МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Використання методології OSINT для отримання оперативно-значимої інформації

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

Одеса – 2024

УДК: 343.132:004.056.5(О75)(477)
В45

Погоджено на засіданні науково-дослідної лабораторії з актуальних питань кримінального аналізу навчально-наукового інституту підготовки фахівців кримінальної поліції Національної поліції України Одеського державного університету внутрішніх справ.
(Протокол № 11 від 13 листопада 2024 р.)

Схвалено та рекомендовано до друку
Вченою радою
Одеського державного університету внутрішніх справ.
(Протокол № 6 від 23 грудня 2024 р.)

Авторський колектив:

Д.С. Афонін кандидат юридичних наук, доцент, завідувач науково-дослідної лабораторії з актуальних питань кримінального аналізу Навчально-науковий інституту підготовки фахівців кримінальної поліції НПУ Одеського державного університету внутрішніх справ;

Д.В. Лісніченко кандидат юридичних наук, доцент, професор кафедри кримінального процесу та криміналістики факультету підготовки фахівців для органів досудового розслідування Одеського державного університету внутрішніх справ;

О.М. Заєць кандидат юридичних наук, доцент, член міжнародної асоціації аналітиків злочинності (*IACA – International Association of Crime Analysts*).

Рецензенти:

В.Г. Пядишев – доктор юридичних наук, професор, професор кафедри кримінального аналізу та інформаційних технологій Одеського державного університету внутрішніх справ;

В.Ю. Калугін кандидат юридичних наук, доцент, професор кафедри кримінального аналізу та інформаційних технологій Одеського державного університету внутрішніх справ.

В45 **Використання методології OSINT для отримання оперативно-значимої інформації** : методичні рекомендації / Д.С. Афонін, Д.В. Лісніченко, О.М. Заєць. — Одеса, ОДУВС, 2024. ⟆— 26 с.

Методичні рекомендації присвячені дослідженню методів і технік розвідки з відкритих джерел (OSINT), які дозволяють ефективно збирати, аналізувати та використовувати інформацію, що має значення для прийняття оперативних рішень. У фокусі розгляду – ключові принципи OSINT, сучасні інструменти для роботи з великими обсягами даних, а також методи їхньої верифікації та оцінки достовірності.

Особлива увага приділяється практичному застосуванню OSINT у правоохоронній діяльності. У матеріалі обговорюються етичні та правові аспекти використання відкритих даних, а також виклики, пов’язані з інформаційним хаосом та ризиком дезінформації.

Основною метою методичних рекомендацій є намагання сформувати практичні навички пошуку, структуризації та аналізу оперативно-значимої інформації з відкритих джерел, що сприятиме прийняттю обґрунтованих та ефективних рішень у динамічному інформаційному середовищі.

Зміст

1. Характеристика OSINT

OSINT (англ. open source intelligence) це процес отримання даних з джерел, які відкрито присутні в суспільстві. На відміну від більшості інших методів збору даних, під час цього процесу не використовується інформація, яка є прихованою а, отже, не вимагає такого ж рівня скритності в процесі (хоча деяка скритність іноді потрібна).

Деякі люди не звертають багато уваги на OSINT, однак це дуже корисно в забезпеченні отримання інформації, що надається з різних джерел, але це ще не все, у багатьох випадках OSINT в змозі забезпечити даними, які безпосередньо можуть бути використані, щоб зробити стратегічне рішення.

Багатьма, якщо не більшістю вважається, що це один з найпростіших і легких способів отримання інформації, але й тут є свої труднощі, одним з найбільших є те, що існує велика кількість даних. На відміну від інших форм та джерел пошуку даних OSINT має стільки даних, що фільтрація її, перетворення, надання форми є найбільш складною задачею.

OSINT використовується протягом тривалого часу урядами, військовими, а також в корпоративному світі, щоб тримати на виду конкурентів і мати конкурентну перевагу перед ними.

OSINT ВКЛЮЧАЄ В СЕБЕ пошук, вибір і збір достовірної інформації, отриманої із загальнодоступних джерел, і її аналіз і складання аналітичних рекомендацій, інформаційно-аналітичні звіти, ретроспективні огляди ЗМІ, моніторинги, рейтинги, індивідуальні тематичні підбірки і аналітичні записки з певних тем (подіям, особам, структурам); проведення конкурентної і бізнес розвідки в Інтернет; складання графічних схем візуалізації інформації.

СУТТЮ ВСЬОГО ПРОЦЕСУ OSINT є наявність сторони, для якої дослідження буде представляти реальну цінність, «аналіз», який є ключовим для проведення оцінки інформації, отриманої з відкритих джерел. Базова ідея OSINT - збір інформації для подальшого аналізу звітів про об'єкт. Аналіз може також привезти до випереджувальним аналізу поведінки і прогнозом, проте все залежить від цілей аналітика. У розвідувальному співтоваристві термін «відкритий» вказує на загальнодоступність джерела (на відміну від секретних джерел і джерел з обмеженим використанням).

АНАЛІТИЧНІ ФУНКЦІЇ OSINT

• контент-аналіз інформаційних матеріалів;

• перегляд результатів тематичної добірки в вигляді цитат (результати збору інформації в мережі Інтернет);

• статистичний аналіз джерел інформації щодо висвітлення подій, які цікавлять користувача.

ЕТАПИ OSINT

• постановка завдання - необхідно зрозуміти завдання, деконструювати аналітичну проблему.

• виконання планування - етап розробки плану збору інформації, що відповідає цій проблемі. Повинно бути прийнято рішення щодо того, що

повинно бути перевірено та проаналізовано. Повинно бути зроблене чітке формулювання цілей і завдань.

• пошукові роботи, для цього необхідно вибрати методи і засоби, які допоможуть ідентифікувати і отримати необхідну інформацію.

• аналіз і оцінка ключових джерел і їх змісту. Аналіз - це ключовий фактор, без якого неможливо інтерпретувати великі обсяги даних. Збір інформації повинен бути цілеспрямованим.

• складання звіту, який відповідає на конкретні питання, які необхідно було зрозуміти.

ДЖЕРЕЛА OSINT

• засоби масової інформації (ЗМІ) - газети, журнали, радіо, телебачення, телефонні довідники;

• офіційні дані про бюджети, демографії, матеріали прес-конференцій, різні публічні заяви, білі книги, технічні документи, керівництва та інструкції - все те, що можна почути, побачити, прочитати;

• спостереження - радіомоніторинг, використання загальнодоступних даних дистанційного зондування землі та аерофотозйомок;

• інформація з професійних або академічних джерел: професійні та академічні звіти, конференції, доповіді, статті, включаючи ту літературу, яка відноситься до «сірої»;

• комерційні дані - наприклад, щорічні звіти компаній; аналітичні роботи окремих експертів.

