ISSN 2311-844X

УДК 658:336:343
DOI: https://doi.org/10.32782/2311-844X/2025-2-6

Ревак Ірина Олександрівна
доктор економічних наук, професор,
завідувач науково-дослідної лабораторії
OSINT-досліджень та безпекової аналітики,
Львівський державний університет внутрішніх справ
вулиця Городоцька, 26, Львів, 79000, Україна
ORCID: https://orcid.org/0000-0003-1755-2947

Підхомний Олег Михайлович
доктор економічних наук, професор,
професор кафедри фінансів, грошового обігу і кредиту,
Львівський національний університет імені Івана Франка
вулиця Університетська, 1, Львів, 79000, Україна
ORCID: https://orcid.org/0000-0003-2642-8657

ВІДКРИТІ ДЖЕРЕЛА ІНФОРМАЦІЇ В УПРАВЛІННІ КОРПОРАТИВНИМ САНКЦІЙНИМ КОМПЛАЄНСОМ ЛОГІСТИЧНИХ ПІДПРИЄМСТВ

Анотація. *У статті розглянуто проблему використання відкритих джерел інформації у системі управління корпоративним санкційним комплаєнсом логістичних підприємств. Підкреслено, що сучасні умови глобалізації та зростання санкційного тиску на міжнародну економіку формують потребу у посиленні прозорості ланцюгів постачання, підвищенні рівня контролю за контрагентами та запобіганні участі компаній у схемах обходу санкційних обмежень. Метою статті є обґрунтування ролі та класифікації відкритих джерел інформації у процесі управління корпоративним санкційним комплаєнсом логістичних підприємств, а також визначення критеріїв їх достовірності для забезпечення ефективного моніторингу та ухвалення управлінських рішень. Запропоновано класифікаційний підхід до систематизації відкритих джерел інформації за ознаками функціонального призначення, походження, рівня офіційності та технологічних можливостей збору даних. Встановлено, що відкриті джерела виконують базову функцію у корпоративному санкційному комплаєнсі, забезпечуючи виявлення ризиків, ідентифікацію порушень санкційного режиму, оцінку ділової репутації контрагентів та документування процесів перевірки. Наукова новизна полягає у розробленні системної класифікації відкритих джерел інформації, адаптованої до потреб санкційного комплаєнсу в логістиці, та у визначенні пріоритетності їх практичного застосування у різних типах управлінських рішень – стратегічних, тактичних, операційних та аналітико-прогностичних. Практичне значення дослідження полягає у можливості використання запропонованих підходів для формування внутрішньої політики комплаєнсу, удосконалення процедур перевірки контрагентів, розроблення автоматизованих систем моніторингу ризиків та підготовки фахівців у сфері інформаційної безпеки бізнесу. Зроблено висновок, що інтеграція відкритих джерел інформації у корпоративну систему санкційного комплаєнсу є необхідною умовою підвищення ефективності управління ризиками, забезпечення прозорості логістичних процесів та формування стійкої репутаційної політики підприємств на міжнародному ринку.*

Ключові слова: *OSINT, корпоративний санкційний комплаєнс, логістичні підприємства, управління ризиками, моніторинг клієнтів та контрагентів.*

Revak Iryna
Lviv State University of Internal Affairs
Pidkhomnyi Oleg
Ivan Franko National University of Lviv

OPEN SOURCES OF INFORMATION IN THE LOGISTICS ENTERPRISES CORPORATE SANCTIONS COMPLIANCE MANAGEMENT

Abstract. *The article examines the problem of using open-source information within the management system of corporate sanctions compliance in logistics enterprises. It emphasizes that under conditions of globalization and increasing sanctions pressure on the international economy, there is a growing need to enhance supply chain transparency, strengthen control over counterparties, and prevent companies from participating in schemes aimed at circumventing sanctions. The purpose of the study is to substantiate the role and classification of open-source information in corporate sanctions compliance management of logistics enterprises and to define criteria for its reliability to ensure effective monitoring and informed managerial decision-making. The author proposes a classification approach to the systematization of open-source information according to its functional purpose, origin, level of officiality, and technological capabilities of data collection. It is established that open sources perform a fundamental function in corporate sanctions compliance, providing risk identification, detection of sanctions violations, assessment of counterparties' business reputation, and documentation of compliance verification procedures. The scientific novelty lies in developing a systemic classification of open-source information adapted to the needs of sanctions compliance in logistics, as well as in determining the prioritization of its practical application across different types of managerial decisions – strategic, tactical, operational, and analytical-predictive. The practical significance of the study is the possibility of applying the proposed approaches to create internal compliance policies, improve counterparty verification procedures, develop automated risk monitoring systems, and train professionals in the field of business information security. It is concluded that the integration of open-source information into the corporate sanctions compliance system is a prerequisite for enhancing risk management efficiency, ensuring supply chain transparency, and strengthening the reputational resilience of enterprises in the international market.*

