https://doi.org/10.31891/2219-9365-2025-84-13
УДК 004.056:621.397.3:004.942

ДЖУЛІЙ Володимир
Хмельницький національний університет
https://orcid.org/0000-0003-1878-4301
e-mail: dzhuliivm@khmnu.edu.ua
МУЛЯР Ігор
Хмельницький національний університет
https://orcid.org/0000-0002-6659-605X
e-mail: muliariv@khmnu.edu.ua
ФІЛЮК Євген
Хмельницький національний університет
https://orcid.org/0000-0003-1878-4301
e-mail: zhenyok3404@gmail.com

МЕТОД ВЕРИФІКАЦІЇ ВІДКРИТИХ ДЖЕРЕЛ ТА ВИЯВЛЕННЯ ДЕЗІНФОРМАЦІЇ ЗА ДОПОМОГОЮ OSINT-ІНСТРУМЕНТІВ

У статті запропоновано метод верифікації відкритих джерел (OSINT) та виявлення дезінформації у цифровому середовищі. Розглянуто теоретичні засади понятійного апарату (OSINT, дезінформація, маніпуляція, фактчекінг), процедури геолокації та хронолокації, триангуляцію джерел, оцінювання достовірності та упереджень, виявлення цифрових слідів та прихованих комунікаційв публічно доступних матеріалах, а також ризики для дослідника й етичні аспекти.

Запропоновано практичний алгоритм із контрольними списками та матрицею достовірності, а також набір інструментів для аналізу текстів, зображень, відео, мережевої інфраструктури та соціальних графів. Наведено короткі кейси застосування методів і визначено обмеження.

Ключові слова: OSINT, верифікація, фактчекінг, дезінформація, геолокація, хронолокація, триангуляція, медіафорензіка, стеганографія, мережевий аналіз.

DZHULIY Volodymyr, MULIAR Ihor, FILYUK Evhen
Khmelnytskyi National University

METHOD OF VERIFICATION OF OPEN SOURCES AND DETECTION OF DISINFORMATION USING OSINT TOOLS

The article proposes a method for verifying open sources (OSINT) and detecting disinformation in the digital environment. The theoretical foundations of the conceptual apparatus (OSINT, disinformation, manipulation, fact-checking), geolocation and chronolocation procedures, triangulation of sources, assessment of reliability and bias, detection of digital traces and hidden communications in publicly available materials, as well as risks for the researcher and ethical aspects are considered.

A practical algorithm with checklists and a reliability matrix is proposed, as well as a set of tools for analyzing texts, images, videos, network infrastructure and social graphs. Short cases of application of the methods are presented and limitations are identified.

The system architecture is built on a modular principle, where each module performs its own research function: the Source Credibility Matrix module analyzes the historical reliability and transparency of the source; the Contextual Reliability Index is responsible for the correlation analysis of facts through independent channels; the Semantic Sentiment Model conducts an in-depth cognitive assessment of the text, determining the level of manipulativeness; the Verification & Reporting Module forms an evidence base in the form of structured PDF/JSON reports. The system architecture is built on the principle of an intelligent data bus, which allows you to gradually move from collecting facts to forming a reliable conclusion.

The formed theoretical and methodological foundation defines the system as a hybrid model that combines the analytical rigor of OSINT intelligence with the cognitive depth of modern artificial intelligence. The system not only reproduces the classic intelligence cycle, but also expands it through intellectual interpretation, contextual reliability and semantic framing of messages.

Keywords: OSINT, verification, fact-checking, disinformation, geolocation, chronolocation, triangulation, media forensics, steganography, network analysis.

Стаття надійшла до редакції / Received 11.10.2025
Прийнята до друку / Accepted 18.11.2025

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

У сучасному світі, де інформація стає один із ключових способів впливу на свідомість людей, а доступ до даних стає практично необмеженим, питання її достовірності та методик перевірки на правдивість, використовуючи відкриті джерела інформації, набуває вагомого значення.

Одним з напрямків, що активно розвивається у цій сфері, є OSINT — розвідка на основі відкритих джерел інформації. Цей термін охоплює в собі процес збору, аналізу, систематизації та інтерпретації інформації, яка є публічно доступною, з метою отримання практичних або аналітичних висновків [1,2,3].

Важливою рисою OSINT є законність і етичність процесу добування інформації. На відміну від розвідувальних методів, які передбачають використання закритих каналів або спеціальних технічних засобів,

OSINT базується виключно на публічно доступних даних, що унеможливлює порушення права на приватність або втручання в особисте життя громадян. Законність використання OSINT є одним із ключових чинників його інтеграції у державні й громадські аналітичні структури. Той факт, що дані є відкритими, не означає, що вони можуть бути оброблені без урахування правових та етичних стандартів. Іншими словами, сам факт того, що дані є загальнодоступними, не означає відсутність обмежень для їх дослідження» [3,4,7].

OSINT еволюціонував із журналістських і розвідувальних практик у міждисциплінарну сферу, що спирається на цифрову криміналістику, лінгвістику, психологію сприйняття та теорію мереж. Серед поширених підходів [1,6,8]:

- класичний фактчекінг (verifiability-first): незалежна перевірка тверджень через первинні джерела, документи, офіційні бази даних;
- медіафорензіка: технічний аналіз зображень і відео (метадані, помилки стиснення, артефакти редагування);
- гео/хронолокація: співставлення візуальних ознак із картографічними та астрономічними даними;
- триангуляція: підтвердження інформації з трьох і більше незалежних джерел різної природи (офіційні реєстри, польові свідчення, цифрові сліди);
- аналіз мережевої інфраструктури: WHOIS, DNS, ASN-аналіз, пасивне спостереження за TLS/ SSL, виявлення мереж ботів.

Фахівці з OSINT повинні бути обізнані з методами стеганографії, щоб ефективно аналізувати цифрові сліди та виявляти приховані комунікації в публічно доступних матеріалах. Це особливо актуально при розслідуванні діяльності організованих злочинних груп або екстремістських організацій, які можуть використовувати стеганографію для координації своїх дій.

В умовах інформаційних операцій важливими є моделі оцінювання достовірності: «admiralty code», 5×5×5 матриці загроз/ймовірності та журналістські шкали надійності джерел.

Особливу роль у поширенні дезінформації відіграють соціальні мережі, де користувачі часто стають не лише споживачами, а й ретрансляторами контенту. Алгоритми рекомендацій у Facebook, X (Twitter), YouTube або TikTok можуть підсилювати ефект «інформаційної бульбашки», коли користувач бачить лише ту інформацію, яка підтверджує його погляди, і не стикається з альтернативними точками зору. Це створює сприятливі умови для маніпуляцій та поляризації суспільства. Хоча наукові дослідження показують, що ефект «бульбашки» не є абсолютним, саме алгоритмічні рекомендації мають вирішальний вплив на поширення маніпулятивного контенту [5,7,9,11].

В умовах гібридної війни та постійного інформаційного тиску, який на даний момент відчуває Україна, питання достовірності інформації що потрапляє в інтернет набуває критичного значення. Кібератаки ворога на інформаційний простір, фейкові новини, маніпуляції у соціальних мережах стали потужною зброєю, що впливає на суспільну свідомість, міжнародні відношення з державою та безпеку життів громадян.

В українських реаліях дезінформація має ще й гібридний характер, поєднуючи елементи психологічного, інформаційного та кібервпливу. Російська агресія проти України супроводжується масованими кампаніями дезінформації, які охоплюють як внутрішній, так і зовнішній інформаційний простір. Основні цілі таких кампаній — підрив довіри до державних інститутів, створення паніки, деморалізація населення та дискредитація міжнародних партнерів України. У контексті війни та гібридних загроз OSINT-інструменти стають невід'ємною складовою інформаційного суверенітету держави. Приклад дезінформації наведено на рис.1. Але насправді світлина була зроблена 6 квітня 2003 з описом: „Затоплений основний бойовий танк (ОБТ) M1A1 Abrams стоїть перед табором федаїнів недалеко від Джаман Аль-Джубурі, Ірак, під час операції «ІРАКІ ФРІДОМ».