• дипломатичні місії;

• торгово-промислові палати - неурядові організації; релігійні організації; розвідувальні організації загальнонаціонального рівня;

• академічна сфера - програмне забезпечення, дисертації, лекції, презентації, науково-дослідні роботи, знання в друкованому та електронному вигляді по економіці, географії, міжнародних відносин, регіональної безпеки, науки і технологій;

• державні, міжурядові і неурядові організації - бази даних, оприлюднена інформація та друковані звіти, огляди широкого спектра в економіці, довкіллі, географії, гуманітарних науках, безпеки, науки і техніки;

• комерційні та громадські інформаційні служби, друковані новини поточних міжнародних, регіональних і локальних подій; архіви (бібліотеки) і дослідницькі центри - друковані документи і цифрові бази даних по ряду питань таких, як знання і навички інформаційного пошуку; індивідуальна і групова інформація - рукописна, мальована, опублікована, друкована або поширена інформація (наприклад, мистецтво, графіті, листівки, постери або веб-сайти);

• «сіра література» - наукові доповіді і записи, підготовлені в приватному секторі, урядових установах або академічних інститутах, які лише обмежено доступні, економічні та дослідницькі звіти, технічні інструкції, робоча документація, неофіційні урядові документи, дисертації (а також тези), препринти , маркетингові дослідження, інформаційні бюлетені, звіти про подорожі, дискусійні документи.

• Інтернет (соціальні мережі, чати, форуми і т.д.), зокрема веб-спільноти та контент, створений користувачами (en: user generated content) - соціальні сайти, відеохостінги, вікі-довідники, блоги, форуми; публічні урядові звіти. На ньому зупинимося детальніше.

Пошукові системи є одним з найбільш поширеніших і простих методів використання OSINT. Кожен день ми робимо сотні пошукових запитів в одному або декількох пошукових систем, в залежності від наших переваг і використовувати результати пошуку для певної мети. Хоча результати, які ми отримуємо, здаються простими, але є це відбувається на основі складних алгоритмів. Те, як ми створюємо наші запити, робить величезну різницю в точності результату, що ми насправді шукаємо за допомогою пошукової системи.

Хоча здається, що пошукові системи мають багато інформації, але вони тільки індексують дані, які вони можуть проаналізувати програмами, відомими як «павуки» або «роботи». Частину мережі, що ці павуки здатні охватити називається відкритою мережею, інша частина називається темною мережею або даркнет. Даркнет не індексується, оскільки відсутні безпосередні посилання.

Сайти новин. Раніше популярними оглядачами новин були газети, радіо і телебачення, але просування інтернет-технологій різко змінили ситуацію і сьогодні кожне велике видання має власний веб-сайт, де ми можемо отримати всі новини в цифровому форматі. Сьогодні існують навіть новинні агентства, які працюють тільки в Інтернеті. Це просування, безумовно, дало можливість отримувати новини кількома дотиками наших пальців в будь-який час, в будь-якому місці, де є підключення до мережі Інтернет.

Крім постачальників новин, є сайти, якими володіють окремі особи або групи, які зосереджуються на окремих темах, які належать до певних категорій. Ці сторінки в основному присутні у вигляді блогів, онлайн-груп, форумів, або чатів, це дуже корисно, коли нам потрібно думка маси щодо конкретної теми.

Корпоративні сайти. Кожна велика корпорація сьогодні запускає власний веб-сайт. Це не просто спосіб представити своє існування, але і спосіб безпосередньої взаємодії з клієнтами. Зазвичай корпоративний веб-сайт містить інформацію щодо ключових осіб в організації, електронну пошту, адресу, номери телефонів і т.д., які можуть бути використані для отримання додаткової інформації.

Сьогодні деякі з корпоративних веб-сайтів також надають інформацію у вигляді корпоративних блогів, інформаційних бюлетенів, що дуже корисно для розуміння не тільки поточного стану компанії, але і їх планів на майбутнє.

Сайти для обміну контентом. Існують різні типи користувацького контенту, а також різних мультимедійних файлів. За допомогою деяких сайтів можливо нам поширити певний тип контенту, такий як відео, фото, музика і т.д. Ці типи сайтів дуже корисні, коли потрібен конкретний тип медіа, що відноситься до необхідної теми, яку ми точно знаємо.

Академічні сайти зазвичай містять інформацію що деяких конкретних тем, науково-дослідні роботи, майбутні події, новини, пов'язані з конкретною

сферою, і т.д. У більшості випадків ця інформація може бути дуже важливою для розуміння сучасних наукових течій, а також подальший розвиток. Академічні сайти також корисні у вивченні тем, які пов'язані з нашою областю інтересів, а також для зрозуміння взаємозв'язку між ними.

Веблоги або блоги є особистим щоденниками у цифровому вигляді, крім того, вони є загальнодоступними. Зазвичай люди звикли писати блоги, як простий спосіб висловити свою думку з деяких тем, що становлять інтерес, але це змінилося в останнє десятиліття. Сьогодні є корпоративні блоги, які говорять про погляди компанії і можуть розповісти багато про свої заняття; є блог по конкретним темам, які можуть бути використані, щоб дізнатися про цю тему; є блоги, пов'язані з подіями і т.д.

Блог вказує не тільки тему написано, але і про його автора. У багатьох випадках блог може бути використаний, щоб зрозуміти психологічний портрет автора, навички спілкування і т.д.

Сайти державних органів та установ містять величезну кількість загальнодоступних даних. Це включає в себе не тільки інформацію про орган чи установу, а й про персонал, який там працює, структуру підрозділу. Є також сайти, де можна поскаржитися з приводу підвідомчих питань і перевірити на ньому статус розгляду і т.д. Це надійне джерело інформації для розуміння сфери його діяльності, планів на майбутнє і т.д.

Переваги відкритих джерел інформації для розвідки очевидні: вони оперативні, особливо зараз, коли будь-які події висвітлюються тележурналістами в режимі онлайн і чим швидше надходить інформація, тим менше можливостей її спотворити. Фахівець зможе зробити безпомилкові висновки, аналізуючи картинку прямого ефіру з гарячої точки.

Як ми вже говорили, в OSINT існують різні відкриті джерела, з яких можна зібрати дані, зокрема, які використовуються в Інтернет середовищі. Цей конкретний тип OSINT називається WEBINT, про що буде говоритися нижче.

2. Мета-пошукові системи

Всі ми знайомі з пошуковими системами і використовуємо їх для нашого повсякденного пошуку.

В основному пошукові системи, охоплюють мережу, використовуючи «пошукових роботів», які індексують веб-сторінки на основі широкого спектру з параметрів, таких як ключові слова, і на основі цієї індексації ми отримуємо наші результати відповідно до ключових слів, які ми зазначаємо.

Коли ми посилаємо запит на звичайну пошукову систему, то вона дивиться в свою власну базу даних для відповідних результатів і представляє їх, але що, якщо ми хочемо отримати більш конкретні результати, то ми звертаємося до мета-пошукових систем. Мета-пошукові системи є такими, що надсилають запит користувача до декількох джерел даних, таких як пошукові системи, бази даних і т.д. зводять агрегати результатів в єдиний інтерфейс. Це робить результати більш повним і актуальними, а також економить час пошуку, оскільки знаходить декількох джерел з одного питання . Мета-пошукові системи не створили базу даних самостійно, але покладатися на різні інші бази даних для збору результатів.

ez2www виробляє пошук по кращим пошуковикам - AlltheWeb, Google, AltaVista, Teoma, Wisenut - і тек - Yahoo! і Open Directory. За допомогою функції "Додатковий пошук" також здійснює пошук на невеликому сегменті невидимою (прихованої) мережі. Також шукає новини, мережеві конференції, MP3, зображення і багато чого іншого. Надає відмінні результати в дуже чіткому інтерфейсі.

