

Використання OSINT технологій для виявлення корупційних правопорушень: сучасні підходи та виклики*

Думчиков М.О.¹

Опубліковано	Секція	УДК
14.10.2024	Право	43.983

DOI: <https://doi.org/10.5281/zenodo.13928363>

Анотація. У сучасному українському суспільстві корупція продовжує бути одним із найсерйозніших викликів, що підриває основи правової держави, знижує довіру громадян до державних інституцій та гальмує економічний розвиток. Традиційні методи виявлення корупційних правопорушень часто виявляються недостатніми в умовах глобалізації, цифровізації та швидкого розвитку інформаційно-телекомунікаційних технологій. Технології відкритої розвідки (OSINT) відкривають нові можливості для збору та аналізу великого обсягу інформації з відкритих джерел, сприяючи більш ефективному виявленню корупційних схем та протидії їм. Однак інтеграція OSINT у антикорупційну діяльність супроводжується низкою правових, етичних, організаційних та технічних проблем, які потребують ґрунтовного наукового дослідження та розробки ефективних рішень.

У статті проаналізовано сучасні підходи до використання OSINT-інструментів у боротьбі з корупцією в Україні, з особливим акцентом на моніторинг соціальних медіа, аналіз відкритих державних реєстрів, геолокаційний та візуальний аналіз, а також застосування штучного інтелекту та машинного навчання. Наведено приклади успішного застосування OSINT у виявленні корупційних правопорушень, зокрема розслідування "Плівки Оніщенко" та виявлення незадекларованих маєтків суддів, що підкреслює ефективність цих методів.

Авторами робиться висновок про необхідність вдосконалення нормативно-правової бази, інвестування в підготовку фахівців та розвиток технічної інфраструктури для повного розкриття потенціалу OSINT у протидії корупції в Україні. Автори наголошують, що лише через системний підхід, який включає правове врегулювання, розвиток технологій та людського капіталу, можна досягти значних результатів у боротьбі з корупційними правопорушеннями та підвищити прозорість і підзвітність державних інституцій.

Ключові слова: цифровізація, OSINT інструменти, корупція, корупційні правопорушення, OSINT розвідка.

* Робота виконана в рамках проекту № 55.16-24/26.3П-01 за темою «Корупція в умовах воєнного стану та післявоєнної відбудови: оптимальна модель протидії»

¹ Д.ю.н., доцент, доцент кафедри кримінально правових дисциплін та судочинства Навчально-наукового інституту права СумДУ, <https://orcid.org/0000-0002-4244-2419>

Using OSINT technologies to detect corruption offenses: modern approaches and challenges

Abstract. In contemporary Ukrainian society, corruption continues to be one of the most serious challenges, undermining the foundations of the rule of law, diminishing citizens' trust in state institutions, and hindering economic development. Traditional methods of detecting corruption offences often prove insufficient in the context of globalisation, digitalisation, and the rapid advancement of information and communication technologies. Open-source intelligence (OSINT) technologies open up new possibilities for collecting and analysing large volumes of information from open sources, facilitating more effective detection and counteraction of corruption schemes. However, the integration of OSINT into anti-corruption activities is accompanied by a range of legal, ethical, organisational, and technical issues that require thorough scientific research and the development of effective solutions.

The article analyses contemporary approaches to the use of OSINT tools in combating corruption in Ukraine, with particular emphasis on monitoring social media, analysing open state registers, geolocation and visual analysis, as well as the application of artificial intelligence and machine learning. Examples of successful OSINT applications in detecting corruption offences are provided, including the investigation of the "Onyshchenko Tapes" and the uncovering of undeclared properties owned by judges, which underscores the effectiveness of these methods.

The authors conclude that it is necessary to improve the regulatory and legal framework, invest in the training of specialists, and develop technical infrastructure to fully realise the potential of OSINT in combating corruption in Ukraine. They emphasise that only through a systematic approach, which includes legal regulation, technological development, and enhancement of human capital, can significant results be achieved in the fight against corruption offences and in increasing the transparency and accountability of state institutions.

