YaSeeker (GitHub, інформація про Яндекс-акаунт за електронною поштою або логіном), Zehef (GitHub, дослідження електронних листів); *валідатори пошти* – Email Hippo, Verifalia (free – 25 перевірок на день), VerifyEmailAddress; аналіз заголовку листа (IP-адреса відправника, поштові сервери, шлях проходження) – Email Header Analysis, Messageheader,
- ***сервіси ДМС*** – Перевірка за базою недійсних документів, Перевірка продовження строку перебування/тимчасового проживання;
- ***сервіси МВС*** – пошук паспорта громадянина України серед викрадених та втрачених, перевірка витягу з Єдиного реєстру осіб, зниклих безвісти за особливих обставин, Зниклі громадяни.

Сімейний стан, родинні зв'язки:

- ***державні реєстри*** – Відкритий реєстр національних публічних діячів України, Єдиний державний реєстр декларацій;
- ***соціально-орієнтовані платформи***;
- ***сайти знайомств*** (потребують реєстрації) – Badoo, Jolly, Tinder, UkrDate;
- ***генеалогічне дерево*** – FamilySearch (потребує реєстрації);
- ***некрологи*** – Legacy.

Освіта, науковий ступінь, вчене звання, наукові публікації:

- ***пошукові та метапошукові системи***;
- ***спеціалізовані сервіси*** – Google Академія, Наука України, Реєстр документів про вищу освіту, Український індекс наукового цитування.

Військові, спеціальні, почесні звання, державні нагороди:

- ***пошукові та метапошукові системи***;
- ***спеціалізовані сервіси*** – сайт Президента України (пошук за документами).

Професійна діяльність, біографічні дані:

- ***державні реєстри*** – Державний реєстр атестованих судових експертів, Єдиний державний реєстр декларацій, Єдиний реєстр адвокатів України, Єдиний реєстр арбітражних керуючих України, Єдиний реєстр нотаріусів України, Єдиний реєстр приватних виконавців України, Реєстр атестованих осіб архітектори, проектувальники, експерти, інженери технічного нагляду), Реєстр ауди-

торів та суб'єктів аудиторської діяльності, Реєстр перекладачів;
- ***участь в юридичних особах, відкриття ФОП***;
- ***сайти з пошуку роботи*** – JOBS.ua, RABOTA.ua, WORK.ua тощо;
- ***політична та/або громадська діяльність*** – База даних політиків та партій, Фінансова звітність партій.

Майновий та фінансовий стан, доходи, транспорт:

- ***державні реєстри*** – Державний реєстр речових прав на нерухоме майно, Єдиний державний реєстр декларацій;
- ***земельні ділянки*** – Кадастрова карта України, КадастрСервіс;
- ***транспортні засоби*** – Autodetective, Baza-gai, Carma, Checkcar, Unda, АвтоНомера (пошук за державним номером та VIN-кодом); Plate Recognizer (розпізнавання марки, кольору, типу авто та країни реєстрації номерного знаку; free – 2500 переглядів на місяць, потребує реєстрації); МТСБУ (перевірка чинності полісу страхування); Транспортні засоби у розшуку; Відомості про транспортні засоби та їх власників;
- ***рекламні оголошення*** (в т.ч. на місцевих ресурсах) – Domik (фото/відео приміщень/будинків), M2bomber (додатково – пошук за телефоном), OLX.ua, Prom.ua, RIA.com тощо:
- ***інтелектуальна власність***;
- ***інше*** – Binlist.net (ідентифікація банку за номером картки).

Судові справи, компромат, виконавчі провадження, конфлікти:

- ***виконавчі провадження*** – Автоматизована система виконавчого провадження, Єдиний реєстр боржників;
- ***державні реєстри*** – Єдиний державний реєстр осіб, щодо яких застосовано положення Закону України «Про очищення влади», Єдиний державний реєстр осіб, які вчинили корупційні правопорушення, Каталог корупційних ризиків, Система пошуку прихованих інтересів (НАЗК, потребує реєстрації);
- ***діяльність на шкоду національній безпеці України*** (за даними НУО) – Evocation.info (колаборанти), Миротворець та IDentigraF (пошук за фото у БД «Миротворець», потребує реєстрації, 5 запитів на день), Реєстр зрадників, ORDILO;
- ***досудове розслідування*** – повістки про виклик, повідомлення про підозру та відомості щодо підозрюваних, стосовно яких надано дозвіл на здійснення спеціального досудового розслідування на сайтах Офісу Генерального прокурора та газети «Урядовий кур'єр»;
- ***матеріали журналістських розслідувань*** – Антикор, Генштаб, громадський рух «Чесно», Гроші, Досьє, Наші гроші, ОРД, Політрада, Слідство.Інфо, Слово і Діло, Схеми, Трансперенсі Інтернешнл Україна (протидія корупції), Укр.Ав, Цензор.Нет, Центр протидії корупції, Bihus.info, DocumentCloud (відкрита база політичних, юридичних документів, які використовують журналісти у своїх розслідуваннях), LittleSis (інформація про публічних осіб);

- ***особи, які переховуються від органів влади*** – Інформація про осіб, які переховуються від органів влади, розшук СБУ та МВС;
- ***санкції*** – Державний реєстр санкцій, Зведений санкційний перелік Ради Безпеки ООН, Перелік осіб, пов'язаних із здійсненням терористичної діяльності або стосовно яких застосовано міжнародні санкції, Реєстр фізичних осіб під санкціями РНБО, Consolidated Canadian Autonomous Sanctions List (Канада), EU Sanctions Map (Євросоюз), Office of Foreign Assets Control (OFAC, США), OpenSanctions, SanctionsExplorer;
- ***судові рішення*** – Єдиний державний реєстр судових рішень, Реєстр судових рішень (потребує реєстрації), Стан розгляду судових справ (пошук сторони по справі за ПІБ на порталі «Судова влада України»).

Найближче оточення, дружні зв'язки, захоплення, інтереси, звички, нахили, регулярні та нерегулярні місця відвідування, перебування за кордоном, спосіб життя, домінуючі потреби, а також інша інформація, яку необхідно мати на увазі:

- ***пошукові та метапошукові системи***;
- ***соціально-орієнтовані платформи***;
- ***судові справи, компромат, виконавчі провадження, конфлікти***.

8. Формування профілю юридичної особи

Юридична особа (далі – ЮО) – це організація, що *пройшла законодавчо затверджену процедуру реєстрації*, є суб'єктом права, має майнові права й можливість виступати в якості позивача та відповідача в суді. *Обов'язковими атрибутами* ЮО можна назвати наступні: а) установчі документи, що відображають систему управлінських органів (одноосібних, де є один керівник; колегіальних, де рішення приймають кілька осіб), які формують і виражають волю ЮО, та підрозділів, що виконують певні функції, закріплені статутом; б) статутний фонд і рахунок в банку; в) наявність відокремленого майна, майнова й в певних випадках субсидіарна відповідальність; г) можливість виступати в суді від свого імені із зазначенням організаційно-правової форми та індивідуального найменування.

Види ЮО: 1) залежно від порядку створення – ЮО приватного права та ЮО публічного права; 2) залежно від основної мети діяльності – комерційні ЮО (здійснюють підприємницьку діяльність для отримання прибутку, а отриманий прибуток розподіляється між її учасниками), некомерційні ЮО (створюється для досягнення соціальних, благодійних, культурних, освітніх, наукових і управлінських цілей, для охорони здоров'я громадян, розвитку фізичної культури і спорту, задоволення духовних та інших цілей, спрямованих на досягнення суспільних благ).

До **профілю ЮО** доцільно відности її реквізити (найменування, місцезнаходження, ідентифікаційний код, банківську інформацію), а також:

Назва юридичної особи

(повна та скорочена українською, іноземною мовою)

Державна реєстрація (код ЄДРПОУ, організаційно-правова форма, місцезнаходження, контактна інформація, дата реєстрації, засновники/бенефіціари/уповноважені особи/співробітники, їх зміни, кількість працівників, розмір та склад статутного капіталу, корпоративна структура, філії, КВЕДи, фінансова та податкова звітність, стан банкрутства/припинення, потенційна фіктивність тощо):

Логотип

- ***пошукові та метапошукові системи***;
- ***державні реєстри*** – Державний реєстр друкованих засобів масової інформації та інформаційних агентств, Державний реєстр наукових установ, яким надається підтримка держави, Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань, Єдиний реєстр громадських формувань, Єдиний реєстр підприємств, щодо яких порушено впровадження у справі про банкрутство, Єдиний реєстр розпорядників та одержувачів

бюджетних коштів, Реєстр громадських об'єднань, Реєстр платників ПДВ;

- ***сервіси-агрегатори державних реєстрів*** – Clarity-Project, ContrAgent, E-data, Nomis, OdnodataUA, Opendatabot, VkursiPro, YouControl тощо;
- ***податки*** – Реєстри Державної податкової служби України (Дані про взяття на облік платників податків, Реєстр страхувальників, Реєстр платників єдиного податку, Реєстр платників, які використовують єдиний рахунок, Довідка про відсутність заборгованості, Дані Єдиного реєстру індивідуальних податкових консультацій, Реєстр неприбуткових установ та організацій, Дані реєстру платників ПДВ, Пошук фіскального чека, Пошук марки акцизного податку, Інформація про РРО, Інформація про ПРРО, Інформація про книги ОРО, Екземпляри РРО, Реєстр ЦСО; деякі сервіси потребують авторизації);
- ***фондовий ринок*** – Агентство з розвитку інфраструктури фондового ринку України (SMIDA), Державний реєстр випусків цінних паперів, Державний реєстр уповноважених рейтингових агентств, Реєстр інститутів спільного інвестування, Реєстр недержавних пенсійних фондів, Реєстр об'єднань професійних учасників ринків капіталу, Реєстри правозастосування (емітенти з ознаками фіктивності, відсутність за місцезнаходженням, заборона торгівлі цінними паперами на біржах тощо), Реєстр професійних учасників ринків капіталу та організованих товарних ринків, Реєстр сертифікованих осіб, Цінні папери іноземних емітентів, допущених до обігу в Україні;
- ***інше*** – Зведений перелік природних монополій, Імпортери та експортери України, Комплексна інформаційна система Національного банку України (Державний реєстр фінансових установ та Реєстр осіб, які не є фінансовими установами, але мають право надавати окремі фінансові послуги, в режимі онлайн), LinkedIn (співробітники), Реєстри Держпродспоживслужби України.