Vivisimo використовує кластерну технологію, що припускає об'єднання результатів в папки. Можливі додаткові опції пошуку: фраза повністю, пошук по полю (домен, хост, ім'я, URL, і т.п.) і інші.

Query Server виробляє пошук по 11 пошукових системах - всі основні, крім Google. Але не варто хвилюватися: Query Server шукає в Yahoo !, Netscape і AOL, частково підтримуваних Google. Це ще один приклад кластерної технології – мета-пошуковий інструмент з відмінними можливостями налаштування. Можна змінювати вид сторінки результатів, вибираючи пошукові системи, кількість результатів, і т.п. Підтримує висновок фраз в лапки.

Infonetware виробляє пошук по WWW і надає релевантні результати, згруповані за темами, в дуже чистому інтерфейсі.

Metaseek відмінна пошукова система з України. Здійснює пошук в більшості міжнародних і місцевих пошукових системах. Крім документів, можна шукати картинки, MP3, FTP файли, новини і багато чого іншого. Можна використовувати "Фраза" (""), обробка на "рідній мові" і пошук по полю (по URL, імені, сайту / домену або лінку)

IBoogie "виконує розумну кластеризації результатів". Шукає в WWW, невидимій (прихованій) павутині, картинки, відео та аудіо файли.

Vinden.NL дає дуже хороші результати в чистому інтерфейсі.

Fazzle (колишній Search Online) використовує відмінну добірку пошукових систем і директорій. Надає релевантні результати в кілька переповненому інтерфейсі. По кожному результату можна бачити пошуковик, де була знайдена відповідь, і рейтинг.

Meta Bear надає релевантні результати як з міжнародних сайтів. Слідкуйте за тим, щоб запит був надрукований в рядку "Search The World".

Web Scout шукає документи, новини, конференції, аукціони, MP3 і роботу, використовує основні пошукові системи - крім Google - і надає релевантні результати в чіткому списку результатів.

argosa: de здійснює пошук в 17 міжнародних і місцевих пошукових системах, що надає відмінні результати, організовані за релевантністю, джерелу (quelle) або імені.

Experts Avenue одночасно шукає в різних пошукових системах веб-сторінки, аукціони, роботу і форуми; надає вельми релевантні результати в чіткому інтерфейсі. Пропонує онлайновий переклад веб-сторінок.

InfoGrid надає відмінні результати в зручному для читання форматі, шукає в Google, AlltheWeb, Yahoo! і каталозі Open Directory. Також шукає новини, аукціони, дискусійні форуми, MP3, FTP файли і багато іншого.

Suchspider.de виробляє пошук аж в 100 міжнародних пошукових системах. Результати можна сортувати за релевантністю, джерелу і - що набагато краще - групувати по імені домену.

EmailPinoy відсилає ваш запит на 15 пошукових систем. Для отримання більш точних результатів укладайте фрази в лапки.

1 SECOND здійснює пошук в хорошій збірці 14 основних пошукових системах, відкидає дублюючі варіанти і чітко узагальнює результати. Є можливість встановити свої параметри пошуку.

My Prowler шукає більш ніж в десяти пошукових системах, новини, зображення, аудіо / MP3, музичне відео, аукціони і різні інші сайти. Компілює результати, видаляє невідповідні варіанти і надає узагальнений звіт. Приймає запит на "рідній мові".

Gimenei рекомендується використовувати з опцією "Advanced Search". Можна налаштувати сторінку результатів, в тому числі опцію - "All Results" (всі результати) на одній сторінці. Всеохоплююча і швидка пошукова система.

Dug Dugi відправляє запит на основні пошукові системи, сортує результати, видаляє непотрібну інформацію і узагальнює результати в супер-чистому форматі. По кожному результату наводиться пошукова система і рейтинг сторінки.

Search 66 групує сторінки з одного і того ж домена, щоб уникнути таймаутів виберіть "Speed": "Comprehensive".

3. Анонімні пошукові системи

На відміну від Google, Yandex та інших, де всі ваші запити зберігаються, обробляються і аналізуються, анонімні пошукові системи не зберігають інтернет-активність.

Анонімна пошукова система Yacy - це децентралізована пошукова система. Працює вона за принципом пірінгових P2P мереж. Щось типу торрента.

У мережі YaCy кожен комп'ютер з встановленим спеціальним ПО є частиною пошукового робота - кравлера. Після кожного збору інформації робот відправляє дані в загальну базу, яку і використовують учасники пошукової системи YaCy.

Те, що у пошукової системи немає єдиного сервера і власника, робить результати пошуку незалежними від уподобань посередників. Всі результати пошукової видачі позбавлені будь-якої цензури.

Його також можна використовувати для організації пошукової системи в корпоративних мережах. Ну і не менш важливим фактором є можливість шукати в DeepWeb.

Основні можливості Yacy: децентралізована пошукова система

На даний момент самим серйозним недоліком Yacy є швидкість роботи.

Анонімна пошукова система DuckDuckGo вважається самим анонімним і є найпопулярнішою пошуковою системою серед усіх подібних.

Головним достоїнством пошукача, поряд з високим рівнем анонімності і безпеки, є релевантність пошукової видачі. Знаходить він інформацію добре, не ідеально як Yandex і Google, але добре. Крім цього із значущих плюсів відзначу швидкість роботи.

Також як Google, пошук DuckDuckGo живе за рахунок реклами, але на відміну від першого працює за іншим принципом. Під час формування та показу рекламних блоків він враховує не історію пошукових запитів, а тільки використовувані користувачем ключові слова.

Крім свого основного пошукового індексу DuckDuckGo черпає інформацію у своїх великих братів: Yahoo, Google і Bing.

Пошукова система в роботі між клієнтом і сервером за замовчуванням використовує протокол HTTPS з алгоритмом шифрування AES і ключем довжиною 128 біт.

В цілому пошуковик працює дуже гідно, має купу налаштувань допомагають в роботі, ну і в плані анонімності і безпеки все дуже навіть непогано.

Анонімна пошукова система eTools.ch - це ще один онлайн-сервіс позиціонує себе як анонімний. Він не має свого власного індексу і алгоритмів ранжирування, результати пошуку беруться з інших сервісів: Ask, Bing, DuckDuckGo, Yandex, Yahoo, Wikipedia, Google і т.д.

eTools.ch в роботі між клієнтом і сервером за замовчуванням використовує протокол HTTPS. eTools.ch зберігає постійно і відстежує Cookies сторонніх осіб.

