АДМІНІСТРАТИВНЕ ПРАВО І ПРОЦЕС; ФІНАНСОВЕ ПРАВО

УДК 342
DOI https://doi.org/10.32782/1813-338X-2025.3.4

Ю. Р. Кардашевський
доктор філософії у галузі права,
керівник відділу внутрішнього контролю НАЗК, м. Київ
https://orcid.org/0009-0009-8940-6384

ПРАВОВА І МЕТОДОЛОГІЧНА ДОКТРИНА АНАЛІТИЧНОЇ РОЗВІДКИ У СЕКТОРІ БЕЗПЕКИ

У статті досліджується аналітична розвідка як міждисциплінарний феномен, що інтегрує правові, інформаційні та управлінські аспекти діяльності в умовах національної та економічної безпеки. Обґрунтовується, що аналітична розвідка вийшла за межі допоміжної функції та перетворилась на системну складову стратегічного планування, оперативного управління й правозастосування. Проаналізовано основні класифікаційні підходи до аналітики за рівнями (стратегічна, оперативна, тактична), напрямами (політична, економічна, кібернетична, соціальна), джерелами інформації (відкрита, технічна, людська) та метою (превентивна, реактивна, адаптаційна). Розкрито правові режими обробки інформації – від відкритих даних до державної таємниці, а також пов'язані з цим ризики й обмеження. Особливу увагу приділено методології аналітичної розвідки: логічним, статистичним, експертним та математичним методам аналізу, а також проблемам правової легітимації аналітичних моделей, необхідності їхньої стандартизації та прозорості. Автор стверджує, що для ефективної реалізації аналітичної розвідки в секторі безпеки України необхідна модернізація нормативно-правової бази, уніфікація термінології та розробка чітких стандартів. Запропоновано бачити в аналітичній діяльності не лише інформаційну, а й правову функцію, що потребує фахового осмислення й регламентації в українському праві. Аналітична розвідка розглядається як інструмент управління знанням, ризиком і безпекою в умовах сучасної інформаційної турбулентності.

Ключові слова: *аналітична розвідка, національна безпека, інформаційно-аналітична діяльність, правовий режим інформаці, OSINT, правова легітимація, стратегічний аналіз, методи аналізу.*

Постановка проблеми. У сучасних умовах безпекових викликів, гібридних загроз та стрімкої цифровізації, аналітична розвідка перетворюється зі спеціалізованої допоміжної функції у ключовий елемент державного управління ризиками. Її значення зростає як у сфері стратегічного планування, так і в оперативній діяльності правоохоронних, розвідувальних і фінансових органів. Проте це зумовлює появу нових правових та методологічних викликів, які потребують системного осмислення.

Однією з головних проблем є відсутність уніфікованої правової дефініції поняття «аналітична розвідка» в українському законодавстві. Це ускладнює інтеграцію аналітичної діяльності в нормативно-правову систему, створює прогалини у регулюванні доступу до інформації, використання джерел, обробки даних, а також формування висновків, що мають наслідки для безпеки держави, прав людини та публічного управління.

Іншою важливою проблемою є розмежування правових режимів інформації – відкритих, обмежених, службових і засекречених. Аналітична діяльність дедалі частіше спирається на OSINT, Big Data та алгоритмічні моделі, однак залишається незрозумілою межа між допустимим збором інформації та порушенням приватності,

недоторканності комунікацій, захистом персональних або комерційних даних.

Суттєвим викликом є також правова легітимація методів аналітики. Логічні, статистичні, експертні та математичні моделі, що широко використовуються в аналітичній практиці, досі не мають єдиного статусу в правозастосуванні. Відсутність прозорих стандартів, сертифікації аналітичних моделей, документування алгоритмів – все це ставить під сумнів достовірність результатів та обмежує їх використання у правоохоронній чи судовій практиці.

Проблематичним залишається також баланс між безпековими інтересами держави та правами людини. Використання аналітики часто пов'язане з ризиком надмірного контролю, втручання в особисте життя, маніпуляцій даними. Міжнародне право (наприклад, Міжнародний пакт про громадянські і політичні права, Конвенція про захист прав людини і основоположних свобод) чітко встановлює межі діяльності держав у цій сфері, вимагаючи пропорційності, законності та підзвітності.

Таким чином, проблематика аналітичної розвідки як правового та методологічного явища охоплює широке коло питань – від термінології та класифікації функцій до принципів, джерел інформації та процедур написання аналітичних висновків. Її вирішення потребує міждисциплінарного підходу, оновлення нормативної бази та впровадження стандартів аналітичної діяльності відповідно до міжнародних практик і викликів цифрової епохи.

Водночас проблематика аналітичної розвідки як інструменту правової оцінки ризиків і формування безпекової політики активно розробляється у працях як зарубіжних, так і вітчизняних дослідників, однак її міждисциплінарний вимір – особливо на перетині права, розвідки та інформаційних технологій – ще не знайшов системного осмислення у науковій літературі.

Аналіз останніх досліджень і публікацій. У західній безпековій науці аналітика розглядається як фінальна фаза розвідувального циклу (intelligence cycle), що забезпечує перетворення інформації на знання, необхідне для прийняття стратегічних рішень. У цьому контексті знаковими є праці Річардса Гойера (Richards Heuer) [1], Марка Лоуенталя (Mark Lowenthal) [2], Грегорі Тревертона [3], які досліджують методологічні, когнітивні та організаційні аспекти intelligence analysis. Ці дослідження лягли в основу концепцій intelligence-led policing, threat-based planning, strategic foresight. Ключовим внеском для формування аналітичної розвідки стали роботи Джері Ретклiффа [4]. Науковець приділяє увагу теоретико-практичному аналізу моделі ILP в Європі / США, способам інтеграції статистичної, кримінологічної та оперативної аналітики у поліції

У вітчизняному науковому дискурсі дослідження розвідувальної аналітичної діяльності демонструють міждисциплінарний підхід до аналітичної розвідки, охоплюючи юридичні, інформаційні та управлінські аспекти національної безпеки. Праці Василової О., Користіна О., Мартинюка С., Свиридюк Н., Томи М. та інших науковців [5; 6; 7; 8; 9; 10; 11] розкривають правову природу інформаційно-аналітичної діяльності та пропонують концепти її функціонального осмислення в межах державного управління, а також значно розширюють досліджену сферу аналітичної та розвідувальної діяльності в українському контексті: від кібербезпеки та воєнного аналізу до навчання кадрів, антиконтролю та держрегулювання.

Такі організації як UNODC, FRA, CISA і NIST публікують відкриті звіти та посібники, що регулюють практичне використання аналітичних методів, зокрема в умовах зростаючих кіберзагроз, поширення дезінформації та розширення цифрового простору. Їхні документи дедалі частіше використовуються як орієнтири для розробки національного законодавства.

Водночас особливої актуальності набуває вивчення проблематики у контексті розширення використання відкритих джерел, зокрема у зв'язку з повномасштабною війною в Україні, коли OSINT став важливим інструментом не лише військової розвідки, але й правозахисту та журналістських розслідувань. Разом з тим, питання правової легітимації аналітичних методів (зокрема методів OSINT) та їх нормативного регулювання в Україні залишаються дискусійними.

Таким чином, незважаючи на зростаючу кількість публікацій, питання правового статусу, принципів, методів та обмежень у застосуванні аналітичної розвідки – зокрема на базі відкритих джерел – вимагають подальшого дослідження з урахуванням міжнародних стандартів та технологічних змін.

Метою статті є дослідження проблематики пов'язаної із упровадженням аналітичної розвідки в системі національної безпеки, визначенням принципів, функції, методологія та правових засад в Україні, враховуючи загально світові підходи та ознаки.

Виклад основного матеріалу. Аналітична розвідка в сучасному праві та практиці безпеки посідає ключове місце, еволюціонуючи з допоміжного інструменту в самостійну складову державного управління. Вона формується на перетині права, управління, інформаційних і аналітичних наук. У широкому розумінні поняття intelligence охоплює обробку, інтерпретацію й трансформацію інформації у знання для ухвалення безпекових рішень [2].

У межах правового поля аналітика виступає як інформаційно-аналітична діяльність із чіткими принципами, процедурами та стандартами, виконуючи ключові функції у сфері національної безпеки, зокрема у боротьбі з економічними злочинами, захисті критичної інфраструктури тощо.

Основні ознаки аналітичної розвідки: цілеспрямованість, багатоджерельність, прогностичність, доказовість, дотримання режиму обробки інформації. Її правове осмислення вимагає міждисциплінарного підходу та врахування українських реалій, де законодавство ще не містить уніфікованого визначення. Це ускладнює впровадження передових моделей, зокрема Intelligence-led Policing і Data-Driven Governance [7].

Для побудови правової доктрини доцільно дослідити: *термінологію* (дані, інформація, аналітика, аналітична розвідка); *функції* (діагностична, прогностична, стратегічна тощо); *принципи* (законність, обґрунтованість); *класифікацію за рівнем і джерелами*; *співвідношення з правовими режимами; методологію* (логічні, статистичні, експертні підходи).

Правова дефініція потребує розмежування з поняттями «інформаційно-аналітична діяльність» та «дані / інформація», що фігурують у законодавстві про розвідку, інформацію, кібербезпеку, ОРД та фінмоніторинг.

Функціонально аналітика виконує: *діагностичну функцію* (оцінка поточних загроз, тенденцій); *прогностичну* (сценарне планування, foresight); *стратегічну* (розробка політик і прогнозів); *оперативну* (швидке реагування, підтримка операцій); та *сигнальну* (раннє попередження про ризики).

Ці функції мають специфіку в залежності від сфери – розвідки, поліції, фінансового моніторингу. Розвідувальні органи працюють зі стратегічними оцінками, поліція – з оперативними даними, фінансова аналітика орієнтована на виявлення аномалій у транзакціях.

Вище означене вказує на те, що аналітична розвідка є багаторівневою системою управління ризиками, що потребує чіткого правового визначення, інституційного оформлення та міжвідомчої інтеграції. Її нормативне закріплення сприятиме ефективній взаємодії суб'єктів сектору безпеки.

У цьому аспекті важливим є розуміння принципів аналітичної розвідки діяльності, її правових основ та практичного значення. Розвідувальна аналітична діяльність є невід'ємною складовою національної системи безпеки, яка вимагає не лише високої професійної компетентності, а й чіткого дотримання визначених принципів, що забезпечують її легітимність, ефективність та відповідальність. Визначення та систематизація базових принципів аналітичної розвідки ґрунтуються на аналізі міжнародних стандартів, національного законодавства та практичних нормативних документів, що регламентують діяльність суб'єктів сектору безпеки і оборони.

Одним із ключових нормативних джерел, що задає стандарти в цій сфері, є Міжнародний пакт про громадянські і політичні права (1966), який встановлює фундаментальні права і свободи, у тому числі право на захист приватного життя, що накладає обмеження на діяльність розвідувальних та правоохоронних органів і визначає межі їхніх повноважень [12].

Важливим принципом розвідувальної аналітичної діяльності є *законність* – фундаментальна норма, що передбачає чітке дотримання норм національного законодавства, міжнародних договорів і внутрішніх нормативних актів під час здійснення аналітичних процедур. В Україні законність є конституційною основою діяльності усіх державних органів, зокрема й розвідувальних та правоохоронних, що регламентується статтями 19 та 92 Конституції України [13], а також спеціальними законами – «Про розвідку» [14], «Про оперативно-розшукову діяльність» [15] та іншими профільними нормативними актами. Цей принцип забезпечує правове поле для аналітичної роботи та захищає від зловживань.

Наступним важливим є принцип *обґрунтованості*, що передбачає використання в аналітичній діяльності лише достовірних, перевірених і релевантних джерел інформації, а також застосування науково обґрунтованих методів аналізу. Відсутність спекуляцій і маніпуляцій у формуванні аналітичних висновків гарантує якість і прийнятність результатів для ухвалення управлінських рішень [1]. У контексті розвідувальної діяльності цей принцип відповідає вимогам професійної етики аналітика та забезпечує довіру до аналітичних продуктів.

Принцип *пропорційності* є важливою складовою балансу між необхідністю забезпечення безпеки та мінімізацією втручання у права і свободи особи. Він зумовлює, що аналітична діяльність повинна бути спрямована на досягнення визначених законних цілей і не може перевищувати необхідних меж. Цей принцип підтримується у сучасних міжнародних стандартах і правових актах Європейського Союзу, які наголошують, що заходи безпеки мають бути співмірними з рівнем загрози [16]. У національному контексті це означає, що аналітичні процедури повинні враховувати ризики порушення приватності та недоторканності особи.

Об'єктивність у розвідувальній аналітичній діяльності передбачає неупереджений, всебічний і системний підхід до оцінки фактів і подій. Аналітик має утримуватися від політичних, ідеологічних чи особистих упереджень, що можуть вплинути на висновки. Відповідно, у професійних стандартах і кодексах етики аналітиків закріплюється вимога неупередженості та суворої фактологічної перевірки [17]. Це підвищує довіру як до аналітичних продуктів, так і до інституцій, що їх готують.

Принцип *змагальності* набуває особливого значення в контексті міжвідомчої взаємодії та конкуруючих інтересів різних суб'єктів безпеки. Він передбачає, що під час аналізу різних сценаріїв і версій подій має бути забезпечений баланс аргументів і контраргументів, що сприяє всебічній оцінці ситуації та ухваленню збалансованих рішень [18]. Практика показує, що ефективність аналітичної розвідки зростає при залученні різних експертних груп і обміні інформацією між установами.

Баланс між публічним і приватним інтересом – це ще один принцип, що визначає межі діяльності в інформаційній сфері. Аналітична розвідка повинна сприяти захисту суспільного інтересу та національної безпеки, водночас не порушуючи права і свободи окремих громадян, підприємств і організацій. В умовах зростаючої цифровізації і обсягу даних ця вимога набуває особливого значення, оскільки діяльність суб'єктів аналітики тісно пов'язана із обробкою персональних даних та комерційної таємниці [19]. В Україні регулювання цих аспектів відображено у ст.ст. 6, 7, 11 та 14 Закону «Про захист персональних даних» [20] та суміжних нормативних актах, що визначають, у яких випадках обробка персональних даних допускається в інтересах суспільства або для захисту прав інших осіб.

Інтеграція цих принципів у практику розвідувальної аналітичної діяльності є не лише запорукою правомірності, а й ефективності роботи. Водночас виклики сучасного інформаційного простору, зокрема поширення дезінформації, гібридні загрози, кібератаки, вимагають постійного удосконалення правового регулювання і розробки нових підходів до дотримання принципів. Наприклад, у рекомендаціях ООН щодо боротьби з тероризмом і кіберзагрозами наголошується на необхідності гнучкості і адаптивності принципів, що має враховувати технологічні та соціальні зміни.

Означені базові принципи розвідувальної аналітичної діяльності, такі як *законність, обґрунтованість, пропорційність, об'єктивність, змагальність, баланс публічного й приватного інтересу* – є фундаментальними етичними та правовими орієнтирами, що забезпечують не лише легітимність, а й високу якість аналітичних продуктів у системі національної безпеки. Їхнє дотримання сприяє посиленню довіри з боку суспільства, підвищенню професіоналізму аналітичних структур і створенню ефективної системи реагування на сучасні виклики.

Водночас, аналітична розвідка виконує ключову функцію державної безпеки, яка вимагає чіткої систематизації для ефективного управління ризиками. Її класифікація здійснюється за рівнями, напрямами, джерелами та метою.

Перший і найбільш поширений ***підхід*** до класифікації аналітичної розвідки базується на виділенні трьох рівнів, що відповідають різним часовим горизонтам і сферам прийняття рішень: *стратегічна аналітика* орієнтована на довгострокове прогнозування загроз, формