

Правоохоронна діяльність та національна безпека

УДК 351.74:004.738.5

DOI <https://doi.org/10.5281/zenodo.15086041>

**Генезис інструментів OSINT та окремі аспекти їх використання
у правоохоронній діяльності**

Басалик Сергій Анатолійович

кандидат юридичних наук, доцент кафедри спеціальних дисциплін, факультету
правоохоронної діяльності, Національної академії Державної прикордонної
служби України імені Богдана Хмельницького, місто Хмельницький, вулиця
Шевченка, 46, 29001, Україна, nadpsu@dpsu.gov.ua,
<https://orcid.org/0000-0002-4060-8673>

Туз Олександр Сергійович

кандидат психологічних наук, доцент кафедри спеціальних дисциплін,
факультету правоохоронної діяльності, Національної академії Державної
прикордонної служби України імені Богдана Хмельницького, місто
Хмельницький, вулиця Шевченка, 46, 29001, Україна, nadpsu@dpsu.gov.ua,
<https://orcid.org/0000-0003-3879-4013>,
Web of Science ResearcherID: MHR-5048-2025

Тищук Віктор Володимирович

доктор філософії у галузі права, доцент кафедри спеціальних дисциплін,
факультету правоохоронної діяльності, Національної академії Державної
прикордонної служби України імені Богдана Хмельницького, місто
Хмельницький, вулиця Шевченка, 46, 29001, Україна, nadpsu@dpsu.gov.ua,
<https://orcid.org/0000-0001-5811-5909>, Web of Science ResearcherID: IUP-1772-
2023, Scopus Author ID: 58791413300

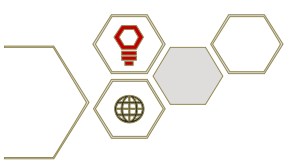


Прийнято: 11.03.2025 | Опубліковано: 25.03.2025

***Анотація.** У статті здійснюється аналіз генезису та еволюції інструментів OSINT (Open Source Intelligence) з акцентом на їх застосування у правоохоронній діяльності. Дослідження базується на комплексі загальнонаукових і спеціальних методів, зокрема аналізі, синтезі, порівняльно-правовому методі та контент-аналізі, що дозволило не лише оцінити історичний розвиток, а й визначити основні проблеми нормативного регулювання у цій сфері. На основі отриманих результатів підтверджено робочі гіпотези щодо становлення, еволюції та інтеграції OSINT у правоохоронну практику.*

Безсумнівно, що початкові форми OSINT, які виникли із діяльності ентузіастів та ранньої розвідки з відкритих джерел, поступово трансформувалися у потужний інструмент аналітики, здатний охоплювати широкий спектр завдань – від виявлення загроз до аналізу криміногенної ситуації. Проте невизначеність правового статусу цього інструменту стримує повноцінну інтеграцію до офіційних процесів правоохоронних органів. Подальша еволюція OSINT супроводжувалася розширенням функціональних можливостей, що сприяло впровадженню новітніх цифрових технологій, але одночасно викликало питання захисту персональних даних і дотримання прав людини, оскільки відсутність чітких правових меж створює ризики порушення основних свобод громадян.

Крім того, з огляду на збройну агресію проти України, традиційні заходи правоохоронної діяльності виявляються недостатніми, тому інтеграція OSINT як системного компонента пошукової роботи правоохоронних органів набуває особливого значення. У результаті, запропоновано створення спеціалізованих підрозділів, розробку єдиних стандартів для збору, перевірки та використання відкритої інформації, а також впровадження механізмів аналізу даних, прогнозування правопорушень та стратегічного планування у сфері забезпечення національної безпеки. Таким чином, комплексний підхід до аналізу



генезису та розвитку OSINT, разом із визначенням основних проблем нормативного регулювання і сучасних викликів, дозволяє сформулювати обґрунтований та актуальний підхід до удосконалення застосування в умовах глобальних та локальних загроз.