4. Пошук інформації про людей в мережі Інтернет

Часто виникає необхідність знайти людину, знаючи про неї вкрай небагато. Іноді це тільки прізвище та ім'я, іноді телефон, а іноді і просто фотографія. Є багато популярних соціальних мереж як Facebook (facebook.com), LinkedIn (linkedin.com) і т.д., де ми можемо багато чого довідатися про людей, але крім цього є багато платформ, де можливо шукати людей в Інтернеті і знайти відповідну інформацію. Інформація, яку ми очікуємо від такого роду пошуку це повне ім'я, адреса електронної пошти, номер телефону, адреса і т.д.; це вся інформація може бути використана для отримання додаткової інформації. Цей вид інформації дуже актуальний, коли, наприклад, необхідна інформація про людину, яка є потенційним чи реальним правопорушником.

http://m.where-you.com/ - пошуковик по людям, в ВКонтакте, Одноклассниках і т.п.

http://www.zillman.us/subject-tracers - найбільш повна колекція ресурсів з пошуку людей від М.Зілмана.

https://www.imageraider.com/ - пошуковик по фотографіях.

http://thatsthem.com/ - якісний пошуковик людей за такими параметрами, як email, домашня адреса, телефон, IP адреса, адреса кореневого сервера, використання сервісу анонімізації і т.п. Найкраще налаштований на Північну Америку, але дає адекватні результати і по інших регіонах.

http://reputometer.ru/ - сервіс відстежує видимість негативних матеріалів, дозволяє цілеспрямовано боротися з негативними відгуками в мережі. Відстежує появу нових матеріалів.

http://www.beenverified.com/ - новий, високо оцінений фахівцями пошуковик людей.

http://www.privacyrights.org/online-information-brokers-list - колекція в інтернеті пошукових систем і сервісів з пошуку людей, а також даних, пов'язаних з їх визначенням та наявністю правопорушень. В основному орієнтована на Північну Америку і Європу.

http://people.yandex.ru/ - сервіс пошуку профілів у всіх основних соціальних мережах. Для пошуку необов'язково знати, чи зареєстрований людина в будь-якої з мереж. Досить просто ввести його ім'я, прізвище і т.п. Сервіс використовує тільки загальнодоступну інформацію - закриті від індексації профілі не потрапляють в пошукову видачу.

http://www.pipl.com/ - кращий пошуковик людей в інтернеті.

TinEye - унікальна пошукова машина, яка виробляє пошук по фотографіях і зображеннях. Для пошуку завантажується шуканий образ і система видає всі виявлені результати. Неоціненний інструмент конкурентного розвідника.

http://fotki.yandex.ru/ - Яндекс запустив технологію face.com для визначення осіб на знімках. До цього, цю технологію використав тільки Facebook. Тепер сервіс не тільки дозволяє вказати знайомих на знімках, але і вміє знаходити на фотографії особи і розпізнавати людей, зіставляючи з фотобанком.

http://www.spokeo.com/ - відмінний пошуковик людей по сайтам, соціальним мережам, адресами, e-mail і багато чому іншому. Підтримує і російську мову.

http://www.peekyou.com/ - новий пошуковик людей по імені, прізвища, інтересам, роботі, школам, багато чому іншому. Локація - США, Великобританія, Ірландія, Австралія, Канада, Нова Зеландія, і, увага, Китай і Індія.

https://infotracer.com/ - сканує по запиту соціальні медіа, перевірить всі бази щодо правопорушень, з'ясує родичів і партнерів того, кого ви шукаєте, і додатково повідомить деталі про сімейний стан. Підтримує стовідсоткову конфіденційність.

http://www.picslikethat.com/ - німецький візуальний пошуковик частково з російськими розробниками. Пошуковик відрізняється від інших тим, що одночасно використовує алгоритм розпізнавання образів та кластерний пошук.

http://www.googleimageslideshow.com/ - служба Google дозволяє легко здійснювати пошук фотографій і інших типів зображень, представляючи у вигляді слайд-шоу. Якщо ви хочете більш докладно розглянути або зберегти зображення, то на нього потрібно просто клікнути мишкою передбачена також функція збільшення-зменшення та фрагментація зображень. Здорово працює з картами Google.

http://www.facesaerch.com/ - пошуковик фотографій по ПІБ, заснований на інструментах Google. Підтримує російську мову.

http://www.truecaller.com - допомагає ідентифікувати людину за номером телефону, вона також може бути використана через веб-браузер. TrueCaller просто дозволяє здійснювати пошук, використовуючи номер телефону, і надає детальну інформацію користувача

5. Сервіси автоматичного пошуку email

VoilaNorbert - досить відомий за кордоном сервіс пошуку email. Просто зайдіть на сайт, введіть ім'я та прізвище людини, чий email ви шукаєте, транслитом і натисніть кнопку Work for me, Norbert.

Email Hunter - сервіс пошуку email на сайті. Представлений як у вигляді веб-версії, так і розширення для Chrome. Просто введіть доменне ім'я сайту компанії, в якій працює людина, чию електронну адресу ви шукаєте, і Email Hunter просканує сайт на наявність контактної інформації, а також покаже джерела знайдених адрес в разі вдалого пошуку:

FindAnyEmail перевіряє прив'язку соціальних акаунтів до адрес. Щоб скористатися сервісів, зайдіть на сайт FindAnyEmail, введіть ім'я та прізвище людини, сайт компанії, в якій він працює і натисніть синю кнопку Find email

AnyMailFinder схожий по функціональності з FindAnyEmail, але з деякими відмінностями. Перше - безкоштовна версія надає можливість робити цілих 20 запитів в день (враховуються тільки вдалі запити). Друге - немає відображення прив'язаного аккаунта в разі вдалого пошуку, тобто доведеться повністю довіритися сервісу, або перевірити знайдений адресу за допомогою сторонніх сервісів. Щоб скористатися AnyMailFinder, зайдіть на сайт додатки, введіть ім'я та прізвище людини, адреса сайту компанії (виду site.ru) і натисніть кнопку Search.

Email Extractor - програма, призначена для пошуку email. Є безкоштовна і платна версії. Єдина відмінність між ними - в безкоштовній версії не можна зберігати знайдені дані. Щоб скористатися Email Extractor, зайдіть на сайт, скачайте і встановіть програму.

Datanyze - платний сервіс, який виконує безліч функцій, одна з яких - пошук і перевірка email. У безкоштовної версії є всього 10 запитів. Враховуються тільки ті запити, після яких сервіс успішно знайшов працює email. Введіть домен сайту компанії, в якій працює людина, в пошукове поле у лівому верхньому кутку, і Datanyze збере всю доступну йому інформацію про компанії. Виберіть вкладку People, щоб відкрити список працівників компанії.

Conspire - зарубіжний сервіс, в основі якого лежить теорія шести рукостискань. Він не допоможе знайти email, але зате з його допомогою можна знайти того, через кого ви зможете знати того кого безпосередньо шукаєте.

Принцип дії сервісу простий - ви входите, дозволяєте Conspire доступ до всіх своїх робочих email, і він аналізує ваші контакти і частоту листування з ними. Після того, як ви завершите реєстрацію, можна приступати до пошуку потрібної людини. Просто введіть його ім'я та прізвище в пошукове поле на головній сторінці Conspire, і сервіс видасть вам список збігів.

6. Сервіси перевірки email на достовірність

Rapportive - популярне розширення для браузера, яке показує, чи пов'язаний email з будь-яким аккаунтом LinkedIn. Працює тільки в інтерфейсі Gmail. Встановіть розширення, зайдіть в Gmail і введіть в поле «одержувачі» передбачуваний адресу. Якщо в правій частині екрана з'явиться вікно з ім'ям і прізвищем людини, а також посиланням на його профіль в LinkedIn, то ви знайшли потрібний email.