Рис. 1. Допис в російському телеграм каналі з дезінформацією про знищення української бронетехніки

Масове поширення цифрових платформ і соціальних мереж спричинило вибухове зростання обсягу відкритих даних, водночас підвищивши вразливість суспільства до дезінформації та маніпуляцій. Верифікація відкритих джерел стала ключовою компетенцією для урядових структур, медіа та приватного сектору. OSINT (Open-Source Intelligence) охоплює методи збирання, обробки та аналізу інформації з відкритих джерел з метою отримання розвідувальної цінності [13,14,17].

Верифікація відкритих джерел та розвідка на основі відкритих джерел (OSINT) дозволяють системно виявляти, перевіряти та документувати різні види матеріалів дезінформаційної, спираючись, в першу чергу на прозорість та достовірність джерела даних.

Розвиток ефективності методів OSINT має ключове значення для протидії дезінформаційним загрозам, особливо в сучасних умовах цифрових медіа та стрімким розвитком Штучного Інтелекту (ШІ), який за допомогою функції для генерації зображень та відео збільшив кількість дезінформації в мережі [19,21,23,24].

OSINT-аналітики можуть використовувати методи стегоаналізу для виявлення прихованих повідомлень у публічно доступних зображеннях, відео чи аудіофайлах, які розміщені в соціальних мережах, на форумах або інших відкритих джерелах. Злочинці, терористи або шпигуни можуть використовувати стеганографію для приховування конфіденційної інформації в нешкідливих на вигляд медіафайлах, які потім публікуються у відкритому доступі.

Дослідження методів верифікації відкритих джерел та виявлення дезінформації є вкрай актуальним та значущим для українських реалій.

У науковій літературі теоретичні підходи до верифікації інформації у відкритих джерелах поєднують різні методології, моделі та принципи, що дозволяють систематично визначати правдивість, достовірність і релевантність даних [12,13,18].

Базовим підходом є модель «інтелектуального циклу» (intelligence cycle), яка передбачає послідовні етапи: планування, збір даних, обробку, аналіз, поширення та оцінку результатів. Така модель дозволяє структурувати верифікаційні процеси, встановити контрольні точки та стандарти якості, що особливо важливо в умовах великого обсягу даних з різнорідних джерел (рис. 2).

Рис. 2. Загальна демонстрація розвідувального процесу (циклу)

Кожен етап підвищує цінність інформації. На початковому етапі не зрозуміло не тільки що робити, але і що взагалі відбувається. Далі усвідомлюється, що відбувається і уявлення структуруються. Цінність інформації підвищилася. Після чого ви формулюєте проблему, ставите завдання й прикидаєте план дій. Цінність інформації ще збільшилася. Далі починається збір потенційно корисної інформації та її накопичення. Цінність інформації ще збільшується. І так у міру наближення до фінішу ви збільшуєте цінність вашої інформації. Але дійшовши до останнього пункту робота не закінчується. Як тільки споживач починає використовувати інформацію, надану вами, його обізнаність збільшується, а це вносить відповідні корективи в його дії і в його інформаційні потреби [8,11,15,16].

Коли OSINT-аналітик завантажує фотографію з соціальної мережі, Twitter, Telegram або будь-якого публічного джерела, він може витягти EXIF-дані, які містять інформацію про модель камери або смартфона, дату і точний час зйомки, GPS-координати місця, де було зроблено фото, налаштування експозиції, версію програмного забезпечення та іноді навіть серійний номер пристрою. Ці дані допомагають встановити автентичність зображення, геолокацію подій, ідентифікувати власника пристрою або побудувати часову лінію подій.

Стеганографія може використовувати ці ж самі поля метаданих для приховування секретної інформації. Наприклад, зловмисник може вставити зашифроване повідомлення в поле коментарів EXIF, змінити значення GPS-координат так, щоб вони кодували певні числа або команди, або використати поля

авторських прав і опису для передачі прихованих даних. На відміну від класичної стеганографії, яка модифікує піксельні дані зображення, стеганографія в метаданих змінює лише службову інформацію файлу, що часто легше реалізувати технічно.

Певне місце займає кореляційний підхід, за якого різні фрагменти інформації порівнюються між собою або зі сторонніми незалежними джерелами для виявлення невідповідностей. Наприклад, аналіз збіжності часових міток, геолокацій, метаданих зображень чи відео дає змогу виявити маніпуляції чи фальсифікації. У статті «Online Multimedia Verification with Computational Tools and OSINT: Russia-Ukraine Conflict Case Studies» наведено приклади таких кореляційних перевірок, коли кілька мультимедійних джерел інформації (архів Інтернету, супутникові знімки, відео з соцмереж) використовувались для підтвердження або спростування тверджень (рис.3) [5,6,20,21].

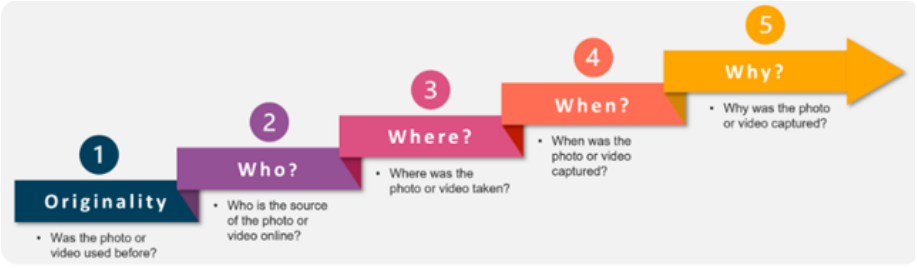

Рис. 3. Загальна структура перевірки мультимедійних даних, якої дотримуються основні новинні ЗМІ

Ще один підхід — використання алгоритмічних і машинно-навчальних методів для автоматизації частини верифікаційних процесів, що набуває дедалі більшого значення, особливо в умовах великих обсягів інформації й швидкого розповсюдження контенту. Це включає застосування моделей для класифікації контенту (наприклад, розділення на правдивий/фейковий), виявлення змінених або вигаданих елементів, таких як deepfake-зображення та відео, аналіз шаблонів поширення дезінформації (наприклад, визначення джерел, які найчастіше генерують маніпулятивний контент, або маршруту його розповсюдження через соцмережі), а також сегментацію тексту для виявлення мовних маркерів фейків чи маніпуляцій (спотворені факти, емоційні наголоси тощо) [5,6,12,17].

На практиці алгоритмічні методи допомагають зменшити навантаження на аналітика. Завдяки попередньої автоматичної фільтрації релевантного контенту, сортування матеріалів за ризиком або категорією, ідентифікація потенційно підозрілих відео, зображень чи повідомлень, дозволяє як слід перевірити інформацію глибше. Наприклад, пропонуються функції втрат (loss functions), які враховують рівність точності по різних демографічних групах, а також методи моделі-агностичного підходу, коли доступна інформація про демографію, або коли її немає. Було показано, що можна модифікувати існуючі детектори deepfake так, щоб зменшити упередженість щодо рас, статі чи інших атрибутів, зберігаючи або мінімально знижуючи загальну точність [3,5,6,9].

Разом з цим, алгоритмічні методи мають низку суттєвих обмежень і ризиків. Перш за все, моделі сильно залежні від якості даних, на яких вони тренуються, тобто якщо набір даних не представлений репрезентативно (наприклад, переважно особи однієї раси, віку чи статі), то модель може мати суттєві відмінності у точності для недостатньо представлених груп даних. Це призводить до упередженості, що зменшує довіру й може спричинити несправедливі помилки. Далі, моделі можуть бути вразливими до змін у форматі. Наприклад, різна якість відео або зображень, різні умови освітлення, стиснення, шум. Також моделі залишають в небезпеці від кібератак, які навмисно спотворюють контент, щоб обдурити детектор. Також існує проблема узагальнення. Це відбувається тоді коли модель, натренована на одному наборі даних, може показувати значно гірші результати на даних із інших джерел чи в реальних умовах [10,18,19,22].