Ключові слова: *розвідка з відкритих джерел, правоохоронна діяльність, національна безпека.*

Genesis of OSINT Tools and Specific Aspects of Their Use in Law Enforcement

Basalyk Serhii Anatoliiovych

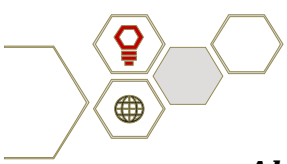
Candidate of Legal Sciences, Associate Professor of the Department of Special Disciplines, Faculty of Law Enforcement, Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, Khmelnytskyi, Shevchenko Street, 46, 29007, Україна, nadpsu@dpsu.gov.ua, <https://orcid.org/0000-0002-4060-8673>

Tuz Oleksandr Serhiiovych

Candidate of Psychological Sciences, Associate Professor of the Department of Special Disciplines, Faculty of Law Enforcement, Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, Khmelnytskyi, Shevchenko Street, 46, 29007, Ukraine, nadpsu@dpsu.gov.ua, <https://orcid.org/0000-0003-3879-4013>, Web of Science ResearcherID: MHR-5048-2025

Tyshchuk Viktor Volodymyrovych

PhD of Law, Associate Professor of the Department of Special Disciplines, Faculty of Law Enforcement, Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, Khmelnytskyi, Shevchenko Street, 46, 29007, Ukraine, nadpsu@dpsu.gov.ua, <https://orcid.org/0000-0001-5811-5909>, Web of Science ResearcherID: IUP-1772-2023, Scopus Author ID: 58791413300

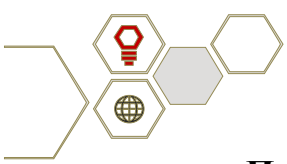


Abstract. *The article analyzes the genesis and evolution of OSINT (Open Source Intelligence) tools, focusing on their application in law enforcement. The study is based on a combination of general scientific and specialized methods, including analysis, synthesis, comparative legal process, and content analysis, which allowed not only for an assessment of historical development but also for identifying key issues in regulatory frameworks in this field. Based on the obtained results, the working hypotheses regarding the emergence, evolution, and integration of OSINT into law enforcement practice have been confirmed.*

Undoubtedly, the initial forms of OSINT, which emerged from enthusiasts and early open-source intelligence efforts, have gradually transformed into a powerful analytical tool capable of addressing a wide range of tasks—from threat detection to the analysis of the criminogenic situation. However, the undefined legal status of this tool hinders its full integration into official law enforcement processes. The further evolution of OSINT has been accompanied by expanding its functional capabilities, facilitating the adoption of advanced digital technologies. At the same time, it has raised concerns regarding personal data protection and human rights compliance, as the lack of clear legal boundaries creates risks of violating fundamental civil liberties.

Furthermore, given the armed aggression against Ukraine, traditional law enforcement measures have proven insufficient, making the integration of OSINT as a systemic component of law enforcement intelligence work particularly significant. As a result, the article proposes the establishment of specialized units, developing unified standards for collecting, verifying, and utilizing open-source information, and implementing mechanisms for data analysis, crime prediction, and strategic planning in the field of national security. Thus, a comprehensive approach to analyzing the genesis and development of OSINT, along with identifying key regulatory issues and contemporary challenges, enables the formation of a well-founded and relevant strategy for its enhancement in the context of global and local threats.

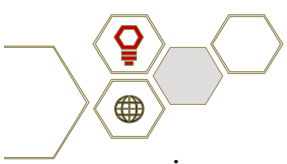
Keywords: *Open-Source Intelligence, Law enforcement activity, National Security.*



Постановка проблеми. Open Source Intelligence (OSINT) як комплекс інструментів збору інформації на основі відкритих джерел набуває важливого значення у правоохоронній діяльності. Використання OSINT дозволяє виявляти потенційні загрози, аналізувати великі бази даних (Big Data) та забезпечувати оперативне реагування на правопорушення. Проте правові аспекти її застосування залишаються недостатньо врегульованими, що створює виклики для правоохоронних органів.

Значення OSINT суттєво зростає на фоні сучасних реалій інформаційних війн та гібридних загроз, які стали невід'ємною частиною міжнародних конфліктів, зокрема у контексті повномасштабного вторгнення країни-агресора в Україну. Це зумовлено швидким розвитком цифрових технологій, які дозволяють здійснювати моніторинг та аналіз інформації в реальному часі. Тому, вивчення генезису OSINT не лише допомагає зрозуміти її еволюцію, але й дає змогу вказати на інструменти, які можуть бути використані для протидії сучасним безпековим викликам, таким як боротьба з організованою злочинністю та злочинами проти основ національної безпеки.