Фінансово-господарська діяльність (тендери, контрагенти/пов'язані особи, експортно-імпортні операції, інтелектуальна власність, ділова репутація, санкції)**:**

- ***публічні закупівлі*** – .007, Антикорупційний монітор, Громадський контроль держзакупівель, Єдиний вебпортал використання публічних коштів, Державні закупівлі, Зведені відомості щодо спотворення результатів торгів, Реєстр рішень АМКУ про антиконкурентні узгоджені дії, Є-data (публічні фінанси), Prozorro, BI Prozorro, Public Bid, Zakupivli.pro;
- ***зовнішньо-економічна діяльність/контрагенти*** – 52wmb.com (агрегатор митних накладних), Business registers EU (бізнес-реєстр Євросоюзу), Dato Capital (приватні компанії світу та їх керівники, free – базовий функціонал), Dun & Bradstreet (агрегатор реєстрів ЮО світу, free – базовий функціонал), European data (відкриті дані ЄС), Eurostat (статистична інформація), EU tenders (публічні тендери ЄС), Global Tenders (тендери з понад 190 країн), ICIJ Offshore Leaks Database (витоки щодо офшорів), ImportGenius, ImportKey, ImportYeti (доступ до бази даних митної служби США, потребує реєстрації), NBD Data, North Data (пошук за європейськими компаніями), OCCRP Aleph (матеріали журналістських розслідувань), OCCRP ID (добірка ресурсів для відстеження

	компаній та активів залежно від регіону, країни або сфери діяльності; можливі платний доступ або потреба реєстрації), OpenCorporates (агрегатор реєстрів ЮО країн світу, free – базовий функціонал), Open Ownership Register (бенефіціарні власники), Opentender (тендери 35 країн Європи), Trade Database Free (торгівельні дані, потребує реєстрації), UN Comtrade (глобальна база даних зовнішньоторговельної статистики), Vat-search (платники ПДВ; free – 3 кредити на місяць, базовий функціонал), Volza, Worldwide Registers (бізнес-реєстри країн світу), YouControl World (зв'язки між компаніями та приватними особами з країн СНД та Великобританії, free – 7 днів); Перелік іноземних торгових реєстрів (реєстрів компаній), • ***санкції*** – санкції щодо фізичних осіб, а також База даних юридичних осіб, до яких запроваджені санкції, Реєстр санкційних компаній РНБО, Спеціальні санкції Мінекономіки України, Список компаній, які станом на 24.02.2022 мали власника або бенефіціара з росії; • ***власність*** – Державний реєстр речових прав на нерухоме майно (запит за кодом ЄДРПОУ); • ***інтелектуальна власність*** – Державна система правової охорони інтелектуальної власності, Митний реєстр об'єктів права інтелектуальної власності, Спеціальна інформаційна система УКРНОІВІ, Український національний офіс інтелектуальної власності та інновацій, Iprop-ua.com, Opendatabot (перевірка торговельних марок, додатково – країни світу); European Union Intellectual Property Office, World Intellectual Property Organization, U.S. Patent and Trademark Office (США); • ***судові справи, виконавчі провадження, ділова репутація***.
Наявність ліцензії або спеціального дозволу:	
	• ***енергетика*** – Ліцензійний реєстр суб'єктів господарювання, що здійснюють господарську діяльність у сфері теплопостачання, Перелік суб'єктів господарської діяльності, які отримали ліцензії з виробництва теплової енергії на теплоелектроцентралях, ТЕС, АЕС, когенераційних установках та установках з використанням нетрадиційних або поновлюваних джерел енергії; • ***ліси*** – Реєстри Державного агенства лісових ресурсів; • ***медицина*** – Ліцензійний реєстр МОЗ, Реєстри Державної служби України з лікарських засобів та контролю за наркотиками; • ***надрокористування*** – Реєстр концесійних договорів, спеціальні дозволи на користування надрами (скан-копії спецдозволів та угод про користування); • ***транспорт*** – Ліцензійний реєстр міжнародних перевезень, Ліцензійний реєстр на провадження господарської діяльності з перевезення пасажирів, небезпечних вантажів та небезпечних відходів автомобільним транспортом, Ліцензійний реєстр на провадження господарської діяльності з перевезення пасажирів, небезпечних вантажів та небезпечних відходів залізничним транспортом, Реєстр ліцензій на перевезення авіаційним транспортом; • ***інше*** – Ліцензійний реєстр господарської діяльності з надання послуг і виконання робіт протипожежного призначення, Перелік дозволів на виконання

	робіт підвищеної небезпеки та на експлуатацію (застосування) машин, механізмів, устаткування підвищеної небезпеки, Перелік суб`єктів господарювання, які мають ліцензії на провадження господарської діяльності з надання послуг в галузі технічного захисту інформації, Реєстр ліцензій на користування радіочастотним ресурсом України, Реєстр ліцензій на провадження охоронної діяльності та ремонту вогнепальної зброї невійськового призначення.

9. Відстеження транспорту та контейнерів

Літальні апарати: *трекери* – ADS-B Exchange, Adsb.fi, Flightradar24, FlightAware, IntelSky Military Radar, OpenSkyNetwork, Planefinder, RadarBox; *інше* – Airframes.org (міжнародний реєстр повітряних суден), Aviation Safety Network (база даних авіаподій), Drone Crash Database (база аварій військових БПЛА за повідомленнями ЗМІ), FlightConnections (планові авіарейси), Jetphotos.com (фото літаків), OpenSky-Network (мережа відстеження польотів), Planespotters.net (інформація про літаки, їх фото, рейси, трекер тощо), SkyVector (повітряна обстановка для планування польотів); Orbitrack (трекер супутників у реальному часі).

Морські судна: *трекери* – MarineTraffic (free – 7 днів), Marine Vessel Traffic, Military Ship Tracker (військові кораблі), MyShipTracking, SeaTracker (RU), ShippingExplorer, ShipTraffic, VesselFinder, VesselTracker, *інше* – Balticshipping та Crewell (працевлаштування моряків), BoatInfoWorld (довідкова інформація про кораблі), Crew List Index Project (історичні відомості про кораблі та екіпажі), LogisticsGlossary (довідник логістичних термінів), Maritime Awareness Project (карта морських кордонів та економічних зон), OpenSeaMap (морська карта, трафік суден, моніторинг погодних умов, глибини), Sea Ports Catalog (каталог портів), Shipspotting (довідкова інформація про кораблі, їх фото), World Shipping Register (Всесвітній реєстр суден).

Контейнерні перевезення: *трекери* – CMA CGM Group, Container-Tracking, Maersk Tracking, SeaRates Container Tracking, ShipIt Container Tracking, ShipmentLink, Shipping Container Info, ShippingLine, Track-Trace, Utopiax Container Tracking, Карта руху суден; *інше* – BIC-Code (міжнародний реєстр власників контейнерів).

Наземний транспорт: geOps (онлайн-трекер потягів), OpenRailwayMap (карта залізничної інфраструктури), Transit Visualisation (візуалізація наземного транспорту), WikiRoutes (RU, довідник громадського транспорту), Яндекс.Расписания (онлайн-карта розкладу та маршрутів поїздів, електричок та автобусів по рф, білорусі та Казахстану).

10. Інструменти для протидії російській агресії

Фізичні та юридичні особи рф:

- каталог сервісів, портал та хаб ***відкритих даних*** рф;
- ***добірка ресурсів*** для пошуку даних щодо фізичних та юридичних осіб (RU), OSINT Russia (каталог посилань від OsintFlow);
- ***громадяни рф*** – Cybersec.org (або CyberSec Karma Bot), DataAnalytic (bot), Mail2Phone (RU, bot, може знайти номер телефону за відомою електронною поштою, яка пов'язана з профілями Сбербанку та Однокласників), OsintFlowFindBot (bot, free – 10 запитів щодня, базовий функціонал), Prob3y (RU, bot), Reveng.ee, X-Ray (free – 2 кредити, потребує реєстрації, пошук росіян на час збройної агресії безкоштовний), Відкрита база даних публічних посадових осіб Росії, Білорусі та Казахстану, Відомості про ІПН фізичної особи, Перевірка дійсності ІПН фізичних осіб (RU, дата визнання недійсності в більшості випадків співпадає з датою смерті), Перевірка дійсності паспорту нромадянина рф (RU), а також боти для універсального пошуку;
- ***воєнні злочинці*** (інформація не завжди є офіційною, а тому потребує перевірки) – Війна і санкції, Воєнні злочинці рф, Книга катів українського народу, «Коллаборанты и предатели» (RU, канал на YouTube), Миротворець та IDentigraF (пошук за фото у БД «Миротворець», потребує реєстрації, 5 запитів на день), «Не жди меня из Украины» (Telegram-канал), «Список коррупционеров и разжигателей войны» (RU, «Международный Фонд борьбы с коррупцией» О. Навального), «Список Путина» (RU, база «Форума Свободной России»), Evocation.info (пропагандисти), Lostivan Wiki, Russian War Criminals, а також *матеріали OSINT-розслідувачів* (InformNapalm, Molfar, OsintFlow, OSINT Бджоли, Truth Hounds тощо); *військова техніка* – WarSpotting;
- ***транспортні засоби*** – Номерограм (RU), сервіси державтоінспекції рф (RU), AVinfoBot (RU, bot, потребує підписки), VIN01 (RU);
- ***фінансовий та майновий стан*** – Декларатор (RU, недержавний агрегатор майнових декларації), Інформаційний портал про об'єти нерухомості (RU), Мої податки (RU), кадастрові карти – Публічна кадастрова карта (RU), Центр боргів (RU), Egrp365 (RU, ЕГРН 365, неофіційний аналог держреєстру нерухомого майна), ShtrafKZBot (RU, bot, перевірка штрафів/налогів/пені);
- ***інше*** – База депутатів єдиної росії (RU), Сервіс перевірки недіючих паспотрів (RU), Dominfo.info (RU, пошук інформації про забудовників, керуючі компанії та нерухомість);
- ***сайти (реєстри) органів державної влади*** – генеральна прокуратура