Усі ці моменти означають, що застосування алгоритмічних методів у OSINT має супроводжуватись строгими вимогами до якості наборів даних, постійним оновленням моделей, використанням метрик правдивості наборів даних, а також поєднанням автоматизованих методів із людською експертизою, щоб кінцевий результат був завжди затверджений саме людиною.

Один із підходів до розвідку даних на основі відкритих джерел є контекстуальний. Він акцентує увагу на обставинах, мовному, культурному, історичному та географічному контексті інформації. Ідентичний факт може бути поданий по-різному, залежно від того, хто, де, коли та як його подає. Без врахування контексту легко зробити хибні висновки. У науковій роботі [11] підкреслюється, що судове визнання цифрових доказів залежить від коректного відтворення джерела, правильного опису контексту, дотримання ланцюжка доказів та методології їх збору – усіх етапів, що гарантують легітимність та достовірність матеріалів. Етапи продемонстровано на рис. 4.

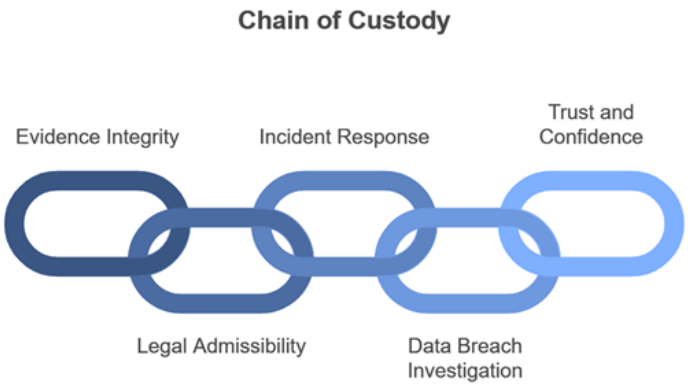

Рис. 4 Етапи методу ланцюжка доказів

Принцип перевірки через множинність джерел — це теоретична основа, коли для підтвердження твердження використовуються щонайменше два або більше незалежних джерел. Такий метод є критично важливий в OSINT, де аналітики підтверджують інформацію, порівнюючи її з даними щонайменше з двох або більше незалежних джерел.

У контексті дезінформації та неправдивої інформації даний метод є безцінним. Метод допомагає відсіяти неправдиві наративи, гарантуючи, що твердження підтверджуються кількома авторитетними точками даних. Наприклад, аналітик, який розслідує можливу кібератаку на державну інфраструктуру, може порівняти хеші шкідливих файлів, знайдені у відкритому репозиторії (наприклад, VirusTotal), з повідомленнями у спеціалізованих кіберфорумів, записами з бази даних MITRE ATT&CK та технічними звітами від незалежних дослідницьких груп (CISA, CERT-UA або ESET Research). Якщо збіг підтверджується з декількох джерел, це значно підвищує достовірність результату. Такий підхід дозволяє мінімізувати ризик маніпуляції, фальсифікації або навмисного вкидання фейкових артефактів у відкриті джерела, що особливо важливо під час гібридних інформаційно-кібернетичних операцій [7,8,20,21].

OSINT-аналітики можуть шукати стеганографічно приховану інформацію в публічно доступних файлах. Наприклад, терористичні угруповання історично використовували стеганографію для приховування координаційних повідомлень у зображеннях, розміщених на форумах чи в соціальних мережах. OSINT-спеціалісти завантажують такі файли з відкритих джерел і аналізують їх за допомогою інструментів стегоаналізу, намагаючись виявити аномалії, які можуть вказувати на приховані дані.

Крім того, **логічні підходи та правила мислення** (зокрема, правило несуперечності, правило достатнього доказу, принцип причинно-наслідкового зв'язку) становлять фундаментальну частину теоретичної бази OSINT-аналізу. Ці принципи передбачають, що будь-яка інформація, перш ніж бути прийнятою за достовірною, має пройти критичну перевірку на відповідність уже відомим фактам, часовим рамкам, просторовим обставинам та джерелам із доведеною репутацією [12,15,19,24].

Правило **несуперечності** вимагає, щоб твердження, отримані з різних джерел, не вступали у логічний конфлікт між собою. Якщо інформація суперечить іншим перевіреним даним — це сигнал для аналітика провести додаткову верифікацію або відкинути її як потенційно хибну. Наприклад, якщо у відкритих джерелах з'являються повідомлення про кібератаку, що нібито відбулася у певний час, але технічні логи або показники мережевої активності цього не підтверджують, аналітик має підстави сумніватися у достовірності такої інформації [13,17,18].

Правило **достатнього доказу** в OSINT передбачає, що жодне твердження не може бути прийняте без наявності підтверджень — цифрових артефактів, метаданих, офіційних документів або незалежних джерел, які взаємно підкріплюють одне одного [14,16,22,24]. Таким чином, логічна перевірка виступає не лише елементом формальної процедури, а ключовим захисним механізмом від маніпуляцій, помилкових інтерпретацій та свідомо сфабрикованих фейків.

Сучасна практика OSINT-аналізу поєднує ці логічні підходи з методами критичного мислення та цифрової етики, формуючи гібридну модель перевірки, у якій автоматизовані алгоритми, аналітичні бази даних і людський досвід взаємодоповнюють одне одного [15,18]. Такий підхід дозволяє не лише перевіряти факти, але й встановлювати їх достовірний контекст, що є особливо важливим в умовах гібридних інформаційних загроз та швидкого обігу даних.

Верифікація часто передбачає також етичні та юридичні підходи. Теорії етики засуджують маніпуляцію, вимагають транспарентності в джерелі та в методах його збору. Юридичні підходи (міжнародні стандарти, національні закони про цифрові докази, права людини) встановлюють рамки, у яких OSINT-дані можуть бути визнані як допустимі або ні. У межах України, як показує дослід Радейка, визнання цифрових доказів від соціальних мереж залежить від процедурних вимог, включаючи методологію, ланцюжок зберігання доказів, забезпечення достовірності контексту і формалізацію цифрових фактів.

У сукупності, теоретичні підходи до верифікації інформації у відкритих джерелах складають багатошарову систему, де технічні методи доповнюються аналітичними, логічними, контекстуальними та юридичними елементами. Така інтеграція дозволяє підвищити точність і достовірність висновків, оскільки автоматизовані інструменти перевірки даних поєднуються з людським аналізом та критичним мисленням. Аналітичні методи допомагають виділити ключові ознаки потенційних загроз, контекстуальні підходи враховують соціально-політичний та культурний фон інформації, а юридичні аспекти забезпечують дотримання норм законодавства та етичних стандартів при зборі і обробці даних.

Такий комплексний підхід стає особливо важливим в умовах інформаційної війни або гібридних загроз, де дезінформація та маніпуляції активно використовуються як інструмент впливу. Наприклад, при розслідуванні кібератак на державні або критично важливі інфраструктури, аналітики використовують поєднання цифрових слідів, OSINT-даних із соціальних мереж, відкритих технічних баз та юридично перевірених документів, щоб отримати надійний і обґрунтований висновок. Таким чином, багатошарова система верифікації не лише підвищує якість аналітичних висновків, а й зменшує ризики маніпуляцій, фейкових сигналів і помилкових інтерпретацій.