Аналіз останніх досліджень і публікацій. У процесі дослідження генезису OSINT та її застосування у правоохоронній діяльності нами було проаналізовано низку наукових праць, серед яких роботи таких дослідників як О. Ангельська [1], О. В. Дикий [2], Думчиков М. О. [3], А. Главацька [1], М. М. Горбач, М. Кирстя, А. О. Кисельов [4], О. Є. Користін [5], Т. І. Коробейнікова [6], С. О. Мартинюк, І. М. Містерман, Є. Є. Міщенко, І. Опірський [1], Н. П. Свиридюк [5], М. М. Серватнюк, В. В. Сидорчук [2], І. А. Симак [6], Р. М. Синеколодезький [4], Т. Федоренко та інших вчених, що стали фундаментом для подальшого аналізу. Зокрема, Н. В. Жмур та М. П. Землянікіна висвітлюють еволюцію OSINT та сучасні інструменти пошуку інформації, що сприяє розумінню інтеграції у правоохоронну діяльність [7]. Дослідження D. Van Puuyvelde та F. Rienzi Tabárez пропонує концептуальну рамку сучасної OSINT, підкреслюючи виклики перевантаження інформацією та питання достовірності даних, що створює основу для дискусій про розбіжності у



підходах до збору та аналізу інформації [8]. Робота А. Yadav, А. Kumar та V. Singh також зосереджена на технологічних інноваціях, зокрема методах машинного та глибинного навчання, для покращення використання OSINT [9]. Практичний poradnik Д. С. Зоренка, Р. В. Леха, Д. О. Кулика та О. І. Червякова [10] демонструє методологічні підходи до збору, аналізу та систематизації інформації з відкритих джерел, що є важливим для оперативно-розшукової діяльності, досудового та судового слідства. Нарешті, Ю. О. Виходець та Г. К. Тетерятник розглядають специфіку застосування OSINT під час бойових дій, акцентуючи на правових та методичних розбіжностях, які можуть спричиняти різночитання отриманих даних [11]. Аналіз цих робіт демонструє, що дослідницькі підходи не лише взаємодоповнюють один одного, але й свідчать про нагальну потребу гармонізації інструментів OSINT для розробки стратегії їх застосування у правоохоронній діяльності. Особливо це актуально в умовах збройної агресії проти України, що в комплексі сприяло формуванню власного підходу до вирішення поставленої проблеми [12].

Виділення невирішених раніше частин загальної проблеми. У сучасних дослідженнях та нормативно-правовій базі, що стосуються OSINT, виявлено кілька аспектів, які потребують подальшого вивчення та уточнення. Зокрема, в Україні відсутні чітко визначені положення, що регулюють порядок використання OSINT у діяльності правоохоронних органів. Крім того, генезис відповідних інструментів, що виник унаслідок стрімкого розвитку інформаційних технологій та зростання обсягів відкритих даних, є важливим чинником, який вимагає узгодження з чинним законодавством.

Крім того, проблема захисту персональних даних під час використання відкритої інформації залишається невирішеною. Недостатня увага до цього аспекту може призвести до ризиків, пов'язаних із порушенням прав людини. Наразі відсутні чіткі критерії, що регламентують застосування відкритої інформації під час досудового та судового розслідування, а також оперативно-розшукової діяльності [13]. Такі прогалини у нормативно-правовому регулюванні в Україні обумовлені відсутністю ретроспективного та



теоретичного підходу до цієї проблематики, що пов'язано зі стрімким розвитком технологій, які значно випереджають можливості існуючих правових норм.

Невирішені питання щодо використання OSINT мають безпосередній вплив на розвиток законодавства та впровадження відповідних інструментів. Для регулювання цієї сфери необхідно забезпечити баланс між підвищенням ефективності правоохоронної діяльності та захистом основних прав і свобод громадян.

Метою даної статті є дослідження напрямків регулювання використання OSINT правоохоронними органами з урахуванням процесу формування та розвитку інструментів, що з'явилися завдяки стрімкому розвитку цифрових технологій та зростанню обсягу відкритих даних.