	росії (RU); державний реєстр компаній ЕГРЮЛ (RU), державний реєстр нерухомості (RU), єдиний федеральний реєстр відомостей про банкрутство, боржників та аукціонів з продажу заставного майна (RU), єдиний федеральний реєстр відомостей про факти діяльності юридичних осіб (RU), кадастрова карта росії (RU), офіційно опубліковані правові акти (RU), реєстр несумлінних постачальників (підрядників, виконавців) та реєстру несумлінних підрядних організацій (RU), реєстр суб'єктів природних монополій (RU), реєстр федерального майна рф (RU), федеральна податкова служба (RU, пошук за реєстрами, сервіс «Прозорий бізнес», виписка з ЄДРЮО/ЄДРІП), фонд соціального страхування (RU); • ***перевірка контрагентів*** – Е-ДОСЬЕ (RU), ЗаЧестныйБизнес (RU, free – базовий функціонал), Оновлена інформація про акціонерні товариства (RU), Чекко (RU), Audit-it (RU), Database for all Russian companies, DataNewton (RU), Egrul_bot (RU, bot), Fek (RU) (free – базовий функціонал), Injust.pro (RU), List-org (RU), Rusprofile (RU, free – базовий функціонал), Star-Pro (RU, free – базовий функціонал); • ***тендери*** – Єдина інформаційна система в сфері закупівель (RU), РосТендер (RU, free – базовий функціонал), TenderGURU (RU); • ***цінні папери*** – Прайм, Скрин, Disclosure.ru (RU, розкриття інформації на ринку цінних паперів); реєстри банку росії (RU); • ***інтелектуальна власність*** – відкриті реєстри федерального інституту промислової власності (RU); • ***освіта*** – національне акредитаційне агенство в сфері освіти (RU), реєстр ліцензій (RU), реєстр організацій, що провадять освітню діяльність за освітніми програмами, які мають державну акредитацію (RU); • ***суди, нотаріат*** – картотека арбітражних справ (RU) та справ загальних судів (RU), портал третейських судів (RU); інформаційний нотаріальний портал (RU, виконавчі провадження, розшук спадкоємців), федеральна служба судових приставів (RU, виконавчі провадження).

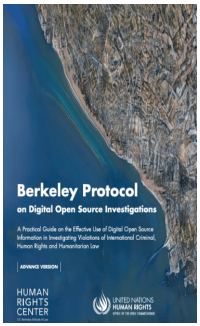
Фізичні та юридичні особи рб:

- ***сайти (реєстри) органів державної влади*** – єдиний державний реєстр юридичних осіб та індивідуальних підприємців (ВУ), єдиний державний реєстр відомостей про банкрутство (ВУ), єдиний реєстр ліцензій (ВУ), міністерство з податків та зборів (ВУ, реєстри фізичних та юридичних осіб), міністерство транспорту і комунікацій (ВУ, ліцензії перевізників); міністерство юстиції (ВУ, відомості про заборгованість); національний правовий інтернет-портал рб (ВУ), публічна кадастрова карта (ВУ), реєстр адрес (ВУ), реєстр нерухомості (ВУ), реєстр свідоцтв про державну реєстрацію товарів (ВУ), реєстр характеристик нерухомого майна (ВУ), торговий реєстр (ВУ);
- ***перевірка контрагентів*** – BizInspect (ВУ), Картотека (ВУ), СтатусПро (ВУ);
- ***інтелектуальна власність*** – національний центр інтелектуальної власності (ВУ);
- ***суди*** – портал електронного судочинства (ВУ).

11. Використання відкритих даних в інтересах досудового розслідування. Протокол Берклі

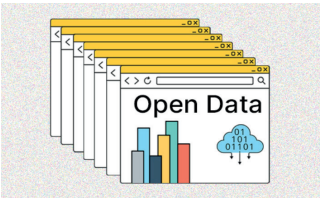
Епоха цифрових технологій незмінно диктує свої вимоги до роботи правоохоронних органів задля ефективного виконання покладених на них завдань у ході здійснення досудового розслідування. За цих умов ІТ-процеси потребують впровадження нових підходів до належного збору та збереження електронних даних з відкритих джерел, що в подальшому можуть використовуватися як докази у кримінальних провадженнях.

З метою імплементації досвіду найкращих світових практик, при неухильному дотриманні вимог Кримінального процесуального кодексу України (далі – КПК України) Офісом Генерального прокурора у 2021 р. рекомендовано запровадити в практичну діяльність слідчих та їх процесуальних керівників принципи, методики й стандарти огляду цифрової інформації з відкритих джерел, що викладені у Протоколі Берклі.



Протокол Берклі (є неофіційний переклад українською мовою) – практичний посібник щодо методів та процедур використання загальнодоступної цифрової інформації при розслідуванні порушень міжнародного кримінального права, прав людини та гуманітарного права, який у 2020 р. представили Центр прав людини Університету Берклі (Каліфорнія, США) та Офіс Верховного комісара ООН з прав людини. Над ним працювали понад 150 міжнародних експертів. Він окреслює мінімальні стандарти пошуку, збирання, зберігання, перевірки та аналізу даних з відкритих джерел з дотриманням професійних, правових та етичних принципів.

За висновками Офісу Генерального прокурора вказана практика може застосовуватися не тільки під час досудового розслідування кримінальних проваджень про злочини міжнародного характеру, вчинені в умовах екстериторіальності, або ті, які розслідуються без доступу до території їх місця вчинення, але також для збору інформації з відкритих джерел, що здатна мати доказове значення в будь-якій категорії проваджень.



Для цілей Протоколу Берклі (п.п. 14-18) **інформація у відкритому доступі** включає загальнодоступні відомості, які будь-хто може *спостерігати* (перейшовши на відповідний сайт з використанням будь-якого безкоштовного веббраузера), *купувати* (платні послуги, що доступні для всіх представників громадськості, а не тільки для певних груп, приміром співробітників правоохоронних органів або приватних детективів) чи *запитувати* (звернення, що можуть бути подані будь-якою особою щодо публічних відомостей до державних органів

відповідно до нормативних актів про свободу обігу інформації або доступу до неї), не вимагаючи особливого правового статусу чи несанкціонованого доступу.

На сьогодні в інтернеті зростає обсяг даних, що оприлюднюються за відсутності згоди власників – через злам, витік, наявність вразливостей безпеки або публікацію іншими особами без відповідних дозволів. Хоча ця інформація є загальнодоступною і, отже, формально вважається відкритою, все ж можуть існувати юридичні та етичні обмеження щодо шляхів її використання. Крім того, цифрові відомості можуть бути доступними для тих, хто має спеціальні технічні знання та здатний підключитися до мереж і даних, недосяжних пересічній людині (наприклад, отримати доступ до Dark Web можна лише за допомогою певних програм, наприклад браузера Tor).

Протокол Берклі включає цю інформацію в сферу відкритого доступу доки не відбувається несанкціонованого зверенння до неї – подібні відомості не передбачають безпосередньої взаємодії з іншими користувачами інтернету. Заволодівання даними від вказаних осіб шляхом комунікації з ними вважається закритим джерелом. У такий спосіб встановлюється загальна заборона доступу до інформації та мереж за відсутності правових чи етичних підстав (приміром, шляхом використання паролів, за допомогою обману чи інших методів соціальної інженерії тощо) (п. 63 Протоколу Берклі).

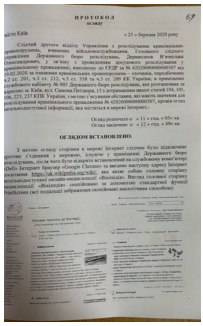
Інформація із закритих джерел – це *відомості з обмеженим доступом* або *доступом, що охороняється нормативними актами*, але які можуть бути отримані на законних підставах через приватні канали, такі як судові процеси або запропоновані особою добровільно.

Відповідно до п. 65 Протоколу Берклі використання віртуальних особистостей порушує умови користувацької угоди сервісів і, зокрема, платформ соціальних медіа. І хоча такі віртуальні особистості необхідні, коли вони використовуються для пошуку та збереження даних у відкритому доступі, їх не слід задіювати для спроб зібрати викладений у соцмережах контент, обмежений у вільному перегляді; або як привід для отримання інформації безпосередньо від особи під прикриттям неправдивої особистості. Така поведінка, на думку міжнародних експертів, виводить дослідників за межі розслідування з використанням відкритих даних, суперечить етичним принципам та може порушувати відповідні правові приписи (право на недоторканність приватного життя та захист даних тощо).

Після того, як цифровий контент буде ідентифіковано та визнано належним для розслідування, слідчий повинен визначити необхідний метод збору. Ці прийоми можуть змінюватись залежно від того, чи мають такі відомості потенційну доказову силу в судовому розгляді та будуть використовуватися

для прийняття процесуальних рішень або вони будуть сприяти лише проміжному результату роботи. У випадках, коли мова йде просто про результати роботи, може бути достатньо скріншоту або перетворення вебсторінки на pdf-файл, тоді як вміст, що має потенційну доказову силу, вимагає більш ретельного та обгрунтованого методу збору (п. 153 Протоколу Берклі).

