темнового рахунку в 100× ID230 зберігає 138 км (59 % від номіналу), тоді як ID220 — лише 24 км (20 %).

На відміну від NuQKD та OpenQKDSecurity, інструмент орієнтований на інженерну задачу: відкритий код, пресети комерційних SPAD 2004–2025 за публічними datasheet, GLLP+MC та інтерактивна карта $L_{max}(\eta_d, Y_0)$ як критерій вибору детектора.

Інструмент валідовано (MC-аналітика $|\Delta| \leq 6$ % при $L \leq 100$ км). Сучасні SPAD (ID Qube, ID230) забезпечують 175–233 км стійкого QKD-каналу проти 163 км зразка 2004. Результати можуть використовуватись для обґрунтованого вибору SPAD при проектуванні QKD-ланок. Перспектива — розширення інструмента на інші протоколи QKD та finite-key аналіз.

1. Chen H.Z., Li M.H., Wang Y.Z. et al. Implementation of carrier-grade quantum
2. communication networks over 10000 km. npj Quantum Information. 2025. Vol. 11. Art. 137. DOI: 10.1038/s41534-025-01089-8.
3. Bennett C.H., Brassard G. Quantum cryptography: Public key distribution and coin tossing. Proc. IEEE Int. Conf. Comput. Syst. Signal Process., Bangalore, 1984. P. 175–179.
4. Lo H.-K., Ma X., Chen K. Decoy state quantum key distribution. Phys. Rev. Lett. 2005. Vol. 94. P. 230504.
5. Gottesman D., Lo H.-K., Lütkenhaus N., Preskill J. Security of quantum key distribution with imperfect devices. Quant. Inf. Comput. 2004. Vol. 4. P. 325–360. arXiv:quant-ph/0212066.

Архітектура системи верифікації відкритих джерел за допомогою OSINT-технологій

УДК 004.056

Олена Пирч[1], Катерина Федоренко[2]

Хмельницький національний університет,
[1]pyrchov@khmnu.edu.ua, [2]katefedorenko8080@gmail.com

В українських реаліях дезінформація має виражений гібридний характер і поєднує психологічні, інформаційні та кіберкомпоненти. Російська збройна агресія проти України супроводжується масштабними інформаційно-психологічними операціями, спрямованими як на внутрішню, так і на зовнішню аудиторію. Основними цілями таких кампаній є підрив довіри до державних інститутів, посилення почуття нестабільності та беззахисності, деморалізація населення, дискредитація Збройних сил України та міжнародних партнерів. Для їх реалізації активно використовуються анонімні Telegram-канали, фейкові акаунти у соціальних мережах, медіаресурси та мережі ботів [1].

Архітектура системи верифікації відкритих джерел побудована як багаторівнева модульна система, у якій кожен рівень відповідає за окремий аспект перевірки допису у відкритому Telegram-каналі на наявність дезінформації. Така структурна організація системи забезпечує не лише логічну послідовність процесу, а й методологічну узгодженість, оскільки кожен модуль

опирається на чітко визначену теоретичну основу та виконує свою функцію в межах загального циклу аналітичної верифікації.

Концепція архітектури системи верифікації відкритих джерел відповідає адаптованій моделі розвідувального циклу, у межах якої виділено чотири ключові етапи: оцінка джерела, контекстна перевірка, семантичний аналіз та інтеграційна верифікація. Кожен з етапів виконує автономну аналітичну функцію, але водночас утворює логічну послідовність, де результати попереднього рівня слугують вхідними даними для наступного. Такий підхід забезпечує системність, масштабованість та можливість багаторазової повторної перевірки отриманих результатів [2].

Архітектура системи верифікації відкритих джерел на наявність дезінформації є комплексною моделлю аналітичної верифікації, у якій поєднано класичні теоретичні засади комунікаційної достовірності, контекстної кореляції та когнітивного аналізу. Кожен модуль виконує окрему функцію, але водночас є частиною єдиного аналітичного потоку, що перетворює сирі дані з відкритих джерел на доказову аналітичну інформацію.

Модуль первинної OSINT-ідентифікації Telegram-поста, у загальній архітектурі системи виконує функцію вхідної ланки для подальшого аналітичного опрацювання. На даному етапі «сирий» контент із Telegram перетворюється на структурований набір даних, придатний для подальшої контекстної, семантичної та інтегрованої перевірки. Модуль забезпечує послідовне отримання метаданих, завантаження медіафайлів, витягнення EXIF-інформації, виконання зворотного пошуку зображення та формування базової часової триангуляції появи інформації у різних джерелах. Завдяки цьому подальші модулі працюють не з неструктурованим повідомленням, а з узгодженим набором полів, які можна обробляти автоматизованими методами.

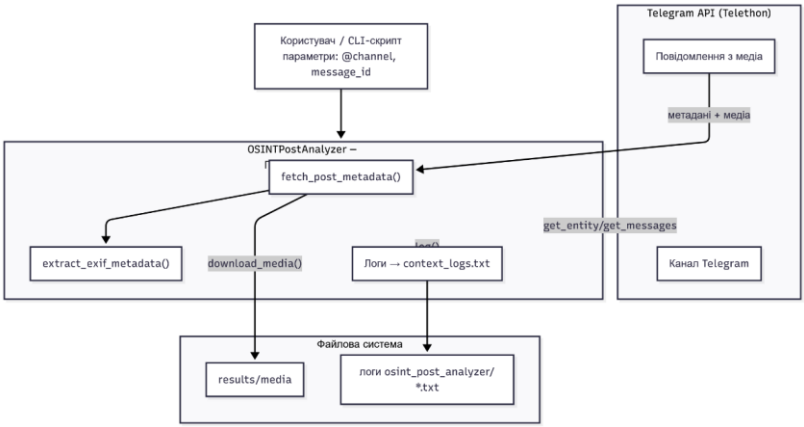

Рис. 1. Отримання Telegram-поста та первинна обробка

Модуль працює в асинхронному режимі з використанням async await. Це дає можливість паралельно звертатися до Telegram та зовнішніх сервісів і не

блокувати виконання програми. Узагальнену схему взаємодії класу з Telegram API, сервісами SerpAPI і imgbb та файловою системою подано на рисунку 1 та наведено основні потоки даних і місця збереження результатів.

На основі проведеного дослідження розроблено архітектуру системи верифікації відкритих джерел, яка охоплює декілька взаємопов'язаних модулів. Усі ці елементи об'єднано у єдину систему інтегрованої оцінки, що забезпечує можливість об'єктивного визначення ступеня достовірності досліджуваного матеріалу. Важливою складовою системи є застосування Source Credibility Matrix, яка дозволяє кількісно характеризувати надійність каналу на основі його історії, активності, стабільності публікацій та виявлених ознак маніпулятивності. Дані елементи створюють теоретично обґрунтований інструмент для оцінювання джерел інформації, що особливо важливо в умовах інформаційних загроз, спрямованих на українське суспільство.

1. What is OSINT: Open-source intelligence? European data. URL: https://data.europa.eu/en/publications/datastories/what-osint-open-source-intelligence.
2. 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.

Сучасні підходи до трансформації систем охорони праці на основі штучного інтелекту та предикативної аналітики

УДК 004.056.5:57.087.1
Михайло Пригара[1], В'ячеслав Шматуха[2], Володимир Щербина[3]

[1]Ужгородський національний університет, misha_prigara@ukr.net,
[2]Київська школа економіки, vvshmatukha@gmail.com,
[3]Державний університет «Київський авіаційний інститут», smya@kai.edu.ua

Традиційні системи управління охороною праці (СУОП) тривалий час базувалися на реактивному підході — аналізі інцидентів, що вже відбулися. Однак у 2025–2026 роках девіз Всесвітнього дня охорони праці «Революційні підходи до здоров'я і безпеки: роль ШІ та цифровізації» підкреслив глобальний перехід до проактивних стратегій. Використання ШІ дозволяє не лише фіксувати порушення, а й передбачати їх, створюючи динамічне безпечне середовище.

1. Ключові напрями використання ШІ в ОП

Сучасні підходи можна класифікувати за технологічними доменами:

- Комп'ютерний зір (Computer Vision) для моніторингу в реальному часі
- Це найбільш поширений напрям у 2026 році. Камери з ШІ інтегруються в існуючі системи відеоспостереження для:
- Автоматичного контролю використання засобів індивідуального