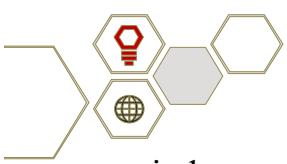
Формулювання цілей статті (постановка завдання). Досліджуючи розвиток інструментів OSINT, необхідно визначити наступні завдання, які сприятимуть їх інтеграції у правоохоронну діяльність з урахуванням правових викликів:

Завдання:

- 1) дослідити еволюцію інструментів OSINT, зокрема визначити етапи їх розвитку та підходи до збору та аналізу відкритої інформації у правоохоронній діяльності;
- 2) розглянути правові аспекти використання OSINT, виявити прогалини в чинному законодавстві, що обмежують застосування цих інструментів правоохоронними органами.

Актуальність дослідження обумовлена необхідністю пристосування національної правової системи до швидкого розвитку технологій, зокрема інструментів OSINT, що стають важливим елементом у правоохоронній діяльності. Тому, враховуючи потенціал цих інструментів для правоохоронних органів, особливо в контексті боротьби з організованою злочинністю, виникає потреба у вивченні та узгодженні правового забезпечення даної сфери.

Виклад основного матеріалу дослідження. Розвідка на основі відкритих джерел, має глибоке історичне коріння, яке тісно переплітається з розвитком

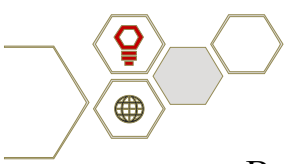


інформаційних технологій. Вона розвивалася з обмежених способів збору та аналізу інформації, що доступна публічно, до одного з основних інструментів у сучасній правоохоронній та безпековій діяльності [2]. Генезис OSINT можна простежити через етапи технологічного розвитку – від простих відкритих джерел (таких як преса та публікації) до Інтернету та соціальних мереж, що нині є основним джерелом збору даних для правоохоронних органів та спеціальних служб [14].

Незважаючи на те, що OSINT виникла у середовищі спеціальних служб і був спершу спрямований на забезпечення національної безпеки, її застосування значно розширилося. Тобто, фокус поступово зміщувався з обмеженого збору інформації про зовнішні загрози до активного використання для внутрішніх оперативних потреб. У результаті, на сьогоднішній день OSINT активно використовується правоохоронними органами для збору інформації, що допомагає у кримінальних розслідуваннях та аналізі протиправної діяльності. Проте, важливо зазначити, що цей інструмент має залишатися лише частиною більш широкої стратегії збору інформації і не повинен ототожнюватися, наприклад, з кримінальним аналізом, який є формою інформаційно-аналітичної роботи.

У цьому контексті необхідно зазначити, що попри здатність значно підвищувати ефективність збору та аналізу інформації, цей інструмент не може розглядатися як самодостатній спосіб боротьби зі злочинністю. Тому OSINT повинна доповнювати традиційні методи кримінального аналізу, оперативно-розшукової діяльності, судового та досудового слідства чи міжвідомчої взаємодії, формуючи комплексний підхід до отримання й обробки даних у правоохоронній сфері.

Особливо це стосується сучасних реалій, зокрема, коли активні бойові дії, посилюють загрози національній безпеці. Під час повномасштабного вторгнення країни-агресора, OSINT стала одним із ключових інструментів у боротьбі з окупантом, оскільки дозволяє не лише відстежувати окремі елементи дій ворога, а й виявляти та запобігати ворожим гібридним атакам.



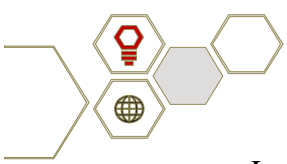
Вищезазначене підтверджує значення OSINT у протидії злочинам, що загрожують національній безпеці, та боротьбі з організованими злочинними угрупованнями, які можуть діяти на користь ворога або дестабілізувати ситуацію. Отже, з огляду на зростаючу роль OSINT у правоохоронній діяльності, важливо розробити чіткі правові норми для регулювання збору, зберігання та використання даних з відкритих джерел.

Методологія дослідження включає аналіз етапів розвитку OSINT, правових норм, що регулюють її застосування, а також вивчення національної та міжнародної практики застосування цього інструменту в умовах боротьби з організованою злочинністю та загрозами у сфері національної безпеки. Крім того, значну увагу було приділено аналізу використання відкритих джерел інформації та можливих негативних наслідків, таких як порушення прав людини. У процесі дослідження було виявлено, що існуючі правові норми не завжди відповідають швидкозмінним технологіям та вимогам сучасної безпеки, що потребує їх вдосконалення для забезпечення правомірності використання OSINT.