Законом України «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» від 15 березня 2022 року № 2137-IX ст. 237 КПК України була доповнена *новим об'єктом огляду* – комп'ютерні дані (ч. 1) та *вимогами до його проведення* – огляд комп'ютерних даних проводиться слідчим, прокурором шляхом відображення у протоколі огляду інформації, яку вони містять, у формі, придатній для сприйняття їх змісту (за допомогою електронних засобів, фотозйомки, відеозапису, зйомки та/або відеозапису екрана тощо або у паперовій формі) (абз. 2 ч. 2).



ПРОТОКОЛ

ОГЛЯДОМ ВСТАНОВЛЕНО:

Водночас суди, маючи на меті додержання засади безпосередності дослідження доказів, отриманих шляхом огляду вебсторінок, ставлять питання про дослідження в ході судового засідання інтернет-ресурсу, з якого виготовлена копія відповідної інформації, що не завжди може бути реалізовано через можливість його видалення чи модифікації. Отже, з метою забезпечення доступності інформації у відкритих джерелах слід здійснювати її цифрове зберігання (архівацію), яке дає змогу захистити та зберегти дані з плином часу, включаючи їх справжність, доступність, ідентичність, постійність, рендеринг (візуалізацію) та зрозумілість. Саме ці індикатори цифрової інформації згідно з Протоколом Берклі підлягають фіксації.

Проводячи вказану слідчу дію відповідно до вимог ст. ст. 223, 237 КПК України, в обов'язковому порядку необхідно на підставі ст. 71 Кодексу *залучати спеціаліста*, який має вищу освіту у сфері інформаційних систем та технологій, для визнання у подальшому судом інформації, що міститься в виготовленому електронному документі як оригіналу згідно ч. 4 ст. 99 КПК.

Слідчі, які 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* (п. 154 Протоколу Берклі).

Тоді як збирання всієї наведеної нижче інформації вважається найкращою практикою, **перші три пункти** слугують **мінімальним стандартом для надання доказів у суді** (п. 155 Протоколу Берклі):

(a) *Цільова вебадреса: вебадресу зібраного контенту, також відому як єдиний локатор ресурсів (URL) або ідентифікатор.*

URL (Uniform Resource Locator, уніфікований локатор ресурсу) – це адреса ресурсу в мережі «Інтернет». Містить назву протоколу доступу (https, ftp, telnet, gopher та ін.) і, власне, шлях до ресурсу, формат якого залежить від схеми доступу, приміром https://www.president.gov.ua/ (сайт Президента України).

Стандарт URL використовує набір символів US-ASCII, тобто лише латинські літери, цифри та кілька знаків пунктуації. Усі інші символи (в т.ч. літери кирилиці) мають програмно перекодовуватися за протоколом URI (Uniform Resource Identifier, уніфікований ідентифікатор ресурсу). Наприклад, за його результатами строка виду https://uk.wikipedia.org/wiki/Вікіпедія відображається браузером як https://uk.wikipedia.org/wiki/%D0%92%D1%96%D0%BA%D1%96%D0%BF%D0%B5%D0%B4%D1%96%D1%8F (т.зв. процентне кодування).

Після опису послідовності дій слідчого щодо знаходження в інтернеті належного для потреб розслідування контенту фіксація його цільової вебадреси відбувається шляхом *копіювання оригінального URL* з адресного рядка браузера (якщо при переході на нього відбулась переадресація, то і початкову, і кінцеву адреси) та включення до тексту протоколу процесуальної дії. Не радимо використовувати сервіси для скорочення посилань (Bitly, is.gd, Short URL, Surli, Tinyurl та ін.) через неочевидність алгоритмів їх роботи, відсутність даних про термін функціонування таких посилань та гарантій їх незмінності.

З метою забезпечння зручності переходу за URL та перегляду вмісту цільової вебсторінки кращою практикою вважається відображення, крім її текстуальної адреси, ще і *QR-коду* (коду швидкої відповіді). Для цього необхідно скористатися вбудованим функціоналом браузера (наприклад, у Chrome на вільному від тексту та зображень місці сторінки правою кнопкою миши викликати контексне меню, обрати пункт «Створити QR-код для цієї сторінки», а потім його скопіювати) або спеціалізованими ресурсами – MeQR, Online QR Code Generator, QRcode Generator, QRCode Monkey.

(b) *Вихідний код: слідчі повинні захопити вихідний код HTML вебсторінки, якщо це можливо. Вихідний код HTML містить набагато більше інформації, ніж видима частина вебсайту. Вихідний код HTML сприятиме автентифікації зібраного матеріалу.*

HTML (HyperText Markup Language, мова розмітки гіпертексту) являє собою стандартизовану мову розмітки документів і використовується для відображення вебресурсів у браузері під час переходу на них. За допомогою HTML можна публікувати на сторінках сайтів не тільки тексти, а й мульти-

медійний контент (відео-, фото-, аудіо-), математичні формули та інші об'єкти. HTML-код обробляється браузером у вигляді текстових документів із розширенням .htm або .html. У спрощеному вигляді це набір рядків з інформацією про те, як відображати той чи інший елемент сайту.

Для завантаження коду HTML вебсторінки правою кнопкою миші викликаємо контекстне меню та натискаємо пункт «Зберегти як» (або через комбінацію клавіш Ctrl+S для ОС Windows чи Cmd+S для Mac ОС). Після цього необхідно обрати один з можливих варіантів збереження – *тільки HTML* (лише код без додаткового контенту; сторінка вподальшому може відображатися некоректно), *один файл* (у форматі MHTML, оптимальне рішення в більшості випадків) або *вебсторінка повністю* (крім HTML-коду зберігається окрема папка з усіма її елементами, в т.ч. з фото- та відеофайлами; водночас виникає необхідність описувати всі ці файли в протоколі) та стисло відобразити вказану дію в процесуальному документі із зазначенням назви (назв) файлу (файлів).

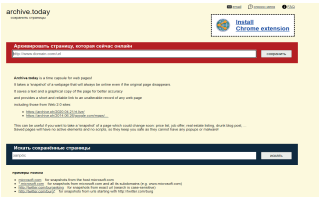
З огляду на технічні особливості окремих вебсторінок Протокол Берклі допускає неможливість в певних випадках завантажити їх код HTML. В такому разі про це необхідно зазначати в протоколі слідчої дії.

(c) *Захоплення всієї сторінки: слідчі повинні спочатку зробити знімок екрана цільової вебсторінки із зазначенням дати та часу. Причина цього полягає в найкращому уявленні того, що було побачено під час збору.*

Знімок екрана можна зробити *вбудованими засобами ОС* – клавіши PrtSc, Print Screen, застосунок «Ножиці» (для Windows) чи Shift+Cmd +4 (для Mac) або *за допомогою програм* – Apowersoft Free Screen Capture, FastStone Capture, Greenshot, LightShot, PicPick, ShareX. Скріншоти мають відображати всю послідовність дій слідчого (особливо для вкладених сторінок), містити системні час і дату, що відповідатиме часу та даті проведення огляду. З міркувань безпеки не буде зайвим заздалегідь прибрати елементи екрана, що не пов'язані з предметом огляду (папки, іконки програм, інші відкриті вкладки, особисту інформацію тощо) або створити окремий віртуальний робочий стіл.

Якщо *цільова вебсторінка містить прокрутку* (нові частини контенту динамічно відображаються, коли користувач прокручує сторінку, зокрема, в соцмережі чи месенджері), можна зробити: 1) декілька її скріншотів з частковим перекриванням один одного; 2) т.зв. довгий скріншот за допомогою Apowersoft Free Screen Capture, FastStone Capture, PicPick, ShareX чи можливостей «Інструменти розробника» браузеру Chrome (Ctrl+Shift+I → Ctrl+Shift+P «Run Command» → почати набирати «screen...», з'явиться підказка «Capture full size screenshot», обрати цю команду та дочекатись завантаження файлу у форматі .png); 3) експорт сторінки в форматі .pdf; 4) відео її перегляду за допомогою програм для запису екрана. При цьому обов'язковою умовою є попереднє відшукання необхідного фрагменту ресурсу (тобто фактичне завантаження частини дінамічного сайту до місця розташування, наприклад, цільового посту).

На додачу до наведених вище трьох обов'язкових пунктів Протоколу Берклі Офіс Генерального прокурора України рекомендував за допомогою інтернет-ресурсів, що призначені для вебархівації, **створювати архів цільової вебсторінки**. Вказані сервіси є своєрідними електронними бібліотеками, що забезпечують довготривале збереження зібраного матеріалу та постійний доступ до них. З огляду на відсутність контролю над серверами подібних вебархівів, а тому неможливість гарантувати незмінність даних та безперешкодність звернення до них, кращою практикою визнається архівування з використанням декількох ресурсів – як Internet Archive (The Wayback Machine), так і Archive.today (чи одному з його дзеркал archive.is, archive.li, archive.ph, archive.fo). При цьому час і дата такого архівування мають відповідати часу та даті проведення слідчої дії, тобто стан цільової вебсторінки зберігається саме на момент проведення огляду. За допомогою скріншотів або стислого опису в тексті протоколу фіксуються дії з архівування та наводиться посилання/QR-код на створений вебархів (краща практика).



(d) *Вбудовані мультимедійні файли: наприклад, якщо завантажують вебсторінку з відео або зображеннями, ці конкретні елементи також слід витягти та зібрати з вебсторінки.*

Завантаження вбудованих медіафайлів може здійснюватися за допомогою: 1) повного збереження вебсторінки (див. п. b); 2) виклику на зображенні правою кнопкою миші контексного меню браузера (пункт «Зберегти зображення як»); 3) використання спеціалізованих сервісів – FetchV (плагін для Chrome, завантажує відео з сайтів, де така функція за замовчанням відсутня), HImage (завантажує всі зображення зі сторінки), а також ресурсів для пошуку та верифікації відео та роботи на соціально-орієнтованих платформах.