У поточному інформаційному просторі України, де інформаційні потоки формують не лише громадську думку, а й можуть підбурювати кібербезпеку держав, питання достовірності контенту з відкритих джерел стає стратегічним чинником інформаційної безпеки. Дана проблематика є особливо актуальною, оскільки саме в українському інформаційному просторі фіксується підвищена активність дезінформаційних кампаній, гібридних впливів і координованих маніпуляцій з боку зовнішніх суб'єктів. Тому створення методу обґрунтованого алгоритмом верифікації відкритих джерел постає не лише технічним завданням, а й науковою необхідністю для забезпечення національної інформаційної стійкості.

Проблема достовірності інформації у відкритих джерелах є ключовою для сучасних аналітичних і безпекових процесів. В умовах гібридної війни, де дезінформаційні атаки стали невід'ємною складовою інформаційного протистояння, особливої актуальності набуває створення ефективних методів перевірки достовірності відкритих даних. Застосування OSINT як системи збору, обробки та аналізу інформації потребує вдосконалення з урахуванням специфіки українського інформаційного простору, який характеризується високою динамікою, політичними маніпуляціями та активним використанням соціальних платформ у інформаційних війнах.

У межах проведеного дослідження розроблено метод верифікації дезінформації з відкритих джерел, який спрямований на месенджер Telegram, який є найбільш використовуваним джерелом інформації. Алгоритм спирається на поєднання класичних теорій розвідувального аналізу даних та когнітивної аналітики. Його теоретична основа формується на базі трьох взаємодоповнюючих концепцій, а саме: модель Intelligence Cycle; методологія Bellingcat Investigative Framework; модель EU DisinfoLab Verification Flow.

Дані підходи об'єднані єдиною метою для створення системи, здатної здійснювати об'єктивну, відтворювану й контекстно точну перевірку інформації.

Модель Intelligence Cycle визначає фундаментальний порядок дій у процесі обробки відкритих джерел. Вона передбачає послідовність етапів - планування, збір, обробка, аналіз і поширення інформації - які формують замкнутий аналітичний цикл розвідки даних. У межах цієї логіки будь-яка одиниця інформації має бути перевірена на кожному рівні, що розпочинаєтьс від первинного збору метаданих до формулювання висновку про її достовірність. Дана модель є універсальною для всіх типів розвідки, однак у контексті OSINT вона отримує специфічне застосування, а саме автоматизовану інтеграцію процесів і відтворюваність перевірки.

Методологія Bellingcat Investigative Framework додає до цього процесу емпіричну точність і доказову базу. Вона базується на принципах відкритості, триангуляції та цифрової верифікації. Bellingcat використовує сукупність цифрових інструментів, які дозволяють співставляти час, місце і джерело виникнення інформації, визначати хронологію її поширення та встановлювати оригінальне джерело. У контексті українського інформаційного простору цей підхід набуває особливої цінності, оскільки дозволяє відокремити спонтанний користувацький контент від цілеспрямованих інформаційних вкидів.

Третім елементом теоретичної основи є модель EU DisinfoLab Verification Flow, орієнтована на виявлення мереж дезінформації та визначення структурних закономірностей поширення фейків. Вона опирається на поняття інформаційних впливових мереж (information influence networks), у межах яких аналізуються не лише окремі повідомлення, а й зв'язки між каналами, сторінками та користувачами. Теоретично цей підхід базується на принципах комунікаційної теорії та аналізу соціальних мереж, що дозволяє виявляти системність поширення неправдивих наративів.

Таким чином, концепція алгоритму є інтегрованою моделлю, яка поєднує структурну логіку Intelligence Cycle, доказову базу Bellingcat Framework та контекстну глибину підходу EU DisinfoLab. Її головна мета полягає у створенні аналітичної системи, здатної одночасно оцінювати достовірність джерела, контекст повідомлення і смисловий зміст контенту. При цьому особлива увага приділяється автоматизації процесів, зменшенню людського фактору та підвищенню прозорості результатів.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Загальний алгоритм верифікації відкритих джерел складається з виконанням наступних кроків:

1. Формулювання перевірюваного твердження (assertion framing): що саме потрібно довести/ спростувати?

2. Класифікація даних (текст, зображення, відео, мережеві артефакти, реєстри).

3. Оцінка джерела (ідентичність, репутація, мотиви, історія).

4. Збирання підтверджень з незалежних каналів (щонайменше три різні типи).

5. Геолокація/хронолокація (де і коли відбулося?).

6.Технічна медіафорензіка (маніпуляції, монтаж, генеративні підробки).

7.Триангуляція + матриця достовірності (формальна оцінка).

8. Документування (журнал дій, збережені артефакти, хеши).

9. Peer review (перехресна перевірка колегами)

Методологічна архітектура алгоритму опирається на декілька фундаментальних принципів:

1. Принцип триангуляції, який передбачає перевірку будь-якого факту через незалежні джерела різної природи - текстові, візуальні та офіційні. Триангуляція забезпечує синергетичний ефект, адже поєднання різних інформаційних каналів дає змогу мінімізувати ризик суб'єктивного сприйняття та випадкових помилок.

2. Принцип модульності, який відображає структурну побудову процесу верифікації: кожен етап має власну функцію, але водночас інтегрується у загальну систему.

3. Принцип прозорості, що забезпечує відтворюваність і верифікованість кожного кроку аналітичного процесу.

4. Принцип локалізації, який відображає культурно-мовну адаптацію алгоритму до українського контексту, включаючи лінгвістичні особливості, політичну символіку та специфіку національних медіа.

На теоретичному рівні метод використовує низку аналітичних моделей, які формують його внутрішню структуру. Першою з них є Source Credibility Matrix (SCM) — матриця достовірності джерела, що базується на класичній теорії комунікативної довіри Ховланда (Hovland-Yale Credibility Model). Відповідно до цієї моделі, довіра до джерела визначається такими параметрами, як експертиза, надійність, незалежність і стабільність поведінкових патернів. Теоретично це означає, що будь-яке джерело інформації оцінюється не лише за формальною історією правдивості, але й за його структурною поведінкою - частотою публікацій, тематичною спрямованістю, політичною афіліацією та аудиторним впливом. SCM дозволяє системно визначати репутаційну складову джерела ще до аналізу самого контенту.

Ключовим елементом методу є Context Reliability Index (CRI) — індекс контекстуальної достовірності, який теоретично опирається на концепцію триангуляції даних. Відповідно до неї, достовірність інформації зростає пропорційно кількості незалежних підтверджень, отриманих із різних джерел. CRI враховує три виміри перевірки, такі як збіг контенту з авторитетними сайтами (Nc), підтвердження архівами або історичними джерелами (Ng) та відповідність часових параметрів повідомлення (Nt). Важливим доповненням є bias-фактор (B), який компенсує політичну або емоційну упередженість джерела. Теоретично ця модель відображає когнітивний аспект сприйняття інформації, що навіть за наявності кількох підтверджень, істина може бути спотворена через системну упередженість.

Важливим етапом методу є Semantic Sentiment Model (SSM) це модель семантичного та емоційного аналізу, що поєднує принципи когнітивного фреймінгу та афективних обчислень. Вона дозволяє виявити не лише зміст повідомлення, а й емоційне забарвлення, риторику впливу та потенційні маніпулятивні техніки. З точки зору теорії, фреймінг розглядається як спосіб структурування реальності через мову. Тому аналіз лінгвістичних патернів у межах SSM є важливим для розпізнавання фейкових або пропагандистських наративів. Таким чином, семантичний аналіз стає не лише технічним інструментом, а й когнітивним механізмом виявлення прихованих смислів у медійному повідомленні.

Важливою концепцією методу є Dynamic OSINT Evidence Base (DOEB). Вона походить із цифрової криміналістики та забезпечує простежуваність усіх перевірених об'єктів. Вона передбачає створення динамічної бази доказів, у якій кожен кейс має цифровий підпис, контрольний хеш та історію змін. Такий підхід узгоджується з принципом наукової відтворюваності, який передбачає що будь-який результат може бути повторно перевірений іншими дослідниками або автоматизованими системами. У цьому контексті DOEB виступає не лише архівом, а й інструментом забезпечення довготривалої достовірності результатів OSINT досліджень.