Keywords: *OSINT, corporate sanctions compliance, logistics enterprises, risk management, monitoring of clients and counterparties.*

Вступ. Підвищення санкційного тиску на міжнародну економіку, трансформація глобальних ланцюгів постачання та зростання вимог до прозорості бізнес-процесів обумовлюють потребу у формуванні дієвих механізмів корпоративного санкційного комплаєнсу. Для логістичних підприємств, які безпосередньо взаємодіють із великою кількістю контрагентів, державних і приватних структур у різних юрисдикціях, питання своєчасного виявлення санкційних ризиків набуває стратегічного значення. Ефективне управління комплаєнсом у цій сфері неможливе без системного використання відкритих джерел інформації, що дають змогу оперативно ідентифікувати ризикові зв'язки, відстежувати динаміку санкційних списків та перевіряти репутаційну надійність партнерів.

Актуальність дослідження зумовлена зростанням значення інформаційної аналітики в корпоративному управлінні та необхідністю переходу від формального виконання вимог санкційного контролю до побудови комплексної системи ризик-орієнтованого комплаєнсу. Відкриті джерела інформації стають не лише інструментом аналітичної підтримки, а й елементом стратегічного управління, який забезпечує прозорість прийняття рішень, відповідальність компанії перед міжнародними регуляторами та підтримання її ділової репутації.

Матеріали та методи. Питання застосування відкритих джерел інформації в системах корпоративного комплаєнсу перебуває на стадії формування та інституціоналізації. Наукові праці, присвячені комплаєнсу, здебільшого зосереджуються на фінансовому секторі або управлінні ризиками у банківській діяльності. Натомість дослідження, які комплексно розглядають OSINT як інструмент управління корпоративним санкційним комплаєнсом саме у сфері логістики, є поодинокими. Відсутність

ціліснoї класифікації відкритих джерел, орієнтованої на потреби логістичних компаній, ускладнює формування ефективних процедур перевірки контрагентів, моніторингу постачань та запобігання участі підприємств у санкційно-ризикових схемах.

Оглядовий аналіз наукової праці Гіоні Р., Таддео М., Флоріді Л. демонструє, що джерела відкритої інформації складають 80–90 % розвідданих в діяльності служб безпеки, при цьому швидке впровадження штучного інтелекту у процеси обробки таких даних породжує значущі соціально-етичні, правові та управлінські виклики [1]. У статті [6] автори пропонують класифікацію даних та інструментів збору відкритої інформації стосовно цифрових ідентичностей, яка може бути адаптована в контексті класифікації джерел інформації для санкційного комплаєнсу. Джерело «Використання OSINT для ідентифікації підсанкційних підприємств» висвітлює практичні підходи до використання відкритих джерел для ідентифікації зв'язків із підсанкційними суб'єктами, акцентуючи на складнощах виявлення афілійованих осіб і організацій та необхідності комплексного інструментарію перевірки [3].

У статті Мартінса К., Медейроса І. [2] представлено платформу AECCP, яка автоматично класифікує й корелює загрози на основі єдиної таксономії для поліпшення якості розвідданих, зібраних із відкритих джерел. Автори наукової праці [5] на основі трьох судових справ, журналістських матеріалів та інтерв'ю з правоохоронцями побудували crime script, який розкриває механізми обходу санкцій у постачанні товарів з Нідерландів до Росії, демонструє взаємозв'язок корпоративної, організованої та державної злочинності та окреслює напрями розроблення превентивних заходів. У публікації [4] розглянуто, як програмні рішення, засновані на використанні відкритих джерел інформації, можуть слугувати стратегічним інструментом забезпечення безпеки, прозорості та цифрової суверенності логістичних систем, з акцентом на правові, економічні та технологічні аспекти їх трансформації.

