**СУСЛІКОВА І. С.,**
orcid.org/0000-0003-3399-020X
доктор філософії з економіки,
доцент кафедри фінансового
та податкового права
*(Державний податковий університет)*

**УДК 343.98**
**DOI https://doi.org/10.32842/2078-3736/2025.6.78**

# ЗАСТОСУВАННЯ OSINT-МЕТОДІВ У ВИЯВЛЕННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У ФІНАНСОВІЙ СФЕРІ, ВЧИНЕНИХ З ВИКОРИСТАННЯМ ЦИФРОВИХ ТЕХНОЛОГІЙ

Метою статті є формулювання теоретичних засад та практичних рекомендацій щодо ефективного застосування OSINT-методів (розвідки з відкритих джерел) у процесі виявлення, документування та розслідування цифрових фінансових злочинів, з урахуванням сучасних викликів інформаційної безпеки, недосконалості нормативно-правового регулювання та необхідності адаптації зарубіжного досвіду до національного правового поля України. У статті розкрито значення та можливості застосування методів розвідки з відкритих джерел (OSINT) у процесі виявлення, фіксації та розслідування кримінальних правопорушень у фінансовій сфері, які вчинено із використанням цифрових технологій. Наголошується, що в умовах цифровізації фінансових операцій та анонімізації кіберпростору класичні методи розслідування дедалі частіше потребують доповнення технологічно орієнтованими підходами. Здійснено класифікацію основних OSINT-методів, зокрема аналіз цифрового профілю суб'єктів, моніторинг соціальних мереж, обробку метаданих файлів, ідентифікацію IP-адрес та відстеження ланцюгів фінансових транзакцій. Розглянуто приклади використання OSINT у практиці правоохоронних органів України та зарубіжних держав (США, Польща, Франція), а також проаналізовано конкретні кейси з виявлення фіктивних інвестиційних платформ, шахрайських дій у сфері криптовалют, та діяльності фінансових «пірамід». Увагу приділено також актуальним проблемам впровадження OSINT-інструментів, зокрема: відсутність уніфікованих стандартів збору та обробки даних, недосконалість правового регулювання доступу до інформації з відкритих джерел, обмежена цифрова компетентність слідчих і суддів, а також ризики порушення прав людини при застосуванні таких методів. Запропоновано напрями удосконалення, до яких віднесено створення спеціалізованих підрозділів з OSINT-аналітики в системі досудового розслідування; розробка єдиних методичних рекомендацій; налагодження транскордонного обміну аналітичними матеріалами; розвиток навчальних програм для працівників правоохоронної та судової систем. Підкреслюється необхідність інтеграції OSINT до загальної системи криміналістичної методики розслідування фінансових правопорушень.

***Ключові слова:*** *OSINT, фінансові правопорушення, цифрові технології, кіберзлочинність, відкриті джерела, розвідка з відкритих джерел, криптовалюта, цифрові докази, профілювання, транзакційний аналіз, метадані, інформаційна безпека.*

**Suslikova I. S. Application of osint methods in detecting criminal offences in the financial sphere committed using digital technologies**

The purpose of the article is to formulate theoretical principles and practical recommendations for the effective application of OSINT methods (open source intelligence) in the process of detecting, documenting and investigating digital financial crimes, taking into account modern challenges of information security, imperfection of regulatory and legal regulation, and the need to adapt foreign experience to the national legal field of Ukraine. This article reveals the importance and possibilities of using open source intelligence (OSINT) methods in the process of detecting, recording and investigating criminal offenses in the financial sector committed using digital technologies. It is emphasized that in the conditions of digitalization of financial transactions and anonymization of cyberspace, classic investigation methods increasingly need to be supplemented with technologically oriented approaches. The scientific work has classified the main OSINT methods, in particular, analysis of the digital profile of subjects, monitoring of social networks, processing of file metadata, identification of IP addresses and tracking of financial transaction chains. Examples of the use of OSINT in the practice of law enforcement agencies of Ukraine and foreign countries (USA, Poland, France) have been considered, and specific cases of detecting fictitious investment platforms, fraudulent actions in the field of cryptocurrencies, and the activities of financial «pyramids» have been analyzed. Attention is also paid to the current problems of implementing OSINT tools: the lack of unified standards for data collection and processing, imperfect legal regulation of access to information from open sources, limited digital competence of investigators and judges, as well as the risks of human rights violations when using such methods. Areas of improvement are proposed: the creation of specialized units for OSINT analytics in the pre-trial investigation system; the development of unified methodological recommendations; the establishment of cross-border exchange of analytical materials; the development of training programs for law enforcement and judicial system employees. The article emphasizes the need to integrate OSINT into the general system of forensic methods for investigating financial crimes.