На основі отриманих результатів висунуто кілька робочих гіпотез щодо становлення, еволюції та впровадження OSINT у правоохоронну практику.

Витоки та становлення. Початкові форми OSINT еволюціонували із діяльності ентузіастів та розвідки з відкритих джерел до потужного інструменту аналітики. Використання розвідки з відкритих джерел поступово охоплювало все ширший спектр завдань – від виявлення загроз до аналізу криміногенної ситуації. Однак правовий статус цього інструменту досі чітко не визначений, що стримує інтеграцію до офіційних процесів правоохоронної діяльності.

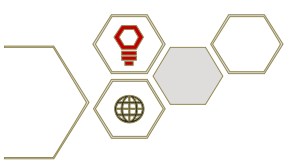
Еволюція та вдосконалення. Розширення функціональних можливостей OSINT супроводжувалося новими викликами, зокрема у сфері захисту персональних даних. Відсутність чітких правових меж використання відкритих джерел створює ризики порушення прав і свобод громадян. Регулювання на законодавчому рівні є необхідним для врівноваження державних інтересів та гарантування дотримання прав людини під час збору, обробки й використання інформації.



Інтеграція у правоохоронну діяльність. Перетворення OSINT на системний компонент пошукової роботи правоохоронних органів дозволяє оперативно реагувати на загрози вчинення злочинів проти основ національної безпеки, що посилюються внаслідок збройної агресії проти України. Інституціоналізація у правоохоронній практиці сприятиме створенню механізмів аналізу відкритих даних, прогнозування правопорушень та стратегічного планування у сфері забезпечення національної безпеки.

Обговорення. Перші кроки розвитку технологій OSINT можна відслідкувати ще з кінця 1941 року, коли в США була створена служба моніторингу зарубіжних трансляцій для аналізу радіопрограм, що дозволило виявляти несподівані зв'язки в публічних даних. За даними дослідників Н. В. Жмура та М. П. Землянікіної, сучасну історію OSINT умовно можна розділити на три етапи. Перший етап (2005-2009 роки) відзначається виникненням центрів аналізу відкритих джерел на фоні стрімкого зростання обсягу даних в Інтернеті, що заклало фундамент сучасних інструментів OSINT. Другий етап (2009–2016 роки) характеризується встановленням нових стандартів доступності інформації завдяки швидкому розвитку цифрових технологій, а з 2017 року відбувається активна інтеграція не лише в оборонну, але й у політичну, економічну та правоохоронну сфери за допомогою впровадження інструментів Business Intelligence, Knowledge Management та інтегрованих процесів типу JISR, що забезпечують своєчасне збирання, обробку та поширення аналітичних даних для підтримки прийняття рішень [7, с. 96-100].

Історія розвитку OSINT отримує дещо інший погляд у роботі М. О. Думчикова, який вважає, що її еволюція як інструменту розвідувальної діяльності почалась наприкінці 1980-х років. Саме тоді американські військові вперше запровадили цей термін у сучасному розумінні в контексті реформування розвідувальних структур та пристосування до нових інформаційних викликів. Важливим етапом становлення стає рішення Комісії Американського розвідувального співтовариства (Комісії Аспіна-Брауна) у 1996 році, яка офіційно визнала необхідність активного використання відкритих джерел для

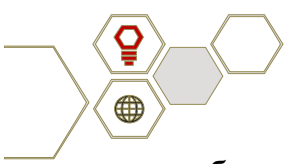


покращення розвідувальної діяльності. У цей самий період НАТО розробило довідники з OSINT, що містили практичні рекомендації щодо збору та аналізу відкритої інформації. Наприкінці 1990-х років OSINT стала невід'ємною частиною роботи урядових установ та міжнародних організацій, таких як НАТО, що сприяло її інтеграції в сферу безпеки та стратегічного планування [3, с. 3-4].