Продукти для автоматизованного *створення стенограми* відеозапису – Buzz (GitHub, підтримка української), Happy Scribe (free – 30 хв. за реєстрацію на сайті), Sonix (free – 30 хв. за реєстрацію на сайті), Trint (free – 3 файли тривалістю до 3 год. на 7 днів) Whisper (GitHub), Whisper WebGPU.

(e) *Вбудовані метадані: слідчі повинні зібрати додаткові метадані цифрового елемента, якщо вони є та застосовні. 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.*

Вбудовані метадані мають значення для опису цифрового контенту, обставин його створення, розповсюдження або зміни (наприклад, для офісного документу – це дата та час створення чи останньої модифікації або копіювання на

певне місце носія інформації; ім'я користувача, який створив файл або вносив до нього останні зміни; розмір файлу тощо). Вони можуть бути або частиною файлу, або відображатися на вебсторінці, або міститися у її вихідному коді.

Для *формування табличного опису* великої кількості завантажених файлів та автоматичного отримання вбудованих метаданих з них кращою практикою є використання спеціалізованого програмного забезпечення – Directory Lister (free – 30 днів; для файлів та папок є можливість отримати хеш-суму), Filelist Creator, MediaInfo та ін.

(f) *Контекстуальні дані: контекстні відомості також слід збирати, якщо це має значення для розуміння цифрового елемента. Вони можуть включати коментарі до відео, зображення чи публікації; передбачати завантаження інформації; та/або інформацію про завантажувача/користувача, таку як ім'я користувача, справжнє ім'я чи біографію. Необхідність збору супутньої інформації слід визначити, виходячи зі специфіки випадку та цифрового матеріалу.*

До контекстуальних даних також можна віднести відомості щодо реакції користувачів на розміщені матеріали – кількість переглядів, цитувань, репостів, вподобайок чи негативних емодзі тощо.

(g) *Дані збору: слідчі, що ведуть розслідування з використанням даних у відкритому доступі, повинні записати всі відповідні дані, що стосуються збору, такі як ім'я збирача, IP-адреса машини, яка використовується для збору інформації, віртуальна особистість, за наявності, та мітка часу. Слідчі повинні переконатися, що системний годинник 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.*

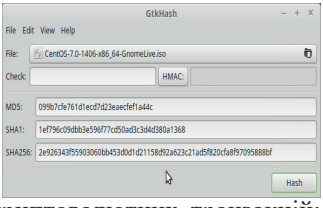
У вступній частині протоколу бажано зазначати: дату та час початку й завершення огляду (призупинення та поновлення), відомості про особу, що його проводить (за необхідності робиться посилання на виконання доручення слідчого); номер, дату та кваліфікацію кримінального провадження; місце проведення; ідентифікатори задіяної комп'ютерної техніки (ноутбуку, принтеру, оптичного приводу тощо); встановлену на персональному комп'ютері операційну систему, назву та версію браузера, а також інших необхідних програм (зокрема, VPN); учасників слідчої дії, обстановку її проведення тощо.

(h) *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 додати – або інструмент збирання – 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.

Хеш-сума (або хеш-значення) – послідовність символів фіксованої довжини, отримана шляхом перетворення за допомогою спеціального математичного алгоритму довільних вихідних даних (чисел, тексту, файлу та ін.), що використовуються для перевірки їх цілісності при передачі або збереженні (тобто захист від змін). Процес перетворення даних у хеш називають хешуванням, а алгоритм хешування – хеш-функцією. Більшість поширених хеш-функцій на виході дають великі числа в шістнадцятковому поданні (приклад для алгоритму SHA-1 – 7DD987F846400079F4B03C058365A4869047B4A0).

Властивості хеш-суми: ***незворотність*** (вихідні дані з неї не можна відновити ні математичними методами, ні перебором), ***відтворюваність*** (опрацювання одних і тих самих вихідних даних за допомогою однієї й тієї самої хеш-функції дає на виході один і той самий результат), ***унікальність*** (під час хешування різних вихідних даних мають виходити різні хеші, навіть якщо дані відрізняються на 1 біт).



Популярні алгоритми хешування – MD5 (довжина хешу – 128 біт, у 2011 р. визнаний недостатньо надійним через високу ймовірність колізій, проте досі використовується для перевірки цілісності контенту); SHA-1 (довжина хешу – 160 біт); SHA-2 (довжина хешу – 224, 256, 384 та 512 біт, зокрема SHA-256 застосовується в технології блокчейн для верифікації криптовалютних транзакцій; працює удвічі-втричі повільніше від MD5 та SHA-1) *та продукти* – HashTab (програма для PC, з 2022 р. не оновлюється), GtkHash (GitHub), Hash Calculator Online (обмеження для файлів – 32 Мб), Hash Checker (програма для PC), Hash Generator (програма для PC), Hash Tool (програма для PC), RapidCRC, (програма для PC, з 2005 р. не оновлюється), RHash (GitHub). Ситуація, коли в результаті перетворення двох різних наборів даних виходить один і той самий хеш, називається колізією. Для належної розрізнення подібних файлів кращою практикою є додаткове зазначення типу та розміру в байтах для кожного з них. Отримані дані заносяться до протоколу (в т.ч. у вигляді таблиці).

Отже, хеш-значення має гарантувати, що саме даний файл був виявлений під час огляду, зазначений в протоколі слідчої дії та додатках до нього, він не змінювався з моменту збору, тобто його можна вважати повноцінним оригіналом, а отже допустимим та належним доказом у провадженні.

Правила оцінки електронних доказів на предмет їх допустимості містяться в постановах об'єднаної палати Касаційного кримінального суду у складі Верховного Суду від 29 березня 2021 року у справі № 554/5090/16-к, від 25 вересня 2023 року у справі № 208/2160/18.

Зокрема, безпідставним є ототожнення електронного доказу як засобу доказування та матеріального носія такого документа. Характерною рисою електронного документа є відсутність жорсткої прив'язки до конкретного матеріального носія. У випадку його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа. Один і той же 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 як оригіналу можуть бути вирішені або повноважною особою, яка його створила (обчисленням контрольної суми файлу або каталогу з файлами (CRC-суми, hash-суми) чи накладенням цифрового підпису), або шляхом проведення спеціальних судових досліджень за наявності підстав.

Для виконання завдань кримінального провадження допустимість електронного документа як доказу не можна заперечувати виняткова на підставі того, що він має електронну форму (ч. 2 ст. 8 Закону України «Про електронні документи та електронний документообіг»).

Відповідно до п. 157 Протоколу Берклі довговічність і доступність інформації в інтернеті часто залежать від непередбачених обставин – вона може бути легко деконтекстуалізована, втрачена, стерта або пошкоджена. Завданням збереження цифрових матеріалів є забезпечення їх незмінності та безперешкодності доступу. Однак, коли йдеться про збереження відкритих даних для в питанні притягнення до юридичної відповідальності, метою є управління цифровими матеріалами та їх збереження з урахуванням забезпечення їхньої доступності, автентичності та можливості використання у процесі притягнення до відповідальності, включно з їхньою допустимістю під час судового розгляду. Таким чином, збереження відкритих даних у контексті розслідування передбачає збереження інформації протягом тривалого часу таким чином, щоб зібраний матеріал залишався зрозумілим для потенційних користувачів незалежно від контексту та мав достатній рівень підтвердження його автентичності.

З урахуванням цього, всі збережені в ході огляду *файли мають бути записані на матеріальний носій інформації* (гарною практикою вважається оптичний диск типу CD-R із серійним номером), який відповідно до ст. 105 КПК України долучається до такого протоколу слідчої дії як невід'ємний додаток.

Для того, щоб цифрові матеріали залишалися доступними і придатними для використання в інтересах досудового розслідування, наведених у цьому розділі рекомендацій бажано дотримуватися і під час їх фіксації, що здійснюється в рамках контррозвідувальної та/або оперативно-розшукової діяльності, шляхом складанням *акту огляду*.

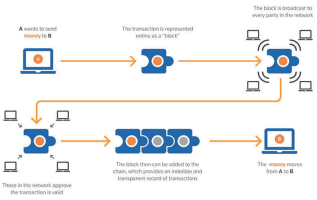
12. Основи дослідження криптовалютних трансакцій

Криптовалюта (Cryptocurrency) – це цифрове представлення вартості. Ця вартість може бути предметом цифрової торгівлі та функціонувати як засіб обміну, як звичайні гроші, що ми маємо в гаманці. Цей тип власності можна передавати іншим людям або зберігати та торгувати ним в електронному вигляді. Криптовалюти дозволяють людям купувати та продавати товари без використання банківської системи, оскільки вони не випускаються центральними банками.

Ці операції можливі на глобальному рівні. Вони роблять національні кордони чи національну валюту продавця та покупця абсолютно неважливими. Зазвичай, якщо є комісії за операції, вони досить низькі, а операції виконуються дуже швидко, оскільки не застосовуються юридичні правила, формальності чи обмеження. Нарешті, ці вартості повністю децентралізовані (тобто не прив'язані до жодної національної грошової системи), що забезпечує певний рівень анонімності.

Першим успішним *коїном* (монетою), що набув широкого поширення в якості засобу для розрахунків, переказу, обміну та накопичення, став Біткоїн (Bitcoin або BTC), створений у 2009 р. анонімним користувачем під ніком Сатоші Накамото. Усі інші монети, що з'явилися після нього (згідно CoinMarketCap на даний час існує близько 10 тис.), отримали назву *альткоїни* (альтернативний коїн), приміром Ether (ETH), Ripple (XRP), Cardano (ADA), Solana (SOL), Polkadot (DOT), Litecoin (LTC), Tron (TRN) тощо.