Таким чином, у сукупності всі ці теоретичні моделі утворюють багаторівневу систему, яка поєднує кількісні та якісні методи оцінки інформації. Кількісна складова забезпечується через формалізовані показники CRI, SCM, NSI. Тоді як якісна зосереджується на контекстному, семантичному та поведінковому аналізі. Такий підхід дозволяє перейти від традиційного фактичного верифікування до комплексного оцінювання інформації в її комунікативному, культурному та політичному контексті.

Алгоритм верифікації відображає сучасну тенденцію інтеграції OSINT-розвідки та когнітивної аналітики. Він опирається на синтез трьох вимірів достовірності: структурного (джерело), контекстуального

(умови появи інформації) та семантичного (зміст і риторика повідомлення). Така структура дозволяє алгоритму діяти не лише як інструмент перевірки фактів, а також як інтелектуальна система, що інтерпретує сенс, визначає рівень маніпулятивності та оцінює ризики дезінформації. З теоретичної точки зору, метод можна розглядати як адаптацію класичних моделей OSINT до умов сучасної інформаційної війни, де головним завданням стає не пошук істини як такої, а відновлення інформаційного балансу через науково обґрунтовану перевірку відкритих джерел.

Рис. 5. Алгоритм роботи модуля SCM

Архітектура алгоритму побудовано як багаторівневу модульну систему, у якій кожен рівень відповідає за певний аспект перевірки посту в відкритому Telegram-каналі на наявність дезінформації. Така структурна архітектура забезпечує не лише логічну послідовність процесу, а й методологічну узгодженість, де кожен модуль опирається на чітко визначену теоретичну основу та виконує функцію в межах загального циклу аналітичної верифікації. Основна ідея полягає в тому, що істинність повідомлення не є абсолютною величиною, а формується через сукупність незалежних підтверджень, отриманих із різних вимірів: джерельного, контекстуального, семантичного та інтеграційного.

ISSN 2219-9365

Концепція архітектури алгоритму відповідає адаптованій моделі розвідувального циклу, у якій виділяються чотири ключові етапи: оцінка джерела, контекстна перевірка, семантичний аналіз та інтеграційна верифікація. Кожен з них не лише виконує автономну аналітичну функцію, але й формує логічну послідовність: результати попереднього рівня слугують вхідними даними для наступного. Така архітектура гарантує системність, масштабованість і можливість багаторазової повторної перевірки результатів.

Перший модуль алгоритму побудований для аналітичного оцінюванню джерела інформації. Його теоретична основа базується на матриці довіреності до джерела, що є класичною моделлю в теорії комунікації. Відповідно до неї, довіра до джерела визначається через три взаємопов'язані параметри — експертизу, достовірність і динамічність. Експертиза відображає рівень компетентності джерела, який оцінюється на підставі історії правдивості попередніх постів, тематичної спеціалізації та авторитету серед інших джерел. Достовірність характеризує ступінь незалежності та неупередженості, тобто відсутність очевидної політичної мотивації у поданні інформації. Динамічність описує швидкість поширення матеріалів, стиль комунікації та поведінкові патерни у взаємодії з аудиторією. У цілому рівень довіри може бути виражено формулою (1):

$$SCM = (E \times 0.4) + (T \times 0.4) + (D \times 0.2), \quad (1)$$

де *E, T, D* - нормалізовані значення експертизи, достовірності та динамічності відповідно. Вагові коефіцієнти (0.4; 0.4; 0.2) визначають відносну важливість кожного параметра у загальній оцінці достовірності джерела: експертиза (*E*) та довіра (*T*) мають домінуючий вплив, оскільки прямо корелюють із сприйняттям авторитетності, тоді як динамічність (*D*) відіграє допоміжну роль, уточнюючи характер поширення інформації, але не визначаючи її правдивість.

OSINT використовує метадані для збору інформації про автора, місце створення, використане обладнання, тоді як стеганографія може приховувати секретні дані саме в метаданих або інших службових полях файлів, які доступні через OSINT-методи.

Алгоритму, що описує процес оцінювання представлений на рис. 5, спочатку ідентифікується джерело (канал, сайт, акаунт), далі здійснюється збір його метаданих і публічної активності, після чого кожен параметр отримує оцінку у шкалі від 0 до 1. Отримані значення інтегруються у єдиний коефіцієнт достовірності, який формує основу подальшої перевірки.

Другий модуль архітектури алгоритму пов'язаний із контекстуальною верифікацією контенту окремого посту, тобто зіставленням вмісту повідомлення з незалежними офіційними, архівними та часовими джерелами (рис.6).

Даний підхід ґрунтується на принципі триангуляції, який у соціальних науках означає підтвердження одного факту через кілька незалежних точок спостереження.

У межах теоретичної моделі CRI враховуються три основні параметри та формально індекс розраховується за формулою (2):

$$CRI = (N_c + N_g + N_t)/3 \cdot B, \quad (2)$$

де N_c - збіг контенту з офіційними джерелами, N_g - підтвердження факту наявності або збереження матеріалу в цифрових архівах, N_t - відповідність часових рамок появи інформації щодо інших джерел, B - корекційний коефіцієнт, що враховує упередженість джерела.

Таким чином, *CRI* є числовим показником контекстуальної достовірності, що інтегрує як технічні, так і когнітивні фактори.

Алгоритм роботи модуля *CRI* демонструє процес, який починається з аналізу тексту або зображення, продовжується перевіркою наявності відповідників у відкритих базах даних, після чого обчислюється середнє значення збігів і від нього віднімається bias-фактор. Отримане значення слугує формалізованим показником рівня відповідності інформації реальному контексту.