MailTester виконує всього лише одну просту, але корисну функцію - перевіряє введений email на працездатність. Просто введіть потрібну адресу в поле на головній сторінці сайту MailTester і натисніть на кнопку Check address.

EmailSherlock - сервіс, який визначає працездатність email, а також його прив'язку до акаунтів в соціальних мережах. Зайдіть на сайт EmailSherlock, введіть потрібну адресу в пошукове поле на головній сторінці та натисніть на кнопку Go. Пошук займе якийсь час, після чого вам будуть показані результати.

Vibe - безкоштовне розширення для Chrome, що дозволяє знайти інформацію про людину, маючи на руках email. Ви можете використовувати Vibe для того, щоб перевіряти, чи є знайдена адреса робочою. Після встановлення розширення, просто наведіть курсор на email, або виділіть його, а потім натисніть на кнопку, що з'явилася з логотипом Vibe. Справа відкриється вікно, в якому буде представлена вся знайдена інформація.

7. Пошук інформації в соціальних мережах

Соціальні мережі є великою платформою і її вплив також , будь то на особистому рівні або корпоративному рівні. Існують пошукові системи, які отримують інформацію з соціальних мереж.

SocialMention непоганий сервіс для самостійного моніторингу соціальних мереж (компанія, бренд, персона, новий продукт, рекламна акція та ін.).

Користуватися сервісом дуже просто: треба вибрати типи джерел, за якими буде здійснюватися пошук (блоги, мікроблоги, коментарі, аудіо, відео та ін.), Скласти пошуковий запит і насолоджуватися результатами :).

Сервіс "в режимі реального часу" моніторить близько 100 джерел (включаючи Twitter, ЖЖ, Facebook, FriendFeed, YouTube, Digg, Google та ін.).

Наприклад, якщо треба подивитися, що пишуть в блогах і соціальних мережах про "marketing research", то в результаті вийде сторінка, на якій є останні пости про маркетингові дослідження, топи ключових слів, джерел і користувачів, які пишуть про дослідження найчастіше .

Також є простий модуль аналізу, який показує "силу" (strength), ставлення (sentiment), прихильність (passion) і охоплення (reach) по потрібному запиту.

"Сила" того чи іншого ключового слова або фрази - показник інтенсивності обговорення аналізованого слова. Розрахунок тут досить простий: кількість згадок слова або фрази за останні 24 години ділиться на загальну кількість знайдених згадок за весь час.

"Відношення" - співвідношення негативних і позитивних згадувань.

"Прихильність" - показник повторних згадок аналізованого слова або фрази. Так, якщо у бренду є кілька лояльних споживачів-блогерів, які постійно про нього пишуть, то показник прихильності буде вище, а якщо споживачів-блогерів багато, але пишуть вони про бренд порівняно рідко, то показник прихильності буде нижче.

"Охоплення" - кількість унікальних авторів, які згадують аналізоване слово, ділиться на загальну кількість згадок.

Щоб вести моніторинг на постійній основі, можна підписатися на RSS потрібного запиту або на щоденні оновлення по електронній пошті.

SOCIAL-SEARCHER це ще один пошукова система. Вона використовує Facebook, Twitter і Google+ як його джерела. Інтерфейс, що надається цією пошуковою системою простий. На вкладці пошуку, результати пошуку будуть розподілені на три вкладки на основі джерела, в цих вкладках перераховані пости з попереднім переглядом, що дуже корисно для виявлення тих, які мають значення для нас.

На вкладці аналітики ми можемо отримати аналіз налаштувань, користувачів, ключові слова, домени і багато іншого. Одним з цікавих з них є закладка популярного, в якій перераховані результати з більшої взаємодії.

Topsy - це інструмент, який дозволяє шукати і відслідковувати Twitter. З його допомогою ми можемо перевірити тенденцію будь-якого ключового слова в Twitter і аналізувати свої досягнення. Інтерфейс досить простий і виглядає як

звичайна пошукоа система, тільки результати на основі Twitter. Результати, подані ним можуть бути звужені до різних часових рамок, таких як 1 день, 30 днів, і т.д. Ми також можемо відфільтрувати результати: тільки побачити фотографії, твіти, посилання, відео. Існує ще один фільтр, який дозволяє нам бачити тільки результати, що містять результати конкретних мов. В цілому Topsy є відмінним інструментом для моніторингу ринку для конкретних ключових слів.

Trendsmap є прекрасною візуальної платформою, яка показує популярні теми у вигляді ключових слів, хештегів з платформи Twitter. Це відмінна платформа, яка використовує візуальне уявлення тенденцій, щоб зрозуміти, що жарко обговорюється в певному регіоні світу. Крім показу візуальної форми інформації, також дозволяє вести пошук по інформації у вигляді теми або місць, що робить його легшим для нас, щоб бачити тільки те, що ми хочемо.

Tweetbeep - це відмінний сервіс, який дозволяє стежити за тим, що цікавить в Twitter, наприклад, бренди, продукти або оновлення, пов'язані з компаніями та навіть посилання на них. З метою моніторингу ринку це відмінний інструмент, який може допомогти нам швидко реагувати на теми, що представляють інтерес.

Twiangulate це відмінний інструмент, який дозволяє нам виконувати Twitter тріангуляції. З його допомогою можна дізнатися про людей, за чим вони слідкують і на яких користувачів Twitter підписані. Також надає можливість порівняти охоплення двох користувачів. Це відмінний інструмент, щоб зрозуміти і порівняти користувачів Twitter.

8. Пошук даних про мережі, веб-сайти та ін.

Whois - мережевий протокол, який базується на протоколі TCP. Його основне призначення - отримання в текстовому вигляді реєстраційних даних про власників IP адрес і доменних імен (головним чином, їх контактної інформації). Запис про домен зазвичай містить ім'я та контактну інформацію «регистранта» (власника домену) і «реєстратора» (організації, яка домен зареєструвала), імена DNS серверів, дату реєстрації та дату закінчення терміну її дії. Записи про IP адреси згруповані за діапазонами (наприклад, 8.8.8.0 - 8.8.8.255) і містять дані про організацію, якій цей діапазон делегований.

Robtex це відмінний інструмент, щоб дізнатися інформацію про інтернет ресурси такі як IP-адреса, ім'я домену, номер автономної системи (AS), і т.д. Інтерфейс досить простий і зрозумілий. У лівому верхньому кутку знаходиться панель пошуку за допомогою якої ми можемо здійснити пошук інформації. Пошук домена дає нам відповідну інформацію, наприклад, IP-адресу, маршрут, AS номер, місце розташування і т.д. Так само надається інша інформація щодо IP-адрес, маршрутизації і т.д.

W3dt є великий онлайн ресурс, щоб дізнатися мережеву інформацію. Існують різні розділи, які можна досліджувати за допомогою цієї єдиної платформи. Перший розділ – системи доменних імен (DNS), інструмент, що дозволяє виконувати різні DNS-запити, такі як DNS пошук, зворотний пошук DNS, сервер DNS і т.д. Другий розділ містить інструменти, пов'язані з мережею/інтернетом, такі як сканування портів, мічених Oute, запис MX ретривера і т.д. наступний розділ веб/HTTP, який складається з таких інструментів, як інформація сертифіката SSL, URL кодування/декодування, пошук в назвах HTTP і т.д., потім йде розділ пошуку в базі даних відповідно до якого можна знайти пошук MAC-адреси, пошук Whois, і т.д., в кінці кінців, є деякі загальні і пов'язані з пінгуванням інструменти.