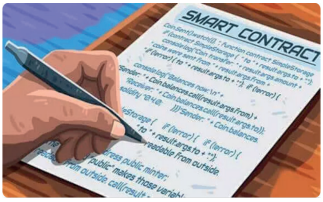
Найважливішою ознакою коїну є наявність власного *блокчейна* (blockchain, ланцюжок блоків) – децентралізованого цифрового реєстру або особливої бази даних, що підтримується численними комп'ютерами, розміщеними по всьому світу (вузлами). Дані блокчейну організовані в блоки, які розташовані в хронологічному порядку та захищені криптографією. Кожен блок містить часову позначку, хеш (контрольну суму) попереднього блоку та дані транзакцій, подані як хеш-дерево. Інформація про транзакції зазвичай надається відкритою, не зашифрованою. Захистом від підробки та спотворення слугує включення хешу всього блоку в наступний блок. Тому внесення змін в один з блоків вимагає відповідних змін в усіх блоках після нього, що зазвичай зробити майже неможливо.



Для того, щоб, наприклад, продати криптовалюту, продавець ініціює транзакцію. Вона транслюється в мережу блокчейна, де кожен вузол (комп'ютер) отримує інформацію про транзакцію. Потім вузли починають процес перевірки її

автентичності, використовуючи алгоритми консенсусу. Після того, як транзакцію схвалили ці вузли, її додають у новий блок разом з іншими нещодавно схваленими транзакціями. Завершений блок потім додається до існуючого ланцюжку блоків у хронологічному порядку. Кожен такий блок містить унікальний хеш попереднього блоку, створюючи безперервний і незмінний ланцюжок. Після додавання нового блоку, усі копії блокчейна на вузлах мережі оновлюються, щоб відобразити останні зміни. Після додавання блоку в ланцюжок усі його транзакції вважаються підтвердженими і незворотними. Верифікація всіх транзакцій, зокрема попередніх, відбувається кожний цикл досягнення консенсусу мережі.

Блокчейн-адреси, де зберігаються криптовалюти, побудовані на базі двох ключів – публічного та приватного. Перший використовується для «відкритої» частини адреси, другий – для підпису транзакцій і доступу до адреси, він призначений тільки для її власника. Наявні комп'ютерні потужності не дають змоги зламати блокчейн-адресу, зокрема «вгадати» приватний ключ методом підбору. Створювати блокчейн-адреси та керувати ними можна в спеціальному додатку – криптогаманці.



Наступним етапом у розвитку віртуальних активів став запуск у 2015 р. на базі блокчейну Ethereum платформи *смарт-контрактів* (smart contract, розумний контракт) – комп'ютерного алгоритму, призначеного для укладення самоздійснюваних угод, виконання яких буде забезпечено цим блокчейном. Завдяки цьому стало можливим випускати необмежену кількість криптоактивів і програмувати їх функції. Так з'явилися *токени* (або жетони). Смарт-контракти містять значення залишків на рахунках власників токенів, що надає можливість їх переказу з одного рахунку на інший без участі зовнішніх посередників в особі банків або державних органів. Крім того, такі транзакції є простежуваними, прозорими та незворотними. Токен не має власний блокчейн, це його основна відмінність від монети. Смарт-контракти не тільки містять інформацію про зобов'язання сторін і санкції за їх порушення, а й самі автоматично забезпечують виконання всіх умов договору.

Фактично, *токен* – це цифровий сертифікат, аналог цінних паперів (акцій), що використовуються у світі фіатних валют. Він фіксує зобов'язання емітента перед власником токена. Крім того, це одиниця розрахунку, яка функціонує на базі інших платформ. Сфера застосування токенів ширша, ніж у монет: вони використовуються для надання послуг; або для посвідчення, підтвердження прав на щось всередині самої онлайн-платформи; їх

можна обміняти на якісь інші послуги або продати за іншу валюту; це потужний інвестиційний інструмент для стартапів, що дає змогу їхнім власникам отримувати дивіденди.

Завдяки розробці та спрощенню смарт-контрактів найпопулярнішою блокчейновою платформою для токенів є Ethereum. Токени, що базуються на цьому блокчейні, мають стандарт (набір узгоджених правил функціонування) ERC-20. Найбільш популярні з них – Shiba Inu, Tether, Uniswap та ApeCoin – були створені за стандартом ERC-20. До найрозповсюдженіших стандартів токенів можна віднести BEP-20 (блокчейн Binance Smart Chain або BSC, має однакову архітектуру з ERC-20), TRC-20 (блокчейн TRON), ERC-721 (дозволяє створювати незамінні токени NFT в мережі Ethereum), ERC-777 (стандарт взаємозамінних токенів, який покращує ERC-20), ERC-1155 (дозволяє групувати транзакції).

Хоча згадані криптовалюти пропонують низку переваг, насамперед, відсутність необхідності довіряти банківській установі для надсилання платежів будь-куди та будь-кому, але одним з ключових недоліків є те, що ціни на них непередбачувані та мають тенденцію коливатися, часто доволі сильно. Це ускладнює їх використання пересічними людьми. Як правило, вони очікують, що зможуть контролювати, скільки коштуватимуть їх гроші за тиждень, як з міркувань безпеки, так і для забезпечення засобів до існування. Одним зі способів стабілізації курсу стала прив'язка коїнів до реальних активів (долару США, цінні папери), біржових товарів (золото, нафта) чи інших криптовалют зі створенням централізованого резерву для їх гарантованого обміну за курсом (різниця коливається в межах 1%). Так з'явилися *стейблкоїни* (стабільний коїн) – Tether (USDT), USD Coin (USDC), TrueUSD (TUSD), Binance USD (BUSD), DAI, Tether Gold (XAUT), FRAX.

Окремий вид активів – NFT або невзаємозамінні токени, що використовуються для підтвердження прав власності та доказу справжності певного віртуального активу. Якщо один біткоїн завжди дорівнює іншому біткоїну, то з NFT це так не працює. Кожен такий токен унікальний, має власний попит і ціну. Експерименти з NFT розпочались у 2013-2014 рр. шляхом випуску творів мистецтва, музики, об'єктів для блокчейн-ігор, колекціонування тощо. У вересні 2023 р. понад 95 % NFT вже мали нульову грошову оцінку.

Криптовалютний гаманець – програмне забезпечення, що дає змогу здійснювати операції з криптовалютою. Важливо зрозуміти, що безпосередньо в браузері або на вашому комп'ютері монети не зберігаються, а лише відображаються, перебуваючи у мережі блокчейна. Щоб мати доступ

до криптовалюти на гаманці та проводити операції з нею, необхідно два ключі шифрування – публічний і приватний. Без них неможливо відкрити доступ до реєстру блокчейна та перевести актив іншій людині.

Публічний або відкритий ключ – це адреса (рахунок), куди відправляються цифрові валюти. Його можна порівняти з номером банківської картки. Відкритий ключ використовується для створення транзакції, його ви можете сміливо розголошувати, якщо очікуєте переказу коштів на рахунок.

Приватний або закритий ключ – це інструмент підтвердження переказу, аналог цифрового підпису. Без цього ключа власник криптогаманця не зможе розпоряджатися його вмістом. Приватний ключ порівнюють з паролем від банківської картки, його не можна розголошувати.

Кожен із ключів має вигляд унікального набору символів, що включає букви і цифри. Для прикладу можна взяти ключі шифрування блокчейна Bitcoin. Він працює на основі алгоритму SHA-256, що генерує 256-бітове число. Для зручнішої роботи ним створено комбінацію, що складається з 64 символів – приміром, 4BBFF74CA25A2A00409DCB24EC0418E9A41F9B3B56216A183E0E9731F4589DC6. Це і є закритий ключ, хоча довжина робить їх вкрай незручними для зберігання, захисту та використання. Ця проблема стає ще масштабнішою під час взаємодії з кількома рахунками, що передбачає запис і безпечне офлайн-зберігання вже декількох таких комбінацій, оскільки для управління кожним криптовалютним рахунком всередині вашого гаманця потрібен окремий приватний ключ. Останній дає змогу користувачеві підписувати транзакції, таким чином підтверджуючи згоду з параметрами кожного переказу.

Однак гаманець має *seed-фразу* або секретну фразу відновлення, що являє собою унікальну мнемонічну комбінацію з 12, 18 або 24 слів, яка виконує роль резервної копії такого криптовалютного гаманця. Якщо точніше, фраза відновлення являє собою довге випадкове число або ентропію. І хоча основа для згаданого числа є випадковою, сам seed завжди включає слова з переліку 2048 можливих слів англійською мовою (або список BIP39).

По суті, це майстер-ключ від усіх ваших приватних ключів. На відміну від них seed-фраза не дозволяє підписувати транзакції, однак у неї є миттєвий доступ до кожного приватного ключа всередині вашого криптогаманця, а отже, і до кожного рахунку на ньому. У разі втрати доступу до гаманця монети та токени, як і раніше, залишаться в рамках блокчейна, тоді як введення seed-фрази в інший гаманець у правильному порядку відновить усі приватні ключі, які зберігалися в початковому криптогаманці. Втім, якщо ця фраза буде втрачена, розпоряджатися криптоактивами вже не вийде.

Криптогаманці поділяються ділять на кастодіальні та некастодіальні. Некастодіальні бувають «гарячими» (десктопними, мобільними, онлайновими) та

«холодними» (апаратними та паперовими).

Створення *кастодіального гаманця* схоже на відкриття рахунку в банку: дані щодо власника передаватимуться та зберігатимуться у третій стороні – кастодіану (наприклад, централізована криптобіржа, деякі обмінники та сервіси-кастодіани). Щоб його отримати, потрібно вибрати компанію та зареєструватися на її сайті, для цього знадобляться email або телефон, а також пароль.Кастодіан має повний контроль над криптоактивами та можуть в будь-який час втрутитися у них (наприклад, заблокувати), водночас він несе відповідальність за збереження коштів клієнта.

Некастодіальний гаманець – це інтерфейс для доступу до гаманця на блокчейні. Особливість *«гарячого»* зберігання: такий гаманець постійно з'єднаний з інтернетом, а ключ перебуває в десктопній програмі чи мобільному застосунку – AtomicDEX, Blockchain Wallet, Coinbase Wallet, Exodus, MetaMask, Phantom, TrustWallet або особистому кабінеті онлайн-сервісу – BitAddress, WalletGenerator, дозволяючи швидко проводити транзакції. Це несе ризики його втрати або викрадення, а отже отримання сторонніми особами доступу до вашої криптовалюти. *«Холодний»* гаманець є більш безпечним способом зберігання активів, оскільки дозволяє розміщувати ключі поза програмами чи сайтами, у вигляді апаратного пристрою – CoolWallet, Ledger, SafePal, Trezor, Walletz (нагадує флеш-накопичувач чи банківську карту з підтримкою Bluetooth, NFC, QR-кодів) чи паперового носія з seed-фразою чи QR-кодом.

Один криптогаманець дозволяє працювати з декількома рахунками.

Існують різні **способи купівлі/продажу криптовалюти**:

• *криптобіржа* – це онлайн-сервіс, який на основі технології блокчейн дозволяє клієнтам обмінювати (купувати, продавати та зберігати) криптовалюти на інші активи, фіатні гроші або інші цифрові валюти. Вона надає можливість користувачам створювати облікові записи, здійснювати торгівлю за допомогою різноманітних інструментів, відкривати депозити та виводити криптовалюту на зовнішні гаманці або банківські рахунки.

Централізовані біржі (Centralized Exchanges, або CEX) часто пропонують більше сервісів, але більш скромний список доступних криптовалют. Вони ведуть легальну діяльність та гарантують безпеку активів користувачів. Щоправда, на таких майданчиках доведеться пройти обов'язкову верифікацію. Найвідоміші CEX біржі криптовалют – Binance, Bitfinex, Bitget, Bybit, Coinbase, Gate.IO, HTX, Kraken, KuCoin, OKX, WhiteBIT (UA).

Децентралізовані біржі (Decentralized Exchanges, або DEX) працюють у «сірій зоні» та не входять до юрисдикції конкретної держави. На відміну від традиційних CEX, на таких платформах транзакції та торги автоматизовані

за допомогою смарт-контрактів і децентралізованих додатків – користувачі торгують безпосередньо між собою, без посередництва централізованої платформи Через особливості архітектури часто мають досить складний інтерфейс. Ключі від гаманців користувачів вони не зберігають, тому не несуть відповідальності за збереження активів. Найвідоміші DEX біржі криптовалют – ApeX Pro, Balancer, Curve, dYdX, KyberSwap, OKX DEX, Slingshot, Uniswap, 1inch;

• *криптовалютний обмінник* – це сервіс, який пропонує послуги з обміну цифрових активів, в т. ч. на фіатні (державні) гроші та навпаки. Вони бувають *трьох типів – онлайн-платформи, фізичні пункти* та *P2P-обмінники*. Принцип дії загалом однаковий – клієнт оформлює заявку, віддає одну криптовалюту й отримує іншу або гроші (або назворот). Різниця полягає у способі отримання фіату: онлайн-обмінник, наприклад BestChange (RU), Bitcoinmarket.global (RU), Bitcoin24, bits.media (RU), Changeit, ChangeNOW, Coin24, ObmenAT24, Obmify, Scanbit, 100btc, КурсЕксперт (RU), переводить його на банківську картку, а фізичний – видає готівкою. P2P-сервіси Bitcoin Global, Binance P2P, ByBit P2P та ін. виконують роль посередника між двома клієнтами, один з яких купує криптовалюту, а інший продає.

На відміну від криптовалютних бірж, обмінники не зберігають активи користувачів. Вони отримують валюту від клієнта на свій гаманець, а замість них видають фіат (гривні, долари, євро тощо) із власних резервів. При цьому, в курс обміну криптовалют на таких сервісах вже включено комісію за їхні послуги, через що її ціна відрізняється від ринкової;

• *криптобанкомати* не пов'язані з банківськими рахунками. Замість цього вони безпосередньо з'єднуються з криптовалютними біржами через блокчейн для забезпечення можливості миттєвої купівлі та продажу. Ці біржі також визначають обмінний курс на основі поточної ринкової вартості на момент транзакції. Потрібно просто відсканувати QR-код, перевести криптовалюту на надану адресу, а потім отримати гроші готівкою або банківським переказом. Для останнього тобі необхідно вставити в криптобанкомат свою дебетову або кредитну картку. Основний недолік криптобанкоматів, якщо ти використовуєш їх для виведення криптовалюти на карту – значна комісія. Банкомати можна розділити на *два основних типи*: *односторонні* та *двосторонні*. Перший тип банкоматів дає змогу тільки купувати криптовалюту, а другий тип пропонує додаткову можливість продажу.

Їх можна знайти через Карту біткоїн-банкоматів чи Coin ATM Radar.

Сервіси для відстеження трансакцій – це майданчики, що володіють різними інструментами для відображення розрахунків чи виводу криптовалюти. Блокчейн-аналіз передбачає дослідження, класифікацію, моніторинг адрес і транзакцій.

Утім некоректно стверджувати, що використання криптовалют забезпечує повну анонімність, оскільки задіювана технологія відкритого блокчейна зберігає записи всіх операцій, а тому вони є доступними і для інших користувачів, хоча ці відомості не містять персональних даних їх учасників. З цієї причини саме криптовалютні трансакції набувають дедалі більшої популярності для здійснення протиправної діяльності.

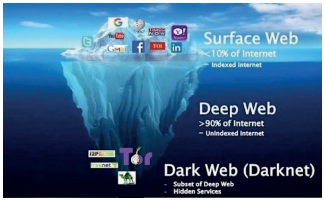
Операції з віртуальними активами – достатньо широке джерело інформації. Належне їх відстеження може допомогти ідентифікувати підозрілу особу чи транзакцію: OSINT-технології, що використовують інформацію з блокчейна у поєднанні з відповідним іпрограмним забезпеченням, яке може зв'язувати криптоадреси з певною централізованою криптобіржею, обмінником та навіть з конкретним користувачем.

Особистість і гаманець – різні поняття: «особистість» необов'язково одна людина, може бути й організація, «гаманець» – в однієї персони може бути кілька гаманців і кілька осіб можуть мати доступ до одного гаманця.

Інструменти для відстеження трансакцій – Arkham Intelligence, Blockchain Explorer, Blockpath, Breadcrumbs (free – 2 запити та 1 сповіщення; потребує реєстрації), Crystal Lite, GraphSense (GitHub), MetaSleuth (free – 200 запитів на місяць), Orbit (GitHub), Shard (RU), Tokenview, WalletExplorer, WalletTracker (GitHub); *для ETH* – Etherscan, Ethtective; *для TRX* – Tronscan; *для BNB* – Bscscan; *інше* – Bitinfocharts (статистика криптовалют), Crypto Sanctions Screening Tools (санкції в криптоекосистемі). Мінусом окремих подібних програмних продуктів є неможливість побудувати візуалізацію ланцюжку трансакцій за певним криптогаманцем. Більш потужні рішення для відстеження – Chainalysis, Crystal Expert, Elliptic, Global Ledger, TRM тощо – вже мають платну підписку.

Подальша ідентифікація власників криптогаманців переважно здійснюється в рамках кримінальної процесуальної діяльності шляхом направлення запитів на розкриття інформації конкретною біржею чи обмінником, в тому числі в рамках міжнародної правової допомоги.

13. Пошук у DarkNet



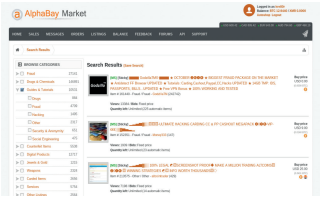
Усі дані в глобальній мережі умовно можно розподілити на три нерівномірні сегменти – Surface Web (приблизно 10 %, є загальнодоступним та індексується стандартними пошуковими системами), Deep Web (близько 90 %, вебсторінки не індексуються цими пошуковиками й на них, зазвичай, не ведуть посилання з «поверхневих» ресурсів) та Dark Web (DarkNet або тіньова мережа, доступ можливий лише за допомогою спеціального програмного забезпечення).

На відміну від *Surface Web* більшість ресурсів *Deep Web* – це інформація, безпосередньо не призначена для широкого перегляду (приміром, окремі сайти державних установ та комерційних структур, сторінки облікових записів різноманітних вебресурсів, хмарні сховища, сайти з платним доступом, бази даних, закриті форуми, каталоги, бібліотеки тощо). Найчастіше через пошукові системи можна знайти лише стартові сторінки таких ресурсів, але не їх контент. Потрапити на них можна через звичайний браузер, але для цього потрібно мати пряме посилання на вебсайт (на відміну від звичної адресації, такий URL містить велику кількість випадкових символів для ускладнення підбору), а також відповідний логін та пароль (іноді ще IP- або MAC-адресу, якщо за ними також відбувається верифікація користувача).

DarkNet (або onion-мережа) складається з ресурсів, що використовують власні DNS (домени) та адресний простір – домен верхнього рівня .onion чи .i2p замість звичних .com або .net. З'єднання між учасниками встановлюється в зашифрованому вигляді із задіянням нестандартних портів і протоколів. Тому цей сегмент недоступний без застосування браузерів з особливими алгоритмами маршрутизації (onion-протоколами) – Tor, Onion Browser, OrNet. У якості альтернативи виступає мережа I2P (Invisible Internet Project), більш безпечна та швидка, але менш інтуїтивно зрозуміла й популярна. Але за її допомогою можна отримати доступ лише до певних сайтів (т. зв. eepsites).

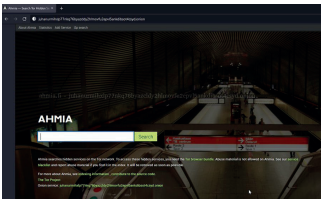
Фактично DarkNet являє собою сукупність анонімних комп'ютерних мереж, архітектура яких влаштована так, щоб унеможливити стеження та контроль за поширенням інформації. Це робить її способом подолання будь-яких обмежень, конфіденційним каналом спілкування чи навіть знаряддям кіберзлочинців. Саме тому в Даркенеті є ресурси громадсько-політичних структур; сайти, присвячені розслідуванням, що небезпечно/заборонено вільно публікувати (наприклад, новинний сайт ProPublica), соціальні мережі та форуми, поштові сервіси, онлайн-бібліотеки без цензури, збірники цікавої інформації, торрент-трекери та головне – товари, послуги або контент, обіг яких законодавчо обмежений або зовсім заборонений.

Тут на торговельних майданчиках, форумах чи дошках оголошень про-



даються різноманітні документи, банківські карти, витоки даних, злами акаунтів, наркотики та зброя, інструкції чи довідники, програмне забезпечення, послуги тощо. В тому числі за допомогою інструментів OSINT можна спробувати деанонімізувати зловмисників, зібрати їх цифрові сліди (наприклад, шляхом тривалого моніторингу вузлів мережі, задіяння методів соціальної інженерії, використання різноманітних вразливостей, через неуважність або випадковість – застосування логінів/паролів з DarkNet у загальнодоступному сегменті та ін.) та запобігти потенційним кібер- або терористичним атакам, відстежити незаконні оборутки тощо. На сьогоднішній день одним з найбільш дієвих способів припинення такої незаконної діяльності є переміщення дій злочинців з віртуального світу в реальний, наприклад в процесі передачі наркотичних речовин, що були придбані в тіньовому інтернеті.

Пошук у DarkNet достатньо трудомісткий через наявність у кінцевій видачі великої кількості *спам-посилань* чи переодичну *зміну адресації окремих сайтів*. Цей сегмент просто не створений для того, щоб бути чітко організованою та проіндексованою частиною мережі, оскільки основна мета більшості сервісів – залишатися прихованими та бути доступними тільки «потрібним» відвідувачам. Орієнтуватися тут можна через:



• *пошукові сервіси* – Ahmia, Candle, Deep search, DuckDuckGo (пошуковик браузера Tor за замовчанням), Excavator, Fess, GDark, Google.onion, Grams, HayStack, Kraken, Not Evil (ранжує видачу), OnionLand Search, OnionSearch (GitHub, створює файл з видачею від різних пошуковиків .onion), Raklet, SearX (метапошук), Submarine, TorBot (GitHub, збирає адреси та назви сторінок з коротким описом), TORch (підтримує пошукові оператори та фільтри видачі), TorDex, VigilantOnion (GitHub, onion-краулер із підтримкою пошуку за ключовими словами) та ін. Кожен з них виводить різні результати за одним і тим самим запитом, тому краще задіювати декілька пошуковиків;

• *каталоги посилань* – Daniel, Dark Catalog, Deep Links Dump, Deep Link Onion Directory, Hidden Links, Hidden Reviews, Hidden Wiki, Oneirun, OnionDir, Onion link list, Onion Links, Runion Wiki, The Dark Web Pug, Годнотаба та її альтернатива darknet.wtf;

• *окремі ресурси* – Archive.today (вебархів), DarkNetLive (інформація про DarkNet та її використання), DarkVideo (аналог YouTube); Dark Lair, Facebook (соцмережа), Hidden Answers (форум); GreenAddress, Onion Wallet, Smartmixer (криптовалюта); Mailpile, Mail2Tor, ProtonMail, SecMail, Sigaint (електронна пошта); Sci-Hub (бібліотека наукових робіт), Just Another Library (література).

Доступ на деякі сайти, особливо форуми, може бути обмежений логіном та паролем, що отримується тільки за рекомендацією інших підписників, вхідного тестування або за гроші.

Завдяки технологіям шифрування трафіку та приховування IP-адреси DarkNet забезпечує високий рівень анонімності для відвідувачів. Однак це не означає, що його використання повністю безпечне. Існує низка *ризиків і загроз*, пов'язаних із цим – зараження ШПЗ, фішинг (заволодіння особистою інформацією, даними банківських карт/криптогаманців, паролями тощо), шахрайство, відстеження користувачів як з боку зловмисників, так і правоохоронців.

Для їх мінімізації слід неодмінно вживати комплексні заходи безпеки, задіюючи під час серфінгу та дослідження контенту окремі фізичні пристрої чи віртуальні машини, орієнтовані на конфіденційність ОС, платний VPN, фейкові особистості, ефективні антивірусні програми, а також власний здоровий глузд та обачність.

Перевіряйте репутацію вебсайту або форуму перед доступом до нього (наприклад, через r/darkweb чи r/TOR) та відвідуйте тільки ті посилання та ресурси, яким можете довіряти. Уникайте підозрілих або ненадійних посилань, що можуть привести до фішингових сайтів або завантаження ШПЗ. Не натискайте на спливаючі вікна, рекламу та будь-які підозрілі запити.

Намагайтесь працювати із завантаженими файлами лише після відповідного сканування, вимкнувши при цьому доступ до інтернету, і бажано в певному ізольованому програмному середовищі. Їх відкриття при наявному підключенні потенційно може призвести до витоку реальної IP-адреси, а також інших непередбачуваних наслідків.

Таким чином, DarkNet – це складна та неоднозначна частина інтернету, яка може бути використана як для законних, так і для протиправних цілей. Розуміння принципів її функціонування, а також методів пошуку та аналізу отриманої в ній інформації, дозволяє ефективно використовувати ці знання в різних сферах – від розслідування злочинів до захисту прав людини. Важливо завжди дотримуватись правил безпечного користування DarkNet та перевіряти достовірність отриманої інформації.

14. Корисні ресурси для розвитку навичок OSINT

Зрештою головне – не забувайте оновлювати свої інструменти та стежити за новинами в сфері OSINT, щоб завжди бути в курсі останніх тенденцій і методів пошуку, а також аналізу зібраних даних. У цьому Вам допоможуть:

• ***збірки інструментів/ресурсів*** – Advanced Search Tools, Analyst Research Tools, AsInt_Collection, Awesome OSINT, BBC Forensics Dashboard, Bellingcat's Online Investigation Toolkit, Commandergirl, CTI, Cyber Detective's website (або в соцмережі X/Twitter), DarkWeb, DeepWeb, Domainname-and-IP, EmailOsint, FBI-tools, Free OSINT and Online Research Resources, Free Osint Tools, IntelTechniques, MetaOSINT, NCSO, OSINT Essentials, OSINT Framework, osintframework.de, OSINTgeek Tools, OsintInception, OSINT Investigation Assistant, OSINT Research, OsintSmartFramework, OSINT Tool Comparison Table, OsintTools (від Molfar), OSINT tools (від Aware Online Academy), OSINT Web Resources, Osint4All, PhotoOsint, Search, SocialMedia, SPJ Toolbox (від Society of Professional Journalists), Technisette, The Hound, The Ultimate Osint Collection, Verification Toolset;

• ***спеціалізовані браузери/колекції закладок*** – Dark Web OSINT Bookmarks (для Tor), OSINT Bookmark Stack (для Chrome чи Firefox);

• ***програми для візуалізації дослідження*** – Obsidian (гайд українською), OSINTBuddy (GitHub, візуалізація та відшукання відправних точок для подальшого розслідування, безкоштовний аналог Maltego), TheBrain;

• ***практичні кейси/рекомендації*** – Bellingcat's Guide, Dating apps and hook-up sites, Global Investigative Journalism Network, Online Research Cheat Sheets, OSINT Handbook 2020, OSINT Techniques, Technisette Tutorials, The Atypical OSINT Guide;

• ***тренувальні вправи*** – OSINT CTF/Челенджи (каталог ресурсів для різнопланових квестів, CTF-ігор, тренінгів з веббезпеки та OSINT-розслідувань), OSINT Exercises with Sofia Santos;

• ***тематичні сайти та Telegram-канали*** – OSINT Team (підбірка ютуб-каналів, інформаційних матеріалів, блогів, підкастів, CTF-ігор, хакатонів тощо); HackYourMom, InformNapalm, Molfar про OSINT, OsintFlow, OSINT Бджоли.

Виробничо-практичне видання

Зоренко Дмитро Сергійович
Кульчицька Людмила Олександрівна
Лех Роман Вікторович
Червяков Олександр Іванович

ВИКОРИСТАННЯ ІНСТРУМЕНТІВ ТА МЕТОДІВ OSINT ДЛЯ ОТРИМАННЯ ПОШУКОВОЇ ІНФОРМАЦІЇ

Практичний порадник
5-те видання, перероблене та доповнене

ISBN 617-8130-64-0

Підписано до друку 26.11.24.
Формат 60×84 $^{1}/_{16}$. Папір офсетний.
Ум. друк. арк. 4,65. Гарнітура Times.
Наклад 50 прим.

Інститут Служби безпеки України
Національного юридичного університету імені Ярослава Мудрого
61002, м. Харків, вул. Мироносицька, 71,
телефон/факс: (057) 700-34-55, e-mail: ipuk@ssu.gov.ua

Видавець: Мірошниченко Олег Анатолійович
61002, м. Харків, вул. Дарвіна, 16, кв. 25.
Свідоцтво Державного комітету телебачення
і радіомовлення України
серія ДК № 5818 від 28.11.2017 р.
ел. пошта: merash@i.ua

Надруковано у друкарні ТОВ «Цифра Прінт».
Свідоцтво про Державну реєстрацію А01 № 432705 від 03.08.2009 р.
Адреса: 61166, м. Харків, вул. Данилевського, 30