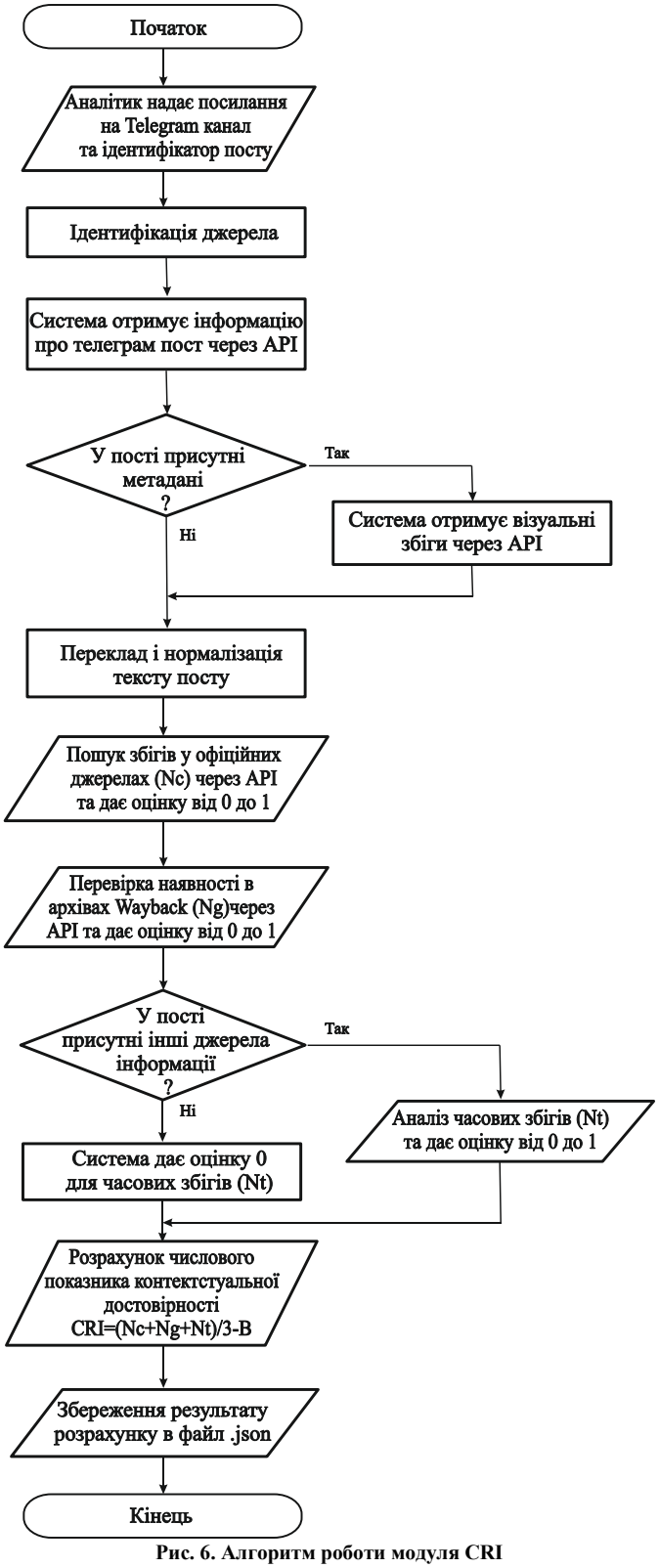

Рис. 6. Алгоритм роботи модуля CRI

Третій модуль спрямований на дослідження лінгвістичної структури та емоційного тону контенту (рис.7).

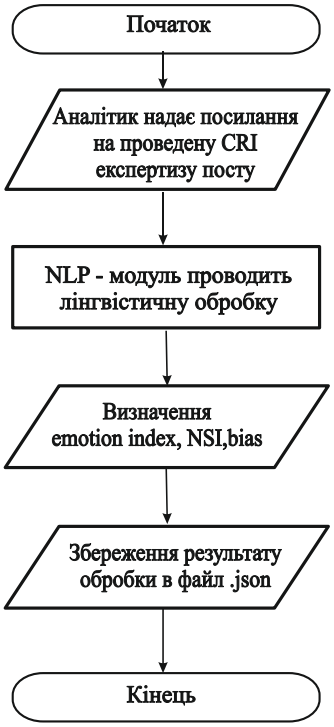

Рис. 7. Алгоритм роботи модуля семантичного аналізу

Теоретично даний модуль базується на двох провідних концепціях: Cognitive Framing Theory. Перша розглядає мову як інструмент формування когнітивних рамок, через які люди сприймають реальність; друга - як модель емоційної взаємодії людини та інформаційних систем. Семантичний аналіз дає змогу виявити ключові смислові ядра повідомлення, домінантні теми, повторювані наративи та маніпулятивні патерни. Емоційний компонент оцінює ступінь емоційної напруги через індекс emotion index (0–1) і коефіцієнт *NSI* (Narrative Saturation Index), що показує рівень повторюваності певних меседжів. Водночас визначається параметр bias, який окреслює загальну тональність тексту — проукраїнську, антиукраїнську або нейтральну.

Алгоритм семантичного аналізу (рис.7), демонструє наступну послідовність обробки: текст розділяється на лексичні одиниці, здійснюється частотний і семантичний аналіз, виділяються емоційно марковані слова, а потім система формує аналітичний профіль - від нейтрального до маніпулятивного. На цьому етапі створюється когнітивна карта змісту, що відображає структуру основних тем і потенційних спотворень.

Завершальним модулем архітектури є узагальнення отриманих даних і формування аналітичного висновку. Теоретично даний модуль виконує функцію інтеграції результатів з усіх попередніх модулів в єдину систему оцінки достовірності. На даному етапі інформація зводиться до узагальнених показників, на основі яких формується первинний вердикт системи: підтверджено, частково підтверджено, недостовірно або фейк/маніпуляція. Ключовим елементом є принцип доказової цілісності, що передбачає архівування усіх даних із контрольним хешем. Інтеграційна верифікація також має когнітивну складову, де результати подаються не як статичні показники, а як інтерпретаційна модель, що відображає логіку прийняття рішення автоматизованою системи. У звіт включаються дані про джерело, зміст, метадані, візуальні підтвердження, контекстні збіги та обчислений *CRI*. Це формує основу для подальшої експертної оцінки або повторної перевірки.

Модуль інтеграційної верифікації демонструє процес від узагальнення даних до формування висновку: результати модулів надходять до інтеграційного блоку, обчислюється комбінований показник достовірності, після чого генерується структурований звіт.

Метод верифікації відкритих джерел на наявність дезінформації являє собою комплексну модель аналітичної верифікації, у якій поєднуються класичні теоретичні основи комунікаційної достовірності, контекстної кореляції та когнітивного аналізу. Кожен модуль не лише виконує окрему функцію, а й формує частину єдиного аналітичного потоку, що перетворює сирі дані з відкритих джерел на доказову аналітичну інформацію. На теоретичному рівні така архітектура демонструє перехід від традиційного OSINT до когнітивно-аналітичного OSINT, де основна мета полягає не лише у виявленні фактів, а у відтворенні механізму інформаційної правди. Це дозволяє не просто визначити, чи є публікація дезінформуючою, а й пояснити, чому система прийшла до такого висновку, забезпечуючи наукову обґрунтованість, відтворюваність і прозорість процесу перевірки.

OSINT-аналітик, який шукає геолокаційну інформацію в метаданих фото терориста, може натрапити на підроблені або модифіковані метадані, що містять приховане повідомлення для іншого члена групи. Водночас багато соціальних мереж автоматично видаляють метадані при завантаженні зображень з міркувань приватності, що ускладнює як OSINT-аналіз, так і стеганографічну комунікацію через ці платформи. Саме тому зловмисники часто використовують платформи, що зберігають оригінальні файли.

Автоматизація процесів верифікації відкритих джерел потребує поєднання аналітичних, когнітивних і технічних інструментів у єдиній інтегрованій системі.

При проєктуванні методу верифікації відкритих джерел на наявність дезінформації було поставлено завдання створити технологічну екосистему, де точність, масштабованість і доказова відтворюваність є ключовими аспектами.

Обраний стек технологій сформовано на основі поєднання гнучких Python-інструментів, зовнішніх API-сервісів і бібліотек для когнітивного аналізу та документування результатів.

Даний підхід відповідає сучасним тенденціям розвитку OSINT-аналітики, де технології не лише виконують функцію збору даних, а стають частиною когнітивного середовища прийняття рішень. Саме тому під час вибору інструментів основну увагу було приділено їхній здатності інтегруватися між собою, підтримувати українську та англомовну семантику, працювати з різними форматами даних (текст, медіа, метадані) та забезпечувати валідацію результатів у формалізованому вигляді.

Для реалізації механізму зовнішньої перевірки фактів обрано сервіс SerpAPI, який надає API-доступ до пошукової системи Google з можливістю фільтрації результатів за доменами, мовами, часовими рамками та типами контенту. Це дає змогу системі автоматично перевіряти наявність повідомлень на офіційних урядових або міжнародних ресурсах (наприклад, gov.ua, europa.eu, un.org). SerpAPI надає значну кількість інтегрованих API для різноманітних пошукових систем (рис.8).

Також невід'ємною перевагою SerpAPI є стабільність результатів, відсутність обмежень на частоту запитів, а також структурований формат відповідей у JSON. Це дозволяє безпосередньо розраховувати коефіцієнт контекстуальної достовірності на основі кількості релевантних збігів. Таким чином, SerpAPI стає мостом між інформаційним простором і аналітичним ядром системи, перетворюючи пошукові дані на формалізовані докази.

Оскільки значна частина фейкових наративів поширюється у Telegram-каналах, важливою задачею стало забезпечення візуальної фіксації першоджерела. Для цього застосовано бібліотеку Playwright, яка автоматизує рендеринг веб-сторінок і створення скріншотів у headless-режимі. У системі OVA-U Playwright реалізовано у вигляді модуля TelegramScreenshotter, який відкриває пости без авторизації, зберігає їхній вигляд і додає до звіту як доказ.

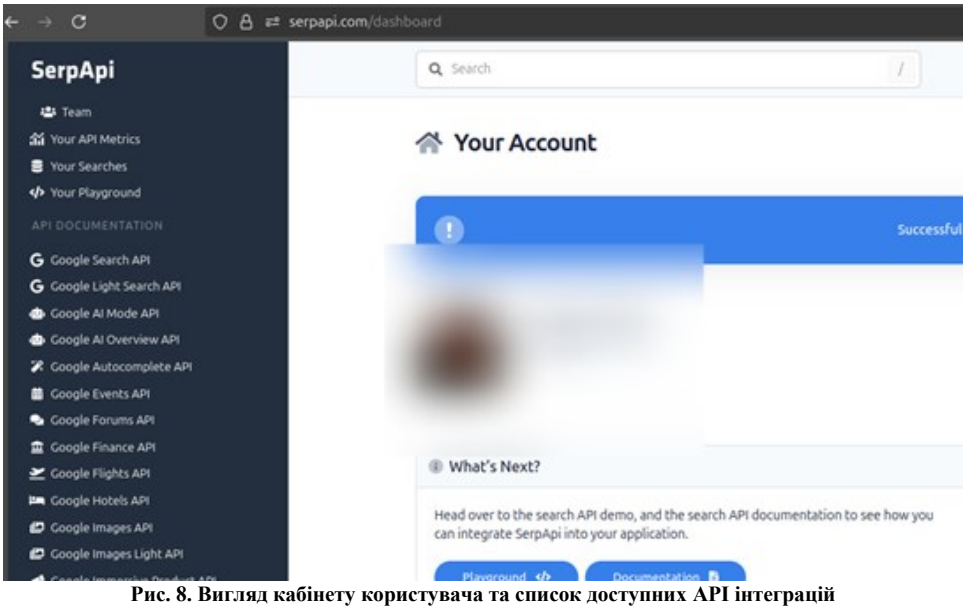

Рис. 8. Вигляд кабінету користувача та список доступних API інтеграцій

Основні переваги Playwright - стабільна робота з JavaScript-завантажуваними сайтами, висока якість зображень і можливість обробки великої кількості посилань без втрати продуктивності. Візуальні матеріали, отримані таким чином, використовуються не лише для архівування, а й як складова доказової бази у фінальному PDF-звітів.

На завершальному етапі роботи системи важливим є створення стандартизованого звіту, який містить результати аналізу, метадані, текстові висновки та візуальні докази. Для цього використовується бібліотека ReportLab, яка підтримує роботу з кирилицею, вставку зображень, таблиць, графічних елементів і

форматованого тексту. Вибір ReportLab продиктований вимогою до доказової цілісності: PDF-файл є незмінним форматом, який може бути архівований, підписаний хеш-підписом SHA-256 і використаний у судово-аналітичних процесах.

Крім того, ReportLab дозволяє створювати структуровані звіти, які поєднують технічні дані, аналітичні показники та описові висновки в єдиному документі, що підвищує рівень наукової відтворюваності. Бібліотека Pillow, що розвиває класичний пакет PIL, використовується для обробки зображень перед вставкою у звіт. Вона дозволяє автоматично масштабувати, обрізати та оптимізувати фотографії або скріншоти Telegram-постів, забезпечуючи збереження пропорцій та якості. Цей етап є важливим для візуальної достовірності, оскільки гарантує, що жоден доказ не зазнає викривлення або втрати контексту під час документування.

Формат JSON використовується як базовий носій структурованих даних між усіма модулями системи. Він забезпечує машинну сумісність, легку серіалізацію об’єктів і можливість інтеграції з будь-якими зовнішніми сервісами. JSON-звіти слугують проміжною ланкою між аналітичним процесом і документуванням, дозволяючи зберігати історію верифікаційних дій та створювати динамічну базу доказів, у якій кожен кейс має свій унікальний цифровий слід.

Не менш важливою складовою архітектури є система логування, яка забезпечує аудит кожного етапу виконання алгоритму. Усі дії — від перекладу тексту до збереження фінального звіту — фіксуються у хронологічному журналі. Це відповідає принципу traceability, який є базовим у науковій та розвідувальній аналітиці, оскільки дозволяє перевірити, яким чином система прийшла до конкретного висновку.

Обраний стек технологій формує синергійну архітектуру, у якій кожен інструмент виконує чітко визначену роль. Python забезпечує модульність і гнучкість, aiohttp - асинхронну ефективність, OpenAI - когнітивну глибину, SerpAPI - доступ до верифікованих джерел, Playwright і Pillow - візуальну достовірність, ReportLab - документальну стабільність, а JSON і логування - структурну прозорість і доказову відтворюваність. Разом вони створюють цілісну систему, що відповідає міжнародним стандартам OSINT-аналітики та враховує український контекст гібридної інформаційної війни.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Проведене теоретичне дослідження дало змогу сформувати цілісну концепцію методу OVA-U (OSINT Verification Algorithm for Ukraine) - інтелектуально-аналітичної системи верифікації відкритих джерел, розробленої для умов українського інформаційного простору. На основі аналізу існуючих моделей OSINT-розвідки (Intelligence Cycle, Bellingcat, EU DisinfoLab) було обґрунтовано доцільність поєднання класичних принципів інформаційного аналізу з новітніми когнітивними технологіями штучного інтелекту.

Метод OVA-U базується на чотирьох концептуальних стовпах: достовірності джерела, контекстуальній перевірці, семантичному розумінні та доказовій фіксації. Кожен із них реалізовано у вигляді окремого модуля, який взаємодіє з іншими через спільну аналітичну платформу. Така модульна архітектура забезпечує масштабованість, адаптивність і можливість повторного використання компонентів у майбутніх OSINT-проектах.

Обґрунтовано теоретичну базу побудови алгоритму, що ґрунтується на поєднанні моделей Intelligence Cycle (для циклічності збору та аналізу даних), Bellingcat Investigative Framework (для геолокаційної та часової верифікації) та EU DisinfoLab Verification Flow (для класифікації дезінформаційних наративів). На цій основі сформовано фундаментальні принципи системи: триангуляцію, модульність, прозорість і локалізацію під український контекст.

Архітектуру системи побудовано по модульному принципу, де кожен модуль виконує власну дослідницьку функцію: модуль *SCM* (Source Credibility Matrix) аналізує історичну достовірність і прозорість джерела; *CRI* (Contextual Reliability Index) відповідає за кореляційний аналіз фактів через незалежні канали; *SSM* (Semantic Sentiment Model) проводить глибинну когнітивну оцінку тексту, визначаючи рівень маніпулятивності; Verification & Reporting Module формує доказову базу у вигляді структурованих звітів PDF/JSON. Архітектура системи побудована за принципом інтелектуальної шини даних, що дозволяє поетапно переходити від збору фактів до формування достовірного висновку. OSINT-аналітики моніторять публічні канали на предмет стеганографічних комунікацій. Це може бути виявлення паттернів публікацій зображень у соціальних мережах, аналіз файлів на хакерських форумах або дослідження медіаконтенту екстремістських груп, де підозрюється використання стеганографії.

Таким чином, сформований теоретико-методичний фундамент визначає OVA-U як гібридну модель, що об’єднує аналітичну строгість OSINT-розвідки з когнітивною глибиною сучасного штучного інтелекту. Система не лише відтворює класичний розвідувальний цикл, а й розширює його за рахунок інтелектуальної інтерпретації, контекстуальної достовірності (*CRI*) та семантичного фреймінгу повідомлень.

Література

1. What is OSINT: Open-source intelligence? European data. URL: https://data.europa.eu/en/publications/datastories/what-osint-open-source-intelligence

2. Van Puyvelde D., Tabárez Rienzi F. The rise of open-source intelligence // European Journal of International Security. Cambridge University Press. URL: https://www.cambridge.org/core/journals/european-journal-of-international-security/article/rise-of-opensource-intelligence/21122432399ECB8078BF0D89A76D0586

3. OSINT: розвідка з відкритим вихідним кодом. European data. 02.05.2022. URL: https://data.europa.eu/en/publications/datastories/what-osint-open-source-intelligence

4. Як ефективно використовувати OSINT-інструментарій? Команда «OsintFlow» ділиться досвідом // Державна прикордонна служба України. URL: https://dpsu.gov.ua/uk/news/43174-YAk-efektivno-vikoristovuvati-OSINT-instrumentariy-Komanda-OsintFlow-dilitsya-dosvidom

5. Зоренко Д. С., Лех Р. В., Кулик Д. О., Червяков О. І. Використання інструментів та методів OSINT для отримання пошукової інформації: практичний порадник. Інститут підготовки юридичних кадрів для СБУ, 2023. 4 с.

6. Івкова В. С., Опірський І. Р. Дослідження існуючих засобів та підходів до проведення OSINT в контексті інформаційної безпеки особи та держави. Наукові праці Національного університету «Львівська політехніка», 2025.

7. Bellingcat. Digital Verification Toolkit. URL: https://www.bellingcat.com/resources/how-tos/

8. MITRE ATT&CK Framework. URL: https://attack.mitre.org/

9. Oxford Internet Institute. Industrialized social media manipulation. 2021. URL: https://demtech.oii.ox.ac.uk/

10. Kuipers C. Ethics and Open-Source Intelligence. NATO Strategic Communications Centre of Excellence, 2021. 34 p.

11. Hybrid CoE. OSINT in Hybrid Warfare: Strategic Implications. European Centre of Excellence for Countering Hybrid Threats, 2022.

12. Wardle C., Derakhshan H. Information Disorder: Definitions, Impacts, Solutions. Council of Europe Report, 2017. 109 p.

13. Judgement acceptance of OSINT evidence from social networks in courts: legal and methodological aspects // Journal of Cybersecurity & Digital Forensics. 2023.

14. Ju Y., Hu Y., Jia S., Lyu S. Improving Fairness in Deepfake Detection. 2023 IEEE International Conference on AI Security (AISec). https://doi.org/10.1109/AISec2023

15. Xu Ying, Terhörst Philipp, Raja Kiran, Pedersen Marius. Analyzing Fairness in Deepfake Detection With Massively Annotated Databases. Pattern Recognition, 2022. https://doi.org/10.1016/j.patcog.2022.108686

16. Hayden M. The Intelligence Cycle Explained. RAND Corporation.

17. Nasibov A. Online Multimedia Verification with Computational Tools and OSINT: Russia-Ukraine Conflict Case Studies, 2023

18. Radev O. Theoretical and legal framework for the admissibility of OSINT evidence from social networks in Ukrainian courts. Юридичний Вісник, 2021.

19. CISA. Cyber Incident Response and OSINT Case Handling. Department of Homeland Security, USA — офіційна методичка.

20. CERT-UA. Рекомендації з розслідування кіберінцидентів з використанням OSINT, 2023.

21. European Centre of Excellence for Countering Hybrid Threats (HybridCoE). OSINT in Hybrid Warfare, 2022 — експертний звіт.

22. Wardle C., Derakhshan H. Information Disorder: Definitions and Proposed Taxonomy. Council of Europe Report, 2017.

23. Oxford Internet Institute. Evidence of social media manipulation by political actors at industrial scale, звіт 2021.

24. EU DisinfoLab. Disinformation Tactics in Hybrid Conflicts, 2020 — аналітичний звіт.

References

1. What is OSINT: Open-source intelligence? European data. URL: https://data.europa.eu/en/publications/datastories/what-osint-open-source-intelligence

2. Van Puyvelde D., Tabárez Rienzi F. The rise of open-source intelligence // European Journal of International Security. Cambridge University Press. URL: https://www.cambridge.org/core/journals/european-journal-of-international-security/article/rise-of-opensource-intelligence/21122432399ECB8078BF0D89A76D0586

3. OSINT: rozvidka z vidkrytym vykhidnym kodom. European data. 02.05.2022. URL: https://data.europa.eu/en/publications/datastories/what-osint-open-source-intelligence

4. Yak efektyvno vykorystovuvaty OSINT-instrumentarii? Komanda «OsintFlow» dilytsia dosvidom // Derzhavna prykordonna sluzhba Ukrainy. URL: https://dpsu.gov.ua/uk/news/43174-YAk-efektivno-vikoristovuvati-OSINT-instrumentariy-Komanda-OsintFlow-dilitsya-dosvidom

5. Zorenko D. S., Lekh R. V., Kulyk D. O., Cherviakov O. I. Vykorystannia instrumentiv ta metodiv OSINT dlia otrymannia poshukovoi informatsii: praktychnyi poradnyk. Instytut pidhotovky yurydychnykh kadriv dlia SBU, 2023. 4 s.

6. Ivkova V. S., Opirskyi I. R. Doslidzhennia isnuiuchykh zasobiv ta pidkhodiv do provedennia OSINT v konteksti informatsiinoi bezpeky osoby ta derzhavy. Naukovi pratsi Natsionalnoho universytetu «Lvivska politekhnika», 2025.
7. Bellingcat. Digital Verification Toolkit. URL: https://www.bellingcat.com/resources/how-tos/
8. MITRE ATT&CK Framework. URL: https://attack.mitre.org/
9. Oxford Internet Institute. Industrialized social media manipulation. 2021. URL: https://demtech.oii.ox.ac.uk/
10. Kuipers C. Ethics and Open-Source Intelligence. NATO Strategic Communications Centre of Excellence, 2021. 34 p.
11. Hybrid CoE. OSINT in Hybrid Warfare: Strategic Implications. European Centre of Excellence for Countering Hybrid Threats, 2022.
12. Wardle C., Derakhshan H. Information Disorder: Definitions, Impacts, Solutions. Council of Europe Report, 2017. 109 p.
13. Judgement acceptance of OSINT evidence from social networks in courts: legal and methodological aspects // Journal of Cybersecurity & Digital Forensics. 2023.
14. Ju Y., Hu Y., Jia S., Lyu S. Improving Fairness in Deepfake Detection. 2023 IEEE International Conference on AI Security (AISec). https://doi.org/10.1109/AISec2023
15. Xu Ying, Terhörst Philipp, Raja Kiran, Pedersen Marius. Analyzing Fairness in Deepfake Detection With Massively Annotated Databases. Pattern Recognition, 2022. https://doi.org/10.1016/j.patcog.2022.108686
16. Hayden M. The Intelligence Cycle Explained. RAND Corporation.
17. Nasibov A. Online Multimedia Verification with Computational Tools and OSINT: Russia-Ukraine Conflict Case Studies, 2023
18. Radev O. Theoretical and legal framework for the admissibility of OSINT evidence from social networks in Ukrainian courts. Yurydychnyi Visnyk, 2021.
19. CISA. Cyber Incident Response and OSINT Case Handling. Department of Homeland Security, USA — ofitsiina metodychka.
20. CERT-UA. Rekomendatsii z rozsliduvannia kiberintsydentiv z vykorystanniam OSINT, 2023.
21. European Centre of Excellence for Countering Hybrid Threats (HybridCoE). OSINT in Hybrid Warfare, 2022 — ekspertnyi zvit.
22. Wardle C., Derakhshan H. Information Disorder: Definitions and Proposed Taxonomy. Council of Europe Report, 2017.
23. Oxford Internet Institute. Evidence of social media manipulation by political actors at industrial scale, zvit 2021.
24. EU DisinfoLab. Disinformation Tactics in Hybrid Conflicts, 2020 — analitychnyi zvit.