Shodan є пошуковою системою комп'ютера, який сканує Інтернет, опитує порти пристроїв і на основі отриманих у відповідь банерів робить висновки про пристрої і сервіси. Це дозволяє нам шукати цю інформацію за допомогою IP-адреси і багато іншого. З його допомогою можна дізнатися інформацію, який певний тип веб-серверів, такі як Internet Information Services (IIS) або Apache використовують веб-сайти, а також інформацію, яка може бути досить цікава, наприклад доступ до IP камери без перевірки автентичності або SCADA системи через Інтернет.

Internet Archive Wayback Machine є великим ресурсом для пошуку як веб-сайт виглядав в минулому. Просто введіть адресу веб-сайту в рядку пошуку, і у відповідь з’явиться графік з наявними знімками веб-сайту виділеної у календарі. Просто над цими датами виділеними у календарі будуть посилання на знімок. Це відмінний інструмент для аналізу того, як веб-сайт розвивається і, таким чином, можна контролювати його зростання в минулому. Ресурс також може бути корисним для отримання інформації з веб-сайту, який був доступний в минулому, але не в даний час.

9. Реверсивний пошук зображення

Ми всі знайомі з фразою «зображення варто тисячі слів» і більшість також знають що платформи, такі як Google Images (http://images.google.com), Flickr (https://www.flickr.com/), Deviantart (http://www.deviantart.com/) дають нам можливість пошуку зображення за ключовими словами. Зазвичай, коли нам потрібен пошук певної інформації, у нас є ключове слово або набір з них у вигляді тексту, дотримуючись їх ведеться пошук пошуковими системи, але ми маємо справу з текстом у якості вихідних даних і так отримуємо результати, але в випадках коли у нас є зображення, і ми хочемо побачити, де воно є ще в Інтернеті, куди ми йдемо? Тут використовуються пошуковики зворотного пошуку зображення, які приймають зображення в якості вхідних даних і шукають веб-ресурси зі схожими на зовнішній вигляд зображеннями.

Google Images дозволяє виконати зворотний пошук зображення. Нам просто потрібно, щоб перейти до http://images.google.com і натисніть на значок камери і надати URL зображення в Інтернеті або завантажити файл локально збережених зображень, можна також перетягнути файл зображення в рядку пошуку і вуаля Google переходить за посиланнями на сторінки, що містять ту або схожі зображення в Інтернеті.

TinEye ще один зворотний пошуковик зображення і має величезну базу даних зображень. Подібно Google Images, пошук в TinEye дуже простий, ми можемо надати URL до зображення, завантажити його, або виконати перетягування. TinEye також є у вигляді плагіна для основних браузерів, що робить задачу набагато простіше.

ImageRaider відображає результати по доменам. Якщо домен містить більше однієї копії зображення, то це також вказується, і посилання на ці зображення, перераховані під доменним ім'ям.

Зворотний пошук зображення дуже корисним, щоб дізнатися більше про когось. Багато людей використовують одну і ту ж фотографію чи зображення для опублікування на різних платформах, через що зворотний пошук зображення може привести нас до інших платформ, де можна отримати інформацію щодо профілю та іншої раніше невідкритої інформації.

10. Розширений веб-пошук GOOGLE

GOOGLE є одним з найбільш широко використовуваних пошукових систем, і є відправною точкою для веб-розвідки для більшості з нас. Спочатку пошук Google був доступний через дуже простий інтерфейс і за умови обмеженої інформації. Крім вікна пошуку були деякі спеціальні пошукові посилання, посилання на компанію, а також поле підписки, де ми могли б ввести нашу електронну пошту, щоб отримати оновлення. Там не було ніяких оголошень, ніяких різних варіантів мови, логіна і т.п.

За ці роки змінився не тільки зовнішній вигляд і інтерфейс, але і функціональні можливості. Google еволюціонував від надання простих веб-посилань на сторінки, що містять відповідну інформацію до цілої купи відповідних інструментів, які не тільки дозволяють нам шукати різні типи носіїв і категорії, а й звузити ці результати за допомогою різних фільтрів.

Сьогодні існують різні категорії результатів пошуку, такі як зображення, новини, карти, відео і багато іншого. Безліч функціональних можливостей, що надається Google сьогодні, безумовно, зробили наше життя набагато простіше і зробили пошук інформації в Інтернеті буденним явищем. Проте, іноді ми стикаємося з труднощами в пошуку точної інформації, яку ми шукаємо, і основною причиною є не відсутність інформації, а, навпаки, велика її кількість.

Майстерне володіння пошуком GOOGLE - це інструмент, який корисний і звичайним користувачам, що бажають використовувати можливості цієї пошукової системи для точного отримання того, що вони шукають; і для тих, хто займається розслідуваннями на основі відкритих джерел;

Ми розглянемо синтаксис пошукових запитів Google, які можуть виявитися корисними для всіх, що б ви не шукали. Більшість операторів можна використовувати в одному запиті в комбінації з іншими. Можна найрізноманітнішим чином групувати елементи запиту і за допомогою дужок і логічних операторів створювати дуже точні запити, які дозволяють, з одного боку, знайти необхідні сторінки, і при цьому виключити зайві дані.

Використовуючи оператори можна відфільтрувати документи з певним вмістом за певними словами в заголовку або тексті, знайти неохідну інформацію, наприклад, конфігураційні файли і документи з паролями.

Просунуті оператори є частиною стандартного запиту Google. Вони мають такий синтаксис.

Коли нам потрібно шукати щось в Google, ми просто вводимо деякі з ключових слів, пов'язаних з цим явищем, в рядок пошуку і натискаємо Enter. На основі індексації, Google просто надає нам інформацію з відповідних ресурсів.

Якщо ми хочемо отримати кращі результати або фільтрувати існуючі результати, засновані на різних факторах, ми повинні використовувати Google оператори розширеного пошуку. Виділяють наступні оператори.

site: - це просунута команда, яка дозволяє вам вказати певний домен, по якому потрібно виконати пошук.

"Site:" можна використовувати з кореневим доменом і субдоменами. Оператор "site:" можна комбінувати з іншими операторами і ключовими словами. Приклад: site:house.gov

inurl: дозволяє шукати за ключовими словами в адресі сайту. Корисно коли необхідно дізнатися конкретні сторінки, які слідують спільне ключове слово в назві. Приклад: inurl:hack

allinurl: подібно «Inurl» цей оператор дозволяє шукати за декількома ключовими словами в адресі сайту. Таким чином, ми можемо знайти кілька ключових слів в адресі. Це також збільшує шанси на отримання якісного контенту, що ми шукаємо. Приклад: allinurl:hack security

intext: гарантує, що необхідне ключове слово буде вказано в тексті сторінки. Ми можемо використовувати цей параметр запиту, щоб отримати відповідний зміст зі сторінки за ключовим словом, яке ми шукаємо. Приклад: intext:hack

allintext: подібно «intext» цей оператор дозволяє пошук кількох ключових слів в тексті. Функція пошуку для кількох ключових слів завжди підвищує якість контенту на сторінці результатів. Приклад: allintext:data marketing.

intitle: дозволяє обмежити результати за ключовим словом, присутнім в заголовку сторінки. Цей параметр запиту завжди допомагає шукати за ключовим словом. Приклад: intitle:blueocean

allintitle: це оператор аналог «intitle», тільки дозволяє пошук кількох слів в назві. Приклад: allintitle:blueocean market

fietype: використовується для пошуку файлів певного типу. Він підтримує кілька типів файлів, такі як PDF, SWF, KML, DOC, SVG, TXT і т.д. Це зручний оператор, коли ми шукаємо тільки файли певного типу на певному домені. Приклад: fietype:pdf, site:xyz.com, fietype:doc

ext: виступає за розширення файлу і працює аналогічно оператору fietype:. Приклад: ext:pdf

defie: використовується, щоб з'ясувати сенс ключового слова. Google надає словникове значення і синоніми для ключового слова. Приклад: define:data

AROUND корисний, коли ми шукаємо результати, які містять два різних ключових слова, але вони в тісному зв'язку. Це дозволяє обмежити кількість слів між двома різними ключовими словами в результатах пошуку. Приклад: A AROUND(6) Z

AND використання двох і більше слів виведе результати, в яких використовуються всі слова. Тобто між словами мається на увазі логічне «І». Тому точно такий же результат можна отримати ввівши «AND». При цьому необов'язково шукається за точним збігом фрази - в результатах пошуку можуть бути слова в іншому відмінку, числі, синоніми. Приклад: Дані and ринок

OR якщо вам потрібно логічне АБО - тобто пошук одного або іншого, використовуйте оператор "OR".Приклад: дані OR розвідка

NOT виключає з результатів пошуку необхідне ключове слово. Приклад: лотос NOT квітка

«» корисний, коли потрібно шукати результати, які містять ключове слово в точній відповідності. Наприклад, ми можемо знайти сторінки, які містять лапки або кілька текстів. Приклад: «час - гроші»

- виключає з результатів пошуку необхідне ключове слово (без пробілу). Приклад: лотос -квітка

***** використовуються в якості родового заповнювача для невідомого терміна. Ми можемо використовувати це, ми частково знаємо необхідне слово, перевіряємо варіанти. Приклад: «* дорогоцінна»

.. використовується для забезпечення діапазону номерів. Це дуже корисно для забезпечення цінового діапазону, діапазон часу (дати) і т.д. Приклад: Японія вулкан 1990..2000

info: надає інформацію, що Google має на певному домені. Посилання на різні типи інформації присутні в результатах, такі як кеш, подібні веб-сайти і т.д. Приклад: info:elsevier.com

related: використовується для пошуку інших веб-сторінок, подібних в одній області. Це дуже корисно, коли ми шукаємо веб-сайти, які надають подібні послуги. Приклад: related:elsevier.com

cache: перенаправляє до останньої кеш сторінки, яку Google сканував. У разі, якщо ми не отримаємо результат для веб-сайту, який був доступний раніше, це хороший варіант, щоб спробувати. Приклад: cache:elsevier.com

Розширений пошук Google можна виконати за допомогою сторінки http://www.google.com/advanced_search, що дозволяє нам виконувати обмежений пошук без використання операторів, згаданих вище.

Крім операторів Google також пропонують деякі операції, які дозволяють нам перевірити інформацію про поточні події, а також виконувати деякі інші корисні речі. Ось деякі приклади:

Просто ввівши ***time(час)*** відображається поточний час в залежності від нашого розташування. Ми можемо також використовувати назву регіону, щоб отримати його поточний час. Приклад: time(час) Франція

weather(погода) показує поточний стан погоди місця нашого знаходження. Подібно ключовому слову «час» ми можемо використовувати його, щоб отримати погодні умови в різних регіонах. Приклад: weather(погода) Швеція

Google також вирішує математичні рівняння, надаючи **калькулятор.** Приклад: 39*(9823-312)+44/3

Google може бути використаний для виконання **переведення для різних типів одиниць вимірювання**, таких як валюти, час і т.д. Приклад: 6 футів в метрах

Це не все, іноді Google також показує відповідну інформацію, пов'язану з глобальними подіями, як і коли вони відбуваються. Наприклад, Чемпіонат світу з футболу.

Крім пошуку в Інтернеті, в загальному, Google також дозволяє шукати певні категорії, такі як зображення, новини, відео і т.д.

Вищезазначені оператори, безумовно, дуже корисні для тих, хто потребує дізнатися якусь інформацію в Інтернеті, але спільнота InfoSec взяв його на наступний рівень. Ці прості і невинні оператори широко використовуються в

індустрії кібербезпеки і продемонстрували, як інформація без шкоди ресурсу може бути з нього вилучена. Цей метод з використання операторів пошукової системи Google називають «Google Hacking.»

Справа в тому, що сотні тисяч сайтів мають відомі уразливості. Не потрібно нічого вигадувати, досить вводити необхідні запити, які будуть відображати існуючі уразливості на конкретних сайтах. Так, серед видачі є дуже багато нерелевантної інформації, але якщо добре пошукати, то можна знайти та отримати доступи до сайтів і БД, доступи до сервісів і т.д

Google Hacking Database, створений Джонні Лонг можна знайти на http://www.hackersforcharity.org/ghdb/хоча він не оновлюється, але це відмінне місце, щоб зрозуміти і дізнатися, як ми можемо використовувати Google, щоб дізнатися конфіденційну інформацію. Регулярно оновлювану версію можна знайти на сайті http://www.exploit-db.com/google-dorks/.

СПИСОК ЛІТЕРАТУРИ

1. Buryk Z., Orliv M., Ismailov K. Trends and Determinants of Lifelong Learning: Regional Differences in Europe. *International Journal of Advanced Biotechnology and Research*. 2019. Special Issue-1. P. 572-579.
2. Open Source Intelligence (OSINT): Issues for Congress. - [Електронний ресурс]. - Режим доступу: https ://www.fas.org/sgp/crs/intel/RL34270.pdf
3. Балтовський О.А., Белека І.А., Ісмайлов К.Ю. Методика аналізу схем цифро-аналогових перетворювачів з використанням матриць гібридного типу. *Вісник Інженерної академії України Кіровоградського національного технічного університету*. 2019. № 3. С. 79-85.
4. Бутко Р. Ю. Розвиток системи кримінального аналізу в діяльності Національної поліції України. Теорія та практика протидії злочинності у сучасних умовах : збірник тез Міжнародної науково-практичної конференції (3 листопада 2023 року) / упор.Р. М. Шехавцов. Львів : Львівський державний університет внутрішніх справ, 2023. 224 с.
5. Варенко В. Методичний аспект створення інформаційно-аналітичних документів: аналіз, технології, проблеми. https://dspace.nau.edu.ua/bitstream/NAU/24833/1/Стаття.pdf
6. Инструменты и сервисы для OSINT http://uplink.motd.org/2017/04/osint-tools-and-service/
7. Інструкція З формування та ведення бази даних «Розшук» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» Наказ Міністерства внутрішніх справ України від 28 червня 2023 року № 534
8. Інструменти для аналізу даних). UPL: https://library.sumdu.edu.ua/uk/doslidnyku/prohramne-zabezpechennia/analiz-danykh-ta-vizualizatsiia/instrumenty-dlia-analizu-danykh
9. Інформаційні технології: підруч. / В.Б. Вишня, К.Ю. Ісмайлов, І.В. Краснобрижий, С.О. Прокопов, Е.В. Рижков. Дніпро: ДДУВС, 2021. 492 с.
10. Ісмайлов К.Ю. Бедрій Т.А., Медведенко С.В. Використання знань про особливості криптовалют у протидії злочинності. *Кібербезпека в Україні: правові та організаційні питання*: матеріали Всеукраїнської науково-практичної конференції, 30 листопада 2018 р. Одеса: Одеський державний університет внутрішніх справ. 2018, С. 140-149.
11. Ісмайлов К.Ю., Бєлих Д.В. Інформаційний суверенітет та доктрина інформаційної безпеки України. *Електронне наукове видання «Порівняльно-аналітичне право»*. 2019. № 1. С. 206-209.
12. Ісмайлов К.Ю., Сіфоров О.І., Лефтеров Л.В. Основні прийоми пошуку та аналізу інформації на підставі відкритих джерел. *Міжнародна та національна безпека: теоретичні та прикладні аспекти:* матер. III Міжнар. наук.-практ. конф., 15 бер. 2019 р. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2019. С. 258-261.
13. Кіреєва О.С., Крутік Ю.В., Махлай О.М., Треус А.С. Основи кримінального аналізу: теорія та практика застосування в оперативних

підрозділах Державної прикордонної служби України: навчальний посібник. Хмельницький: Вид-во НАДПСУ, 2022. 388 с.

14. Кожушко О.О. Розвідка відкритих джерел інформації (OSINT) у розвідувальній практиці США [Електронний ресурс].- Режим доступу: http://jml.nau.edu.ua/index.php/IMV/artide/viewFile/3264/3217

15. Комплекс методичних рекомендацій з протидії діяльності нарколабораторій / С.В. Албул, О.А. Гритенко, К.Ю. Ісмайлов, О.М., Заєць, В.Б. Любчик, Д.М. Ноздрин. Одеса: Одеський державний університет внутрішніх справ, 2018. 175 с.

16. Користін О., Кирилюк О. Основи аналітичної розвідки в системі державної безпеки: навчальний посібник. Київ: НА СБ України, 2023. 144 с.

17. Користін О.Є., Бабенко А.М., Заєць О.М., Ісмайлов К.Ю., Некрасов В.А., Пефтієв Д.О. Основи кримінального аналізу: підручник; за заг. ред. Користіна О.Є., 2019. 296 с.

18. Ляшук А.М. Семантична структура юридичних термінів української та англійської мов: дис... канд. філол. наук: 10.02.17 / Кіровоградський держ. педагогічний ун-т ім. В. Винниченка. Кіровоград, 2007. 335 с. 10. Вікіпедія. URL: https://uk.wikipedia.org/wiki/

19. Методичні рекомендації щодо використання інформаційних ресурсів Інтегрованої інформаційно-пошукової системи ОВС України / О.О. Мельнікова, К.Ю. Ісмайлов. Одеса: Одеський державний університет внутрішніх справ, 2018. 39 с.

20. Методичні рекомендації щодо виявлення, фіксації та вилучення криміналістично значущої інформації з мобільних пристроїв під час розслідування кримінальних правопорушень / Д.С. Афонін, К.Ю. Ісмайлов, Д.В. Лісніченко, О.І. Постол. Одеса: Одеський державний університет внутрішніх справ, 2018. 38 с.

21. Навчальний посібник Тактичний кримінальний аналіз: теорія і практика / Н.П. Свиридюк, О.М. Цильмак, Заєць О.М., Ісмайлов К.Ю., Некрасов В.А. за заг. ред. Користіна О.Є.; МВС України, ДНДІ, ОДУВС. Одеса: РВВ ОДУВС, 2019. 298 с.

22. Навчально-методичні рекомендації щодо застосування програми Proton VPN для анонімного пошуку оперативнозначущої інформації в Інтернеті / К.Ю. Ісмайлов, Сіфоров, В.С. Жогов, О.І. Одеса: ОДУВС, 2019. 14 с.

23. Навчально-методичні рекомендації щодо пошуку оперативнозначущої інформації в мережі Інтернет К.Ю. Ісмайлов, В.С. Жогов, Л.В. Лефтеров. Одеса: ОДУВС, 2019. 28 с.

24. Навчально-методичні рекомендації щодо пошуку оперативнозначущої інформації на електронних носіях / К.Ю. Ісмайлов, В.О. Русавський, Л.В. Лефтеров. Одеса: ОДУВС, 2019. 14 с.

25. Олійник О. Юридичні терміни як вербальні репрезентанти правового концепту. Наукові записки. Серія: Філологічні науки. 2018. Вип. 165. С. 331-338.

26. Основи кримінального аналізу: підручник / Бабенко А.М., Заєць О.М., Некрасов В.А., Ісмайлов К.Ю., Пефтієв Д.О. та ін.; за заг. ред. Користіна О.Є., 2019. 270 с.
27. Пошукова система. URL: https://uk.wikipedia.org/wiki/Пошукова_система
28. Про запровадження системи управління ризиками та системи кримінального аналізу у Державній прикордонній службі України: наказ Адміністрації Держприкордонслужби України від 21 лют. 2007 р. № 130. URL: https://old.dpsu.gov.ua/ua/Rozvitok-sistemi-analizu-rizikiv-Derzhprikordonsluzhbi-/
29. Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні. Наказ 07.07.2017 N 575 URL: https://ips.ligazakon.net/document/view/RE30805?q=Обшук%20на%20підприємстві&bl=
30. Про затвердження Інструкції з формування та ведення бази даних «Розшук» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України»
31. Про затвердження Інструкції про організацію та ведення кримінального аналізу оперативно-розшуковими підрозділами: наказ Адміністрації Держприкордон служби України від 15 січ. 2008 р. № 28.
32. Рішення Ради національної безпеки і оборони України. URL: https://zakon.rada.gov.ua/laws/show/n0004525-17
33. Свиридюк Н., Кардашевський Ю Аналітичні продукти методи, інструменти та трендові новації кримінального аналізу в Україні URL:https://vaite.kiev.ua/doi/ilp/ILP_Ch_32.pdf
34. Федчак І. А. Основи кримінального аналізу : навчальний посібник. Львів : Львівський державний університет внутрішніх справ, 2021. 288 с.-merezha/

Науково-методичне видання

Авторський колектив:
Афонін *Дмитро Сергійович*
Лісніченко *Дмитро Вікторович*
Заєць *Олександр Михайлович*

Використання методології OSINT для отримання оперативно-значимої інформації

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

Підписано до друку 23.12.2024. .Формат 60х84/16 Папір офсетний.
Гарн. «Times New Roman». Друк цифровий. Ум. друк .арк. 1,46.
Надруковано з готового оригінал-макета.
Наклад 10 прим.
Видавництво ОДУВС
м. Одеса, вул. Успенська, 1
Свідоцтво суб'єкта видавничої справи ДК № 3507 від 25.06.2009 р.