Дослідження D. Van Puuyvelde та F. Tabárez Rienzi аналізує сучасний стан OSINT, визначаючи її як процес збору, аналізу та поширення інформації з відкритих або комерційно доступних джерел. Вони звертають увагу на основні виклики для OSINT, зокрема перевантаженість інформацією, надійність даних та етичні питання, а також дискутують щодо її статусу як окремої дисципліни чи складової розвідувальної діяльності. Дана праця також вказує на роль комерційних організацій у розвитку OSINT та необхідність удосконалення правового регулювання. Крім того, автори наголошують на необхідності подальших досліджень щодо правових аспектів, соціологічних факторів, що сприяють поширенню OSINT, зокрема взаємозв'язків між спільнотами дослідників та активістами у сфері ІТ-технологій [8, с. 13-15].

A. Yadav та ін. підкреслюють важливість розвитку нових підходів до інтеграції OSINT в різні галузі, зокрема в правоохоронну діяльність. Автори акцентують увагу на доцільності більш глибокого вивчення зв'язків між OSINT і розвідувальними заходами, а також на можливостях використання відкритих джерел для покращення результатів у сфері правоохоронної діяльності, зокрема у таких сферах як визначення моделей поведінки (або кримінологічних профілів) правопорушників [9, с. 12431].

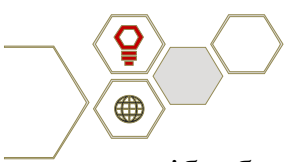
Українські вчені Д. С. Зоренко та ін. розглядають OSINT як процес пошукової роботи, що включає кілька етапів: визначення вихідних даних та мети пошуку, вибір інструментів і заходів (пасивний чи активний пошук), збір та систематизація інформації, а також формулювання висновків на основі отриманих даних. На їхню думку, творчий підхід до вибору ключових слів, комбінування різних варіантів пошуку та критичне ставлення до надійності джерел є важливими для досягнення результату. Вчені також підкреслюють



проблеми роботи з великими обсягами даних, необхідність верифікації інформації та високі вимоги до кваліфікації аналітиків. Такий підхід дозволяє розкрити чітку картину об'єкта дослідження, що допомагає приймати обґрунтовані рішення [10, с. 6-7].

В умовах збройної агресії проти України, що триває з 2014 року та отримала ескалацію з 24 лютого 2022 року, правоохоронні заходи часто недоступні через окупацію частин території, тому OSINT стає важливим інструментом розслідування воєнних злочинів. Використовуючи дані з соціальних мереж, публічних баз, медіа та відкритих месенджерів, фахівці забезпечують збір, класифікацію та аналіз доказів (фото-, відеоматеріал, геодані, метадані та ін.), які потім використовуються як у національних судах, так і в Міжнародному кримінальному суді. Приклади ефективного застосування OSINT – розслідування збиття рейсу MH17 та ідентифікація російських військових за даними з відкритих джерел – підтверджують практичну цінність даної методики, попри виклики, пов'язані з обробкою великих обсягів даних (Big Data), їх «шумом» та забезпеченням достовірності зібраної інформації [11, с. 70-73].

Цікавим є дослідження А. Главацької та ін., яке підтверджує, що OSINT є ефективним інструментом аналізу відкритих джерел, здатним ідентифікувати особу за цифровими слідами, які вона залишає в мережі. Автори встановили, що використання соціальних мереж, відкритих державних реєстрів, медіа порталів та геолокаційних даних дозволяє отримати конфіденційну інформацію без згоди власника. Основними ризиками є можливість маніпуляцій, дезінформації, кіберзлочинності та незаконного стеження, що може використовуватися як у кримінальних цілях, так і у воєнних конфліктах. Автори доходять висновку, що OSINT має подвійний характер: з одного боку, вона є цінним інструментом для правоохоронних органів або, навіть, журналістських розслідувань, а з іншого – становить загрозу конфіденційності громадян. Основними проблемами є відсутність правового регулювання щодо збору та використання OSINT-даних, недостатня цифрова грамотність населення та можливість зловживань у сфері



кібербезпеки. Це вимагає розробки механізмів контролю, які б запобігали незаконному використанню відкритих даних [1].