Keywords: digitization, OSINT tools, corruption, corruption offenses, OSINT intelligence.

Вступ

Постановка проблеми. Сьогодні наше суспільство стикається зі архіскладними викликами у сфері протидії корупції, яка підриває основи правової держави, знижує довіру громадян до державних інституцій та стримує економічний розвиток. Зауважимо, що традиційні методи виявлення корупційних правопорушень часто виявляються недостатніми в умовах глобалізації, цифровізації та швидкого розвитку інформаційно-телекомунікаційних технологій. Сьогодні, технології відкритої розвідки (OSINT) відкривають нові можливості для збору та аналізу великого обсягу інформації з відкритих джерел, сприяючи більш ефективному виявленню корупційних схем. Водночас, інтеграція OSINT у антикорупційну діяльність супроводжується низкою проблем, зокрема правових, етичних, організаційних та технічних, які потребують ґрунтовного наукового дослідження, розробки ефективних рішень та адаптації законодавства до сучасних реалій. Відсутність чітких методик та нормативно-правового регулювання використання OSINT у цій сфері створює додаткові перешкоди для правоохоронних органів та вимагає комплексного підходу до вирішення поставлених завдань.

Стан дослідження. Питаннями використання OSINT методів та інструментів для отримання пошукової інформації було предметом наукового інтересу на теоретичному рівні таких науковців, як: Зоренко Д.С., Лех Р.В., Кулик Д.О., Яровий Т.С. та інші. Водночас, проблематика використання OSINT методів в розрізі виявлення та розслідування корупційних правопорушень залишається актуальною як науковою так і практичною проблемою

Мета дослідження полягає в аналізі та висвітленні проблем та можливостей використання OSINT методів та інструментів для виявлення корупційних правопорушень, а також визначення ролі відкритих джерел у протидії таким правопорушенням.

Результати

Розвиток інформаційно-телекомунікаційних технологій, мобільного зв'язку та глобальної мережі Інтернет сприяв формуванню нової реальності, у якій сучасна людина вже не уявляє свого життя без використання електронних технічних засобів та відповідних можливостей, які вони забезпечують. Сьогодні, практично кожен громадянин має в особистому користуванні смартфон, ноутбук або планшет з доступом до мережі Інтернет. Більшість таких осіб мають особисті профілі в соціальних мережах, акаунти на різних онлайн-платформах та активно використовують цифрові ресурси для комунікації, розваг і професійної діяльності.

Перехід українського суспільства у інформаційну епоху обумовив як зміну існуючих механізмів захисту національних інтересів та реалізації політики державної безпеки, так і запровадження нових механізмів, зокрема – підходів, форм, інструментів обробки великих масивів інформації як у цивільній, так і у військовій сферах [1].

Варто зауважити, що зловмисники у своїх протиправних цілях дедалі частіше використовують інформаційно-телекомунікаційні технології, а саму інформацію про особу що вчинила кримінальне правопорушення та власне про саме кримінальне правопорушення, загалом нерідко можна знайти у відкритому доступі в мережі Інтернет. Водночас, пошук інформації з відкритих джерел не є таким простим, як може здаватися на перший погляд, оскільки для цього необхідне володіння певними навичками і знаннями щодо того, де шукати та що шукати. Ця діяльність має назву «OSINT».

OSINT (англ. "open source intelligence") – це методи розвідки, що полягають у пошуку, зборі та аналізі інформації з відкритих джерел [2]. Він зародився ще у 1941 році в США. У 1947 році аналітик ЦРУ (пізніше – керівник Бюро національної розвідки ЦРУ, відомий як «батько розвідувального аналізу») Шерман Кент зазначив в одному з інтерв'ю, що 80 % інформації, необхідної для прийняття рішень, ЦРУ отримує з відкритих джерел.

Сьогодні OSINT стає все більш актуальним не лише для урядових структур, але й для приватного сектора, журналістів, громадських активістів та дослідників. Сучасний розвиток інформаційно-комунікаційних технологій та широке поширення інтернет-ресурсів значно розширили можливості використання OSINT. Соціальні мережі, онлайн-видання, державні реєстри, форуми та багато інших джерел стали доступними для аналізу, що дозволяє ефективно отримувати інформацію про різні аспекти діяльності осіб чи організацій [3].

Водночас, незважаючи на доступність, ефективне використання OSINT вимагає специфічних знань і навичок, таких як знання технік пошуку, методології аналізу даних та розуміння юридичних аспектів, пов'язаних із використанням відкритої інформації. Крім того, у контексті сучасних загроз, таких як дезінформація та фейкові новини, критичне мислення та вміння відрізнити надійні джерела стають важливими елементами OSINT-досліджень [4].

Сам термін «OSINT» у тому значенні у якому він використовується сьогодні був запроваджений американськими військовими наприкінці 1980-х років у зв'язку з реформуванням розвідувальної служби та виникненням нових інформаційних вимог. У 1996 році Комісія Американського розвідувального співтовариства (відоміша як комісія Аспіна-Брауна) заявила, що «необхідно докласти

більше зусиль для використання загальносвітової інформації, доступної зараз з відкритих джерел». У цей же час в НАТО були розроблені довідники з OSINT, які містили керівництва та практичні рекомендації щодо використання відкритої інформації.

Вже з кінця 1990-х років OSINT став невід'ємною частиною розвідувальної діяльності не лише урядових установ, а й міжнародних організацій, таких як НАТО, які визнали важливість об'єднання ресурсів з відкритих джерел для підтримки безпеки та прийняття рішень. Завдяки швидкому розвитку інформаційних технологій та інтернету, OSINT отримав новий поштовх, що зробило його важливим інструментом у сфері інформаційної безпеки, боротьби з тероризмом та у різних галузях комерційної діяльності [4, с. 678].

Дослідження в галузі OSINT мають широкий спектр застосувань, включаючи виявлення та протидію корупційним правопорушенням, кібербезпеку, розвідку, управління репутацією, а також боротьбу зі злочинністю та тероризмом. Варто наголосити, що OSINT відіграє важливу роль у протидії корупційним правопорушенням, оскільки дозволяє аналізувати відкриті джерела інформації, такі як реєстри власності, бази даних компаній, соціальні мережі, урядові документи та медіа-матеріали.

Використовуючи ці дані, можна виявляти потенційні конфлікти інтересів, сліди незаконних транзакцій, приховані активи та інші корупційні схеми, як результат це робить OSINT цінним інструментом для журналістів-розслідувачів, громадських активістів та антикорупційних організацій.

Однак варто зауважити, що, використання OSINT для виявлення корупційних правопорушень потребує не лише технічних навичок, але й глибоких знань законодавства та дотримання етичних норм. Водночас, робота з відкритими даними має відповідати правовим вимогам щодо захисту особистих даних та приватності, що є важливим аспектом під час проведення антикорупційних розслідувань.

Пропонуємо розглянути сучасні підходи використання OSINT інструментів в антикорупційній діяльності з акцентом на Україну. На нашу думку найбільш прийнятною буде застосування типологізації на основі наступних індикаторів: 1) інформаційно-телекомунікаційний моніторинг; 2) аналіз відкритих джерел та баз даних; 3) геолокаційний та візуальний аналіз; 4) використання спеціалізованих OSINT-інструментів та платформ; 5) використання машинного навчання та генеративних елементів штучного інтелекту; 6) спеціалізовані OSINT інструменти; 7) журналістські розслідування.

Пропонуємо розглянути деякі з зазначених індикаторів. Моніторинг соціальних медіа та онлайн-ресурсів відіграє важливу роль у боротьбі з корупцією в Україні.

Акцентуємо увагу на тому, що журналісти-розслідувачі, часто використовують соціальні мережі типу інстаграму та фесбуку для виявлення незадекларованих активів. Вони знаходять фотографії, де посадовці демонструють розкішні автомобілі або подорожі, які не відповідають їхнім офіційним доходам, що свідчить про можливі приховані джерела прибутку. Так, наприклад, журналісти програми «Схеми» Радіо Свобода викрили на недекларуванні майна та доходів Депутатки Житомирської міської ради на понад один мільйон доларів [6].

Аналіз соціальних зв'язків у мережах дозволяє виявити зв'язки між чиновниками та бізнесменами. Проект "Bihus.Info" часто публікує розслідування, які показують приховані стосунки, що можуть вказувати на конфлікт інтересів або корупційні схеми [7].

Не менш важливу роль у боротьбі з корупцією відіграють спеціалізовані OSINT-інструменти та платформи. На нашу думку, одним із ключових ресурсів онлайн-платформа YouControl. Ця платформа надає доступ до детальної інформації про компанії, їхніх власників та пов'язаних осіб. Цей інструмент широко використовується для

перевірки контрагентів та виявлення можливих корупційних схем, оскільки дозволяє аналізувати зв'язки між бізнесом і посадовими особами [8].

Інший важливий сервіс - Opendatabot, який агрегує дані з державних реєстрів та судових рішень. Він допомагає виявляти судові процеси, пов'язані з корупцією, і надає можливість відстежувати юридичні дії щодо певних осіб або компаній. Це сприяє підвищенню прозорості судової системи та дозволяє громадськості бути обізнаною про перебіг важливих справ [9].

Наголошуємо, що використання цих спеціалізованих OSINT-інструментів підвищує ефективність антикорупційних заходів, надаючи можливість швидко та точно обробляти великі обсяги відкритих даних. Водночас, повномасштабне вторгнення яке супроводжується постійними кібератаками на державний інформаційний сектор, зумовило тимчасове закриття багатьох відкритих реєстрів з міркувань безпеки.

Напевно одну з ключових ролей у боротьбі та викритті корупційних зловживань, відіграє геолокаційний та візуальний аналіз, які стають дедалі важливішими інструментами у боротьбі з цим деструктивним явищем в Україні. Використання сервісів, таких як Google Earth, дозволяє аналізувати супутникові знімки для виявлення незадекларованих маєтків посадовців. Ці технології сприяють виявленню незаконних забудов у заповідних зонах або розкішних об'єктів нерухомості, що не відповідають офіційно задекларованим доходам чиновників.

Варто звернути увагу на сервіси типу Street View, які надають можливість перевіряти реальний стан об'єктів нерухомості, зазначених у деклараціях. Завдяки цьому можна підтвердити або спростувати інформацію про наявність та стан певних об'єктів, що допомагає виявляти розбіжності між офіційними даними та фактичною ситуацією.

В нашому дослідженні ми не може оминати сучасні технології, зокрема штучний інтелект та машинне навчання, які, активно впроваджуються в Україні для підвищення ефективності боротьби з корупцією. Так, наприклад, проєкт «Прозорро.Продажі» використовує алгоритми для аналізу аномалій у процесах продажу державного майна. Завдяки цьому вдається виявляти підозрілі операції та запобігати зловживанням під час реалізації державних активів. На нашу думку, використання штучного інтелекту та машинного навчання дозволяє державним органам оперативно реагувати на потенційні корупційні ризики, підвищуючи прозорість та підзвітність державного сектору [10].

В рамках нашого дослідження не можемо оминати приклади успішного використання OSINT інструментів в Україні. На нашу думку зослідування "Плівки Оніщенко" стало яскравим прикладом ефективного застосування відкритих джерел інформації у боротьбі з корупцією. Олександр Оніщенко, колишній народний депутат та бізнесмен, опинився в центрі скандалу, пов'язаного з корупційними схемами в газовій сфері. У 2016 році Національне антикорупційне бюро України звинуватило його в організації схем, які завдали державі збитків понад 1,6 мільярда гривень. Журналісти отримали доступ до аудіозаписів, відомих як "Плівки Оніщенко", та проаналізували їх для встановлення автентичності і змісту. Вони також використовували відкриті дані з державних реєстрів, судових рішень та міжнародних баз даних для виявлення компаній, пов'язаних з Оніщенком, і їхніх фінансових операцій. Результатом цього розслідування стали кримінальні провадження проти Оніщенко та його спільників, міжнародна співпраця з іноземними правоохоронними органами та підвищення обізнаності громадськості про корупцію у вищих ешелонах влади [11].