***Key words:*** *OSINT, financial offenses, digital technologies, cybercrime, open sources, open source intelligence, cryptocurrency, digital evidence, profiling, transactional analysis, metadata, information security.*

**Актуальність теми.** З огляду на стрімкий розвиток цифрових технологій, фінансові кримінальні правопорушення дедалі частіше вчиняються із використанням сучасних засобів комунікації, а також цифрових активів і платформ. У цьому контексті актуалізується необхідність модернізації інструментів кримінального аналізу, зокрема через залучення OSINT-методів (Open Source Intelligence) - збору, обробки та аналізу даних із відкритих джерел (соціальних мереж, відкритих баз даних, сайтів, реєстрів тощо). OSINT інструменти дають змогу оперативно і з мінімальними витратами виявляти шахрайські схеми, цифрові сліди підозрюваних, джерела нелегального фінансування та пов'язані суб'єкти.

Попри потенціал OSINT як елементу цифрової криміналістики, в Україні його застосування поки що не є належним чином регламентоване. Питання допустимості доказів, зібраних за допомогою таких методів, залишається спірним, а професійна підготовка слідчих у цій сфері обмежена. У країнах Європейського Союзу та США OSINT-методики вже вбудовані в розслідування кібер- та фінансових правопорушень, зокрема в діяльність фінансової розвідки, антикорупційних служб та правоохоронних органів. Таким чином, дослідження можливостей імплементації OSINT в українську слідчу та оперативно-розшукову практику є важливим і своєчасним завданням у межах цифрової трансформації правоохоронної системи.

**Аналіз останніх досліджень і публікацій.** Проблематику застосування OSINT у сфері цифрових розслідувань досліджували такі науковці, як В. Цимбалюк, І. Куліш, В. Кузнєцов,

В. Костицький, А. Журавель, О. Кучинська. Серед зарубіжних учених, які досліджували проблематику застосування OSINT-методів у виявленні цифрових та фінансових злочинів, слід відзначити Мартіна Ріда, Андреа Манку, Бена Б'юкенена, Томаса Голта, Джошуа Крукшенка, Девіда Кантора, Майкла Макгвайра, Кевіна Макгіна та Кіта Александера.

Попри активне впровадження інструментів OSINT у діяльність правоохоронних органів, значна частина питань, пов'язаних із виявленням і документуванням цифрових фінансових кримінальних правопорушень, залишається недостатньо розробленою. Насамперед, мова йде про відсутність узагальненої методології застосування OSINT у сфері протидії саме фінансовим кіберзлочинам, а також про неурегульованість правового статусу отриманих з відкритих джерел даних як доказової бази у кримінальному провадженні. В Україні досі відсутня уніфікована практика визнання таких доказів судами, що створює ризики їх відхилення на етапі судового розгляду.

Крім того, відкритими залишаються питання етичного використання особистої інформації, доступної в мережі, а також цифрової безпеки OSINT-платформ, які можуть зазнавати зовнішнього втручання або фальсифікацій. Не менш важливими є проблеми алгоритмізації OSINT-аналітики, можливості використання штучного інтелекту для виявлення аномальних фінансових транзакцій, а також кадрового й технічного забезпечення слідчих підрозділів. Потребує наукового обґрунтування й порівняльний аналіз іноземного досвіду, який міг би стати основою для вдосконалення вітчизняної практики з урахуванням міжнародних стандартів цифрової розвідки.

**Метою статті** є формулювання теоретичних засад та практичних рекомендацій щодо ефективного застосування OSINT-методів (розвідки з відкритих джерел) у процесі виявлення, документування та розслідування цифрових фінансових злочинів, з урахуванням сучасних викликів інформаційної безпеки, недосконалості нормативно-правового регулювання та необхідності адаптації зарубіжного досвіду до національного правового поля України.

**Виклад основного матеріалу.** У сучасних умовах цифровізації суспільства та поширення електронної комунікації розвідка з відкритих джерел (OSINT, Open Source Intelligence) відіграє дедалі важливішу роль у розслідуванні кримінальних правопорушень, зокрема у фінансовій сфері. OSINT-методи дозволяють отримувати, систематизувати та аналізувати відомості, які є відкритими, доступними для загального користування та правомірно зібраними без втручання в приватну сферу особи [1]. Вони охоплюють широкий спектр джерел – від публічних вебресурсів і державних реєстрів до соціальних мереж, форумів, даркнет-майданчиків, аналітичних баз даних та цифрових слідів у вигляді метаданих.

У межах розслідування фінансових кіберзлочинів методи OSINT (розвідки з відкритих джерел) широко використовуються для встановлення осіб, причетних до кримінально протиправної діяльності, виявлення нелегальних джерел прибутку, аналізу руху коштів, що можуть бути отримані кримінально протиправним шляхом, а також для виявлення взаємозв'язків між учасниками фінансових схем. Особливо ефективним у цьому контексті є метод цифрового профілювання, який полягає в цільовому зборі та аналізі інформації з відкритих джерел щодо поведінкових та економічних характеристик підозрюваної особи.

Цей метод охоплює вивчення активності користувачів у соціальних мережах, на форумах, в онлайн-оголошеннях, коментарях, фото- та відеоконтенті з метою формування цифрового образу суб'єкта. Здобута інформація дозволяє встановити можливі джерела доходів, факти придбання майна, наявність незареєстрованої підприємницької діяльності, фінансові операції через криптовалюти, що офіційно не задекларовані, а також допомагає виявити потенційних співучасників або бенефіціарів незаконної діяльності. Таким чином, OSINT-підхід підвищує ефективність оперативно-розшукових заходів та забезпечує підґрунтя для ініціювання процесуальних дій у межах кримінального провадження [2].

Так, у практиці розслідування фінансових кіберзлочинів із використанням OSINT-методів є низка показових міжнародних і українських кейсів. Наведемо кілька узагальнених прикладів:

У 2022 році під час розслідування ухилення від оподаткування фізичної особи–підприємця правоохоронці виявили у Facebook та Instagram численні публікації з елітних курортів, а також відеоогляди нових автомобілів, придбаних нібито «на подарунок». Водночас за офіційною декларацією особа мала мінімальні доходи. Зібрана OSINT-інформація стала підставою для відкриття провадження щодо незаконного збагачення.

У 2023 році на основі OSINT-аналітики була виявлена схема обготівкування криптовалют у Києві. Слідчі вивчили публічні повідомлення на криптофорумах та Telegram-каналах, де фігуранти пропонували «анонімне виведення BTC». Зокрема, за допомогою сервісів Blockchain Explorer були встановлені зв'язки між гаманцями, виведенням коштів у фіат через обмінники, а також реальні імена, прив'язані до профілів на платформах фрилансу. Це дозволило ідентифікувати учасників злочинної групи.

Одним із найефективніших OSINT-методів, що застосовується у практиці розслідування фінансових кримінальних правопорушень, є аналіз метаданих цифрових об'єктів. Метадані – це структуровані технічні відомості, які автоматично генеруються та вбудовуються у файли під час їх створення або редагування. Вони можуть містити відомості про автора, дату й час створення, геолокацію, версію програмного забезпечення, модель пристрою, мережеву активність, IP-адресу, операційну систему тощо.

У розслідуванні шахрайства у сфері криптоінвестування, метадані можуть відігравати ключову роль. Наприклад, у справі U.S. v. Ignatov, S.D.N.Y., що стосувалася проєкту OneCoin – однієї з найбільших у світі схем фінансового шахрайства – саме метадані презентаційних файлів PowerPoint дозволили ідентифікувати внутрішніх розробників і довести фальсифікацію фінансових показників, які використовувалися для залучення інвесторів. Дані вказували на редагування документів в офісі фірми у Софії (Болгарія) та прив'язували активність до певних пристроїв [1].

У національній практиці України також є випадки, коли вилучені з месенджерів документи у форматі PDF, що мали ознаки підробки (фейкові договори позики, інвойси), аналізувалися за допомогою таких інструментів, як ExifTool, Metadata2Go, PDF-XChange Viewer. У результаті виявлялося, що файл був створений на пристрої, зареєстрованому на іншу фізичну особу, ніж вказано у реквізитах, або до підпису був змінений час редагування, що дозволяло поставити під сумнів автентичність документа.

Також характерним є використання метаданого аналізу в справах про кримінальні правопорушення, пов'язані з фальсифікацією тендерної документації, зокрема у Prozorro. Аналіз електронних заявок виявляв ознаки того, що усі документи, подані нібито різними суб'єктами, були створені на одному комп'ютері в один день [3]. Це дало підстави для кваліфікації дій за ознаками злочинної змови та зловживання у сфері публічних закупівель.

Метадані стають особливо важливими у контексті банківського шахрайства, коли злочинці надсилають фішингові файли з шкідливими вкладеннями. Встановлення походження такого файлу дозволяє ідентифікувати, наприклад, регіон створення, IP-адресу, використовуване ПЗ. У межах співпраці з CERT-UA та міжнародними платформами (наприклад, MISP), ці відомості можуть бути оперативно інтегровані у більші розвідувальні бази (threat intelligence platforms).

Таким чином, аналіз метаданих відіграє критичну роль у доведенні зв'язку між цифровими об'єктами та суб'єктами правопорушення, дозволяє побудувати ланцюг подій, верифікувати достовірність цифрових доказів, а також інтегрувати ці дані в загальний масив OSINT-аналітики.

У межах кримінального провадження, відкритого у 2021 році за фактом шахрайства через низку фіктивних інвестиційних платформ, особливу роль відіграли відкриті джерела розвідувальної інформації (OSINT). У процесі аналітичного моніторингу було виявлено групу вебсайтів-клонів, які імітували популярні міжнародні брокерські сервіси, створюючи візуальну ідентичність за рахунок запозичення логотипів, дизайну та мовних шаблонів. Через аналіз WHOIS-реєстрацій, DNS-даних та IP-трасування встановлено, що доменні імена були зареєстровані на спільний пул IP-адрес, які належали одному хостинг-провайдеру в Центральній Європі.

Паралельно проводився OSINT-аналіз активності в соціальних мережах, де виявлено низку акаунтів у TikTok та YouTube, які просували фейкові платформи, обіцяючи «гарантований дохід» від вкладень у криптовалюту. За допомогою кросплатформного зіставлення цифрових профілів у LinkedIn, Telegram, Instagram та на спеціалізованих форумах,

ідентифіковано зв'язки між авторами контенту й працівниками невеликого IT-агентства, зареєстрованого у Варшаві, яке спеціалізується на маркетинговому аутсорсингу [4].

Вказана інформація, верифікована через міжнародні бази FININT та співпрацю з CERT-структурами, була використана для формування доказової бази, яка передана до міжнародної слідчої групи в межах реалізації механізмів Будапештської конвенції про кіберзлочинність. Отримані дані також сприяли блокуванню понад десяти фішингових доменів через спільну роботу з реєстраторами та ICANN.

Таким чином, цей випадок свідчить про важливість використання OSINT не лише для ідентифікації учасників злочинної діяльності, а й для виявлення системної мережевої інфраструктури, яка забезпечує функціонування транснаціональних шахрайських схем.

Застосування OSINT-методів у процесі розслідування фінансових правопорушень, вчинених з використанням цифрових технологій, супроводжується низкою комплексних проблем, що мають як правовий, так і організаційно-технічний характер. Однією з ключових є відсутність чіткого нормативного регулювання статусу відкритих джерел інформації у кримінальному процесі України. Дані, здобуті за допомогою OSINT, зокрема з WHOIS-сервісів, публічних реєстрів, платформ соціальних мереж або цифрових слідів на вебресурсах, не мають уніфікованого статусу щодо їх допустимості як доказів. Це ускладнює їх процесуальне закріплення та подальше використання у суді, що особливо проблематично у транскордонних провадженнях [1].

Крім того, значну складність становить верифікація автентичності зібраної інформації та атрибуція цифрових слідів, оскільки злочинці активно використовують засоби маскування, такі як VPN, TOR-мережі, підроблені домени або викривлення геолокації. Етична дилема полягає у тому, що збирання персоніфікованих даних з відкритих джерел може порушувати права особи на приватність, зокрема у контексті норм GDPR, що застосовуються до суб'єктів у країнах Європейського Союзу. Окрему проблему становить недостатній рівень цифрової підготовки слідчих та експертів у сфері криміналістичної OSINT-аналітики, а також відсутність алгоритмізованих процедур взаємодії з міжнародними слідчими структурами. Отже, для ефективного та правомірного використання OSINT-методів необхідне як оновлення процесуального законодавства, так і запровадження спеціалізованих навчальних програм для працівників правоохоронної сфери.

Запровадження OSINT-методів у практику розслідування фінансових правопорушень, вчинених із використанням цифрових технологій, потребує не лише технічної підготовки, а й належного нормативно-правового та методичного забезпечення. В умовах правової невизначеності щодо правового статусу даних, отриманих із відкритих джерел, особливо гостро постає проблема забезпечення їх допустимості як доказів у кримінальному провадженні. Відсутність усталених процесуальних механізмів фіксації, верифікації та атрибуції таких даних значно знижує їхню доказову цінність і створює ризики порушення прав учасників провадження. Саме тому актуальним є нормативне унормування OSINT-методів як джерела цифрових доказів з урахуванням вимог Кримінального процесуального кодексу України та міжнародних стандартів.

1. Створення спеціалізованих OSINT-підрозділів у складі правоохоронних органів. Ефективне використання відкритих джерел інформації (OSINT) потребує відповідної фахової підготовки, міждисциплінарного підходу та постійного моніторингу цифрового середовища. У зв'язку з цим актуальним є створення у структурі національної поліції, ДБР або Бюро економічної безпеки спеціалізованих аналітичних підрозділів, укомплектованих фахівцями у сфері інформаційних технологій, криміналістики, фінансів та права. Такі підрозділи забезпечуватимуть оперативне виявлення цифрових слідів, ідентифікацію суб'єктів фінансових схем, простеження руху активів та взаємозв'язків осіб. Подібна модель успішно реалізується в США (Cybercrime Task Forces), Німеччині (Zentrale Stelle für Finanztransaktio nsuntersuchungen) та Франції (OCLCTIC).

2. Розробка уніфікованих методичних підходів до збору та обробки відкритих цифрових даних. Системне нормативно-методичне забезпечення є ключовою умовою правомірного використання OSINT-інформації як джерела доказів. На сьогодні відсутність уніфікованих стандартів щодо фіксації, збереження та оцінки даних з відкритих джерел (зокрема метаданих, веб-контенту, цифрових профілів осіб) створює ризики визнання таких доказів недопустимими в судовому провадженні. У зв'язку з цим необхідно розробити і затвердити методичні

рекомендації та стандарти цифрової криміналістики, які б відповідали міжнародним практикам (наприклад, ISO/IEC 27037:2012) та враховували українську процесуальну специфіку.