Наступна таблиця висвітлює законодавчі підстави, обмеження та проблеми використання відкритих джерел інформації:

Правові аспекти та особливості застосування OSINT
у правоохоронній діяльності [4]

Аспект	Зміст	Нормативна база
Законодавче врегулювання отримання інформації	Законодавчо передбачені способи отримання первинної оперативно-розшукової інформації через оперативний пошук [15]	Закон України “Про оперативно-розшукову діяльність” (ст. 7, 8)
Відсутність правового регулювання OSINT	Законодавство не передбачає окремого правового механізму для здійснення моніторингу відкритих джерел	Відсутність законодавчих норм, які регулюють OSINT у правоохоронній діяльності
Використання OSINT приватними суб’єктами	OSINT застосовується організаціями приватного сектору (журналістами, приватними детективами, ІТ-компаніями) [5]	Діяльність OSINT-суб’єктів поза державними органами не врегульовано
Загрози для конфіденційності	Систематичний збір даних без згоди особи може кваліфікуватися як порушення права на недоторканність приватного життя [6]	ЄСПЛ, справа “С. Віберг проти Швеції” (06.06.2006 р.), ст. 8 Конвенції про захист прав людини та основних свобод 1950 р.
Обмеження збору інформації поліцією	Правоохоронні органи мають право збирати інформацію лише в межах, визначених законом	Закон України “Про оперативно-розшукову діяльність” (ст. 9), КПК України (ч. 3 ст. 214)
Проблеми досудового розслідування	Здійснення слідчих (розшукових) дій до відкриття кримінального провадження не допускається	КПК України (ч. 3 ст. 214)



Принципи отримання інформації OSINT	Загальні принципи: законність, верховенство права, презумпція невинуватості. Відомчі принципи: безперервність, відкриті та негласні дії	Загальні правові стандарти та внутрішньовідомчі інструкції правоохоронних органів
-------------------------------------	---	---

Таким чином, у ході дослідження нами було підтверджено висунуті гіпотези та встановлено, що OSINT еволюціонувала від неформального збору інформації до аналітичного інструменту, здатного охопити широкий спектр завдань. Проте, незважаючи на розширення функціональних можливостей, її правовий статус залишається невизначеним, що ускладнює інтеграцію у процесуальну діяльність правоохоронних органів. Крім того, систематичний збір відкритої інформації створює ризики порушення конфіденційності, що потребує розробки чітких нормативних механізмів для врівноваження державних інтересів та прав громадян.

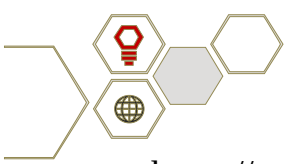
Висновки. Отже, одним із основних результатів дослідження є виявлення необхідності комплексного підходу до використання OSINT. Фрагментарність і нечіткість правових норм у цій сфері ускладнюють його ефективне застосування у правоохоронній діяльності. Тому для підвищення результативності доцільно створювати спеціалізовані підрозділи, розробляти єдині стандарти збору, перевірки та використання відкритих даних, а також впроваджувати аналітичні механізми прогнозування правопорушень.

У зв'язку з цим, погоджуючись з висновками А. Главацької та ін. [1], доцільно буде обмежувати публічний доступ до персональної інформації, підвищувати рівень цифрової безпеки користувачів та впроваджувати заходи захисту від OSINT-загроз. Для правоохоронних органів пропонується активніше використовувати OSINT для боротьби з кіберзлочинністю та передбачити відповідні законодавчі норми. Крім того, необхідно посилити міжнародну співпрацю для розробки єдиних стандартів використання OSINT та запровадження механізмів контролю за обробкою персональних даних.



Список використаних джерел

1. Главацька А., Ангельська О., Опірський І. Дослідження технології використання OSINT як нової загрози з деанонізації особи в інтернет просторі. *Електронне фахове наукове видання “Кібербезпека: освіта, наука, техніка”*. 2024. № 1 (25), С. 19-50. DOI: <https://doi.org/10.28925/2663-4023.2024.25.1950>.
2. Дикий О. В., Сидорчук В. В. Поняття OSINT та суміжні категорії the concept of OSINT and related categories. *Юридичний науковий електронний журнал*. 2024. № 9, С. 332-335. DOI: <https://doi.org/10.32782/2524-0374/2024-9/78>.
3. Думчиков М. О. Використання OSINT технологій для виявлення корупційних правопорушень: сучасні підходи та виклики. *Академічні візії. Секція Право*. 2024. № 36, С. 1-6. DOI: <https://doi.org/10.5281/zenodo.13928363>.
4. Синеколодезський Р. М., Кисельов А. О. Соціальні мережі та ОСІНТ-аналіз в розшуковій діяльності та діагностиці особистості. *Студентський науковий журнал. Universum. Молодіжна наукова ліга. Інститут правоохоронної діяльності, судова система та нотаріат*. 2024. № 12, С. 40-48. URL: <https://archive.liga.science/index.php/universum/article/view/1204/1216> (дата звернення: 05.03.2025 р.).
5. Користін О. Є., Свиридчук Н. П. Зарубіжний досвід антитерористичного використання OSINT. *Науковий вісник Ужгородського Національного Університету. Серія Право*. 2024. № 82 (2), С. 177-181. DOI: <https://doi.org/10.24144/2307-3322.2024.82.2.28>.
6. Коробейнікова Т. І., Симак І. А. Збір даних в технологічному ланцюжку OSINT розслідування. *Sworld-Us Conference Proceedings*. № 1 (usc24-00), С. 41-45. DOI: <https://doi.org/10.30888/2709-2267.2024-24-00-012>.
7. Жмур Н. В. Землянікіна М. П. Історія становлення та сучасний стан технології пошуку інформації OSINT. *Наукові праці Київського авіаційного інституту. Серія: Юридичний журнал “Повітряне і космічне право”*. 2022. № 3 (64), С. 95-101. DOI: <https://doi.org/10.18372/2307-9061.64.16895>.
8. Van Puyvelde D., Tabárez Rienzi F. The Rise of Open-Source Intelligence. *European Journal of International Security*. 2025. № 1. С. 1-15. URL: <https://ppdnz.com.ua/index.php/home/about>



[https://www.cambridge.org/core/journals/european-journal-of-international-security/article/rise-of-opensource-](https://www.cambridge.org/core/journals/european-journal-of-international-security/article/rise-of-opensource-intelligence/21122432399ECB8078BF0D89A76D0586)

[intelligence/21122432399ECB8078BF0D89A76D0586](https://www.cambridge.org/core/journals/european-journal-of-international-security/article/rise-ofopensource-intelligence/21122432399ECB8078BF0D89A76D0586) (дата звернення: 05.03.2025 р.).

9. Yadav A., Kumar A., Singh V. Open-source intelligence: a comprehensive review of the current state, applications and prospects in cyber security. *Artificial Intelligence Review*. 2023. № 56, С. 12407-12438. DOI: <https://doi.org/10.1007/s10462-023-10454-y>.

10. Використання інструментів та методів OSINT для отримання пошукової інформації : практичний poradnik / Зоренко Д. С., Лех Р. В., Кулик Д. О., Червяков О. І. Х.: ППЮК для СБУ, 2023. 36 с.

11. Виходець Ю. О., Тетерятник Г. К. Окремі питання використання OSINT при розслідуванні злочинів в умовах військової агресії рф. *Правові новели. Науково-юридичний фаховий журнал. Актуальні питання юридичної науки*. 2023. № 18, С. 70-76. DOI: <https://doi.org/10.32847/ln.2022.18.10>.

12. Karpilianskyi D., Makhlai O., Tuz O., Pavlenko O., Basalyk S. Development of competence of the Armed Forces of Ukraine officers to manage military units under change conditions. *Multidisciplinary Science Journal*. 2024. № 6(12), С. 1-10. DOI: <https://doi.org/10.31893/multiscience.2024251>.

13. Туз О. С., Тищук В. В. Сутність оперативно-розшукової діяльності. *Науковий вісник Ужгородського Національного Університету. Серія Право*. 2025. № 87(4), С. 146-151. DOI: <https://doi.org/10.24144/2307-3322.2025.87.4.22>.

14. Басалик С. А., Тищук В. В. Контррозвідувальна діяльність: концептуальні засади та організаційні особливості. *Юридичний науковий електронний журнал*. 2025. № 1, С. 449-453. DOI: <https://doi.org/10.32782/2524-0374/2025-1/103>.

15. Басалик С. А., Матняк В. М. Аспекти та сутність оперативного пошуку в оперативно-розшуковій діяльності. *Юридичний науковий електронний журнал*. 2023. № 11, С. 449-451. DOI: <https://doi.org/10.32782/2524-0374/2023-11/109>.