Висновки

Український досвід використання OSINT в антикорупційній діяльності демонструє значний потенціал зазначених технологій у виявленні та розслідуванні корупційних

правопорушень. Завдяки активній участі громадянського суспільства, незалежних журналістів та підтримці міжнародних партнерів, в Україні сформовано інноваційне середовище для розвитку та застосування відкритої розвідки. Перш за все це сприяє впровадженню нових методів та інструментів, які підвищують ефективність антикорупційних розслідувань та сприяють підвищенню прозорості та підзвітності державних інституцій. Зокрема, використання відкритих даних з державних реєстрів, аналіз соціальних мереж та публічних ресурсів дозволяє виявляти складні корупційні схеми та притягати до відповідальності винних осіб.

Водночас для повного розкриття потенціалу OSINT необхідно подолати існуючі виклики, серед яких ключовими є вдосконалення законодавчої бази та інвестування в підготовку кадрів. Нинішнє законодавство потребує адаптації до сучасних реалій, забезпечення правової визначеності щодо використання відкритих даних та захисту персональної інформації. На наше переконання, лише через системний підхід, який включає нормативно-правове врегулювання, розвиток технічної інфраструктури та людського капіталу, можна досягти максимального ефекту від використання відкритої розвідки у боротьбі з корупцією в Україні.

Список використаних джерел

1. Яровой, Т. С. OSINT, як перспективний інструмент контролю за лобістською діяльністю в контексті державної безпеки. Експерт: парадигми юридичних наук і державного управління, (4(6)), 201-208. [https://doi.org/10.32689/2617-9660-2019-4\(6\)-201-208](https://doi.org/10.32689/2617-9660-2019-4(6)-201-208)
2. Коротка історія розвідки на основі відкритих джерел (OSINT). URL: <https://postinfosociety.com/kоротка-istoriya-rozvidky-na-osnovi-vidkrytyh-dzherel-osint/>
3. NATO Handbook Open Source Intelligence. URL: <http://information-retrieval.info/docs/NATO-OSINT.html>
4. Open source intelligence tools and resources handbook. URL: https://intelligence.eu/uploads/public-documents/OSINT_Handbook_June-2018_Final.pdf
5. Michael Glassman, Min Ju Kang. Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). Computers in Human Behavior. Volume 28, Issue 2. 2012. P. 673-682. <https://doi.org/10.1016/j.chb.2011.11.014>.
6. «Схеми»: Депутатка Розенблат не задекларувала майна та доходів у Дубаї на 1 мільйон доларів. Офіційний веб-сайт. Радіо Свобода. URL: <https://www.radiosvoboda.org/a/skhemy-rozenblat-nerukhomist-dubay-deklaratsiya/33153792.html>
7. Інформаційний ресурс bihus.info. URL: <https://bihus.info/>
8. Українська аналітична онлайн-система YouControl. Офіційний веб-сайт. URL: <https://youcontrol.com.ua/>
9. Українська аналітична онлайн-система Опендатабот. Офіційний веб-сайт. URL: <https://opendatabot.ua/>
10. Українська універсальна біржа - офіційний майданчик системи прозорро.продажі. Офіційний веб-сайт. URL: <https://sale.uub.com.ua/>
11. "Плівки Онищенко": Депутат оприлюднив запис розмови з Порошенком. Офіційний веб-сайт. Українська правда. URL: <https://www.pravda.com.ua/news/2018/04/19/7178113/>