Як показує проведений аналіз, у наукових джерелах ґрунтовно розкрито загальні можливості використання відкритих джерел та штучного інтелекту в розвідувальній діяльності; описано підходи до систематичного пошуку ідентифікаційних даних у відкритому інтернет-просторі; наведено практичні алгоритми виявлення підсанкційних зв'язків через публічні дані, зокрема афілійованих осіб і посередників; представлено таксономії, розроблені для суміжних галузей, які доводять, що класифікація сприяє підвищенню якості даних; а також окреслено кримінологічні моделі обходу санкцій, що відображають складність багаторівневих схем і необхідність багатоджерельного моніторингу. У науковій літературі досі недостатньо розробленим залишається питання валідації та ранжування відкритих джерел інформації в контексті корпоративного санкційного комплаєнсу логістичних підприємств, зокрема щодо перетворення класифікаційних підходів на дієвий інструмент підтримки управлінських рішень.

Розроблення класифікації відкритих джерел інформації в управлінні корпоративним санкційним комплаєнсом логістичних підприємств здійснювалось із застосуванням низки взаємодоповнюючих наукових методів, що забезпечили її теоретичну обґрунтованість і логічну структурованість. Основу відповідного методичного підходу становили аналіз і синтез, які використано для узагальнення існуючих наукових підходів до структурування інформаційних ресурсів та виокремлення їх ознак за функціональними та правовими критеріями. Порівняльний метод дав змогу встановити відмінності між групами джерел за походженням, рівнем офіційності та технологічними властивостями. Структурно-функціональний метод застосовано для визначення місця і ролі кожного типу джерел у системі корпоративного комплаєнс-менеджменту, а класифікаційно-аналітичний метод – для формування системи класифікаційних ознак. Методи узагальнення й логічний забезпечили формування концептуальної єдності розробленої класифікації, а метод експертних оцінок – перевірку можливості її практичного застосування в управлінні санкційними ризиками логістичних підприємств. Системне використання цих методів

дало змогу створити науково обґрунтовану та придатну до практичної імплементації класифікацію відкритих джерел інформації у сфері санкційного комплаєнсу.

Метою статті є обґрунтування ролі відкритих джерел інформації в управлінні корпоративним санкційним комплаєнсом логістичних підприємств, розроблення класифікаційного підходу до їх систематизації та визначення критеріїв достовірності для підвищення ефективності управлінських рішень у сфері санкційного контролю.

Результати. Проведене дослідження відображає систематизоване узагальнення ключових тенденцій у застосуванні відкритих джерел інформації для забезпечення корпоративного санкційного комплаєнсу логістичних підприємств та розвитку їхнього інформаційно-аналітичного потенціалу. На основі вивчення наукових, нормативних та галузевих матеріалів виокремлено основні типи відкритих джерел, що забезпечують ідентифікацію, перевірку, правову оцінку та репутаційний аналіз контрагентів у межах корпоративних процедур дотримання санкційних вимог. Розроблена класифікація демонструє системний зв'язок між походженням, рівнем офіційності та функціональним призначенням інформації, що дає змогу підвищити точність моніторингу санкційних ризиків і адаптувати процеси управління комплаєнсом до сучасних вимог прозорості та міжнародної відповідності (табл. 1).

За функціональним призначенням відкриті джерела інформації, що використовуються в управлінні корпоративним санкційним комплаєнсом логістичних підприємств, поділяються на ідентифікаційні, верифікаційні, правові та репутаційно-аналітичні. Ідентифікаційні джерела забезпечують встановлення основних відомостей про контрагентів – юридичний статус, структуру власності, бенефіціарів, географію діяльності та участь у міжнародних ланцюгах постачання. Їх використання дозволяє виявляти потенційні зв'язки із підсанкційними структурами на початковому етапі аналізу ризиків. Верифікаційні джерела призначені для підтвердження достовірності та актуальності даних, отриманих на етапі ідентифікації, зокрема шляхом порівняння з офіційними санкційними списками, базами регуляторів, митними реєстрами чи судовими документами. Правові джерела охоплюють нормативно-правові акти, міжнародні договори, рішення санкційних органів і судових інстанцій, що визначають правовий статус суб'єктів і дають змогу оцінити законність взаємодії з ними. Репутаційно-аналітичні джерела формують уявлення про етичну, соціальну та корпоративну відповідальність контрагентів через аналіз публікацій у ЗМІ, розслідувань,

Таблиця 1

Ознаки класифікації відкритих джерел інформації в управлінні корпоративним санкційним комплаєнсом та їх ранжування за практичною значущістю

№	Ознака класифікації	Види
1	За функціональним призначенням	Ідентифікаційні джерела; Верифікаційні джерела; Правові джерела; Репутаційно-аналітичні джерела.
2	За походженням інформації	Державні та міждержавні ресурси; Корпоративні відкриті джерела; Медійні ресурси; Аналітичні матеріали; Джерела транспортної інформації; Соціальні мережі.
3	За рівнем офіційності	Первинні офіційні джерела; Комерційні та галузеві ресурси, створені на основі офіційних джерел; Неофіційні, але верифіковані джерела.
4	За технологічними можливостями збору та обробки	Статичні джерела; Динамічні джерела; Інтерактивні джерела.

Джерело: складено авторами

професійних рейтингів і соціальних мереж. Сукупне використання цих типів джерел забезпечує комплексність санкційного моніторингу, підвищує достовірність висновків OSINT-аналітики та зміцнює інформаційне підґрунтя для прийняття управлінських рішень у сфері корпоративного комплаєнсу.

За походженням інформації відкриті джерела, що застосовуються у корпоративному санкційному комплаєнсі логістичних підприємств, поділяються на державні та міждержавні ресурси, корпоративні відкриті джерела, медійні ресурси, аналітичні матеріали, джерела транспортної інформації та соціальні мережі. Державні та міждержавні ресурси охоплюють офіційні реєстри, санкційні списки, митну та судову статистику, а також публікації міжнародних організацій, які забезпечують високий рівень достовірності та юридичної верифікації даних. Корпоративні відкриті джерела включають інформацію про структуру власності, бенефіціарів, фінансову звітність і декларації компаній, що дає змогу оцінювати ризики співпраці з підсанкційними або афілійованими суб'єктами. Медійні ресурси формують додатковий інформаційний фон через публікації у ЗМІ, офіційні заяви компаній, журналістські розслідування та тематичні портали, які дозволяють виявляти непрямі ознаки обходу санкцій. Аналітичні матеріали, зокрема галузеві огляди, дослідження громадських організацій та OSINT-звіти, забезпечують системне розуміння тенденцій і механізмів санкційного впливу на логістичні потоки. Джерела транспортної інформації, такі як системи суднового трекінгу, митні бази та логістичні платформи, мають практичну цінність для відстеження руху товарів і транспортних засобів у режимі реального часу, що є критичним для виявлення схем обходу санкцій. Нарешті, соціальні мережі виступають динамічним каналом збору ознак ризикової поведінки суб'єктів, дозволяють фіксувати комунікації, зміни у власності чи діяльності, які не відображені в офіційних документах. Сукупне використання цих джерел створює комплексну інформаційну базу для управлінських рішень, підвищуючи ефективність системи санкційного комплаєнсу в логістичних компаніях.

За рівнем офіційності відкриті джерела інформації, що використовуються у корпоративному санкційному комплаєнсі логістичних підприємств, поділяються на первинні офіційні, комерційні та галузеві ресурси, створені на основі офіційних даних, а також неофіційні, але верифіковані джерела. Первинні офіційні джерела охоплюють державні та міждержавні реєстри, офіційні санкційні списки, нормативно-правові акти, судові рішення, публікації регуляторів і митних органів, що забезпечують найвищий рівень достовірності та мають юридичну силу для підтвердження або спростування санкційної відповідності контрагентів. Комерційні та галузеві ресурси формуються на основі відкритих офіційних даних, проте проходять додаткову аналітичну або технічну обробку – це, зокрема, агрегатори санкційних баз, платформи для моніторингу суден, логістичні аналітичні сервіси та системи корпоративного ризик-скорингу. Вони підвищують зручність доступу до інформації, дозволяють інтегрувати її в автоматизовані комплаєнс-процеси, хоча вимагають перевірки джерела походження даних. Неофіційні, але верифіковані джерела включають результати журналістських розслідувань, матеріали незалежних аналітичних центрів, експертні огляди та OSINT-звіти, які не мають офіційного статусу, але підтверджуються кількома незалежними джерелами та мають високу доказову цінність у практиці корпоративного аналізу ризиків. Такий багаторівневий підхід до класифікації джерел за рівнем офіційності забезпечує баланс між юридичною легітимністю, оперативністю отримання інформації та глибиною аналітичного опрацювання даних у системі санкційного комплаєнсу.

За технологічними можливостями збору та обробки інформації відкриті джерела, що використовуються у корпоративному санкційному комплаєнсі логістичних підприємств, поділяються на статичні, динамічні та інтерактивні. Статичні джерела містять фіксовану, малозмінну інформацію – офіційні реєстри, архіви фінансової звітності, публікації санкційних списків, судові рішення чи бази корпоративних даних. Їхня цінність полягає у стабільності та можливості ретроспективного аналізу, однак вони потребують регулярного оновлення для підтримання

актуальності. Динамічні джерела характеризуються постійним оновленням даних у режимі реального часу – це зокрема системи моніторингу суден (MarineTraffic, VesselFinder), митні та логістичні інформаційні потоки, агрегатори санкційних змін або автоматизовані новинні API. Вони забезпечують оперативність реагування на зміни в санкційних реєстрах і маршрутах постачання. Інтерактивні джерела поєднують ознаки попередніх двох типів і дають змогу користувачам здійснювати цільовий пошук, фільтрацію, порівняння та аналітичну візуалізацію даних у спеціалізованих OSINT-платформах. Такі джерела сприяють інтеграції відкритих даних у процеси ризик-скорингу, автоматизованого моніторингу контрагентів і прийняття управлінських рішень. Поєднання статичних, динамічних й інтерактивних джерел формує технологічну основу для створення комплексної системи інформаційної підтримки санкційного комплаєнсу в логістичних підприємствах.

У практиці корпоративного санкційного комплаєнсу достовірність інформації визначається поєднанням таких параметрів, як надійність інформаційних джерел (автентичність, незалежність, репутація), верифікаційна підтверджуваність (узгодженість, відтворюваність) та операційна актуальність (своєчасність, повнота, технічна цілісність).

Управлінські рішення в системі корпоративного санкційного комплаєнсу логістичних підприємств охоплюють чотири рівні, що відрізняються за масштабом, часовою перспективою та функціональною спрямованістю. Стратегічні рішення визначають загальну політику комплаєнсу, вибір партнерів та країн для співпраці й формують довгострокові межі дотримання санкційних норм. Тактичні рішення спрямовані на організацію процесів моніторингу та перевірки контрагентів, коригування маршрутів постачань і внутрішніх процедур контролю. Операційні рішення реалізуються на рівні щоденної діяльності, включаючи блокування угод із ризиковими контрагентами, зміну логістичних маршрутів та адаптацію банківських і страхових умов. Аналітико-прогностичні рішення забезпечують оцінку й передбачення потенційних санкційних ризиків, моделювання сценаріїв розвитку подій та розробку превентивних заходів для підвищення ефективності управління ризиками й мінімізації можливих втрат підприємства.

Таким чином, тип управлінського рішення в системі корпоративного санкційного комплаєнсу прямо залежить від глибини, достовірності та своєчасності інформації, отриманої з відкритих джерел. Ефективне використання OSINT дозволяє логістичним підприємствам не лише реагувати на санкційні обмеження, а й передбачати ризики, формувати адаптивні стратегії та підтримувати репутаційну стійкість на міжнародних ринках.

Висновки. Проведене дослідження засвідчило, що відкриті джерела інформації є важливим елементом системи корпоративного санкційного комплаєнсу логістичних підприємств, оскільки вони забезпечують своєчасне виявлення ризиків, пов'язаних із клієнтами, контрагентами, маршрутами постачання та юрисдикційними обмеженнями. Використання таких джерел сприяє підвищенню прозорості бізнес-процесів, удосконаленню управлінських механізмів дотримання санкційних вимог і посиленню фінансової безпеки в логістичних ланцюгах.

Розроблена класифікація відкритих джерел за походженням, рівнем офіційності, функціональним призначенням і технологічними можливостями сприятиме систематизації різнорідних інформаційних потоків та визначенню їх ролі у процесах корпоративного контролю. Вона забезпечує концептуальну основу для оцінювання достовірності даних, ідентифікації та верифікації контрагентів, а також формування аналітичних рішень у системі управління санкційними ризиками.

Отримані результати мають як теоретичне, так і прикладне значення, створюючи передумови для вдосконалення корпоративних політик комплаєнсу, розроблення внутрішніх процедур перевірки клієнтів, контрагентів і впровадження аналітичних інструментів автоматизованого моніторингу. Перспективним напрямом подальших досліджень є розроблення моделей оцінювання вагомості більш деталізованих типів відкритих джерел у процесі прийняття комплаєнс-рішень та алгоритмів їх інтеграції у цифрові системи управління ризиками логістичних підприємств.

Список використаних джерел:

1. Ghioni R., Taddeo M., Floridi L. Open source intelligence and AI: a systematic review of the GELSI literature. *AI & SOCIETY*: веб-сайт. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC9883130/ (дата звернення: 30.10.2025)
2. Martins C., Medeiros I. Generating Quality Threat Intelligence Leveraging OSINT and a Cyber Threat Unified Taxonomy. *ACM Transactions on Privacy and Security*. Vol. 25, No. 3. Article 19: веб-сайт. URL: https://dl.acm.org/doi/pdf/10.1145/3530977 (дата звернення: 30.10.2025)
3. Nihad A. Hassan Using OSINT to identify sanctioned entities: веб-сайт. URL: https://authentic8.com/blog/using-osint-identify-sanctioned-entities (дата звернення: 20.10.2025)
4. Plevnik M., Gumzej R. Open Source as the Foundation of Safety and Security in Logistics Digital Transformation. *Systems.* 2025. 13, 424: веб-сайт. URL: https://www.mdpi.com/2079-8954/13/6/424 (дата звернення: 30.10.2025)
5. Santvoord V.D., Visser N. Scripting the evasions of sanctions: A case analysis of the circumvention of sanctions on the supply of goods to Russia from the Netherlands. *Journal of Economic Criminology*: веб-сайт. URL: https://www.sciencedirect.com/science/article/pii/S2949791425000533 (дата звернення: 30.10.2025)
6. Walkow M., Pöhn D. Systematically Searching for Identity-Related Information in the Internet with OSINT Tools: веб-сайт. URL: https://ar5iv.labs.arxiv.org/html/2407.16251 (дата звернення: 20.10.2025)

References:

1. Ghioni R., Taddeo M., Floridi L. (2023) Open source intelligence and AI: a systematic review of the GELSI literature. *AI & SOCIETY.* Available at: https://pmc.ncbi.nlm.nih.gov/articles/PMC9883130/ (accessed 30 October, 2025)
2. Martins C., Medeiros I. (2022) Generating Quality Threat Intelligence Leveraging OSINT and a Cyber Threat Unified Taxonomy. *ACM Transactions on Privacy and Security.* Vol. 25, No. 3. Article 19. Available at: https://dl.acm.org/doi/pdf/10.1145/3530977 (accessed 30 October, 2025)
3. Nihad A. Hassan (2023) Using OSINT to identify sanctioned entities. Available at: https://authentic8.com/blog/using-osint-identify-sanctioned-entities (accessed 20 October, 2025)
4. Plevnik M., Gumzej R. Open Source as the Foundation of Safety and Security in Logistics Digital Transformation. *Systems.* 2025. 13, 424. Available at: https://www.mdpi.com/2079-8954/13/6/424 (accessed 30 October, 2025)
5. Santvoord V.D., Visser N. (2025) Scripting the evasions of sanctions: A case analysis of the circumvention of sanctions on the supply of goods to Russia from the Netherlands. *Journal of Economic Criminology*. Available at: https://sciencedirect.com/science/article/pii/S2949791425000533 (accessed 30 October, 2025)
6. Walkow M., Pöhn D. (2024) Systematically Searching for Identity-Related Information in the Internet with OSINT Tools. Available at: https://ar5iv.labs.arxiv.org/html/2407.16251 (accessed 20 October, 2025)

Стаття надійшла: 31.10.2025
Стаття прийнята: 17.11.2025
Стаття опублікована: 22.01.2026