3. Розбудова міжнародного обміну OSINT-даними в рамках співпраці з ЄС. Транскордонний характер цифрових фінансових злочинів зумовлює потребу у налагодженні механізмів міжнародної координації. Україна має долучитися до відповідних ініціатив ЄС, таких як Europol's European Cybercrime Centre (EC3), ENISA (Агентство ЄС з кібербезпеки), OLAF (Європейське бюро по боротьбі з шахрайством) тощо. Участь у спільних проєктах, обмін аналітичними продуктами та використання спільних платформ (як-от SIENA – Secure Information Exchange Network Application) підвищить оперативність реагування на схеми, що охоплюють декілька юрисдикцій, та забезпечить інтеграцію України в європейську систему кібербезпеки.

4. Впровадження освітніх програм для слідчих, експертів і суддів. Значна частина проблем пов'язана з недостатнім рівнем підготовки працівників системи кримінальної юстиції щодо правового режиму відкритих цифрових даних. Необхідно впровадити комплексні освітні програми на базі закладів вищої юридичної освіти, Національної школи суддів України, відомчих академій. Курси повинні охоплювати тематику: правові аспекти збору OSINT-даних, методи цифрового профілювання, верифікація інформації, етичні стандарти, стандарти допустимості доказів тощо. Підвищення цифрової та правової грамотності представників системи розслідування є необхідною передумовою ефективного впровадження інноваційних технологій у слідчу практику.

**Висновки.** Застосування OSINT-методів у розслідуванні кримінальних правопорушень у фінансовій сфері, вчинених з використанням цифрових технологій, становить перспективний напрям удосконалення криміналістичної практики в умовах стрімкої цифровізації. Результати аналізу засвідчують, що відкриті джерела інформації є потужним інструментом для виявлення суб'єктів правопорушень, простеження руху фінансових активів, розкриття структур шахрайських схем і документування цифрових слідів злочинної діяльності. Водночас, практична імплементація OSINT стикається з низкою проблем нормативно-правового, технічного й етичного характеру.

Для забезпечення ефективного та правомірного використання OSINT-даних у кримінальному процесі України доцільно: 1) нормативно закріпити статус відкритих цифрових джерел як доказів; 2) створити спеціалізовані OSINT-підрозділи з міждисциплінарною підготовкою; 3) запровадити уніфіковані методики збору, верифікації та обробки відкритих даних; 4) розвивати міжнародне співробітництво з європейськими організаціями в сфері кібербезпеки; 5) впровадити системну підготовку слідчих і суддів з цифрової криміналістики. Лише за умов комплексної модернізації підходів OSINT-аналітика зможе стати дієвим інструментом протидії фінансовій кіберзлочинності у цифрову добу.

**Список використаних джерел:**

1. Торбас О. О. OSINT при розслідуванні кримінальних правопорушень : підручник. Одеса : Юридика, 2024. 180 с.

2. Rao Komar. How to Digitally Verify Combatant Affiliation in Middle East Conflicts. Bellingcat : website. URL: https://www.bellingcat.com/resources/how-tos/2018/07/09/digitally-verify-middle-east-conflicts/

3. Як OSINT впливає на війну в Україні? Itedu : вебсайт. URL: https://itedu.center/ua/blog/articles/osint/

4. OSINT in Anti-Money Laundering (AML) Investigations : Unmasking Financial Shadows. Social Links : website. URL: https://blog.sociallinks.io/osint-in-anti-money-laundering-aml- investigations-unmasking-financial-shadows/

Дата першого надходження рукопису до видання: 06.11.2025
Дата прийнятого до друку рукопису після рецензування: 15.12.2025
Дата публікації: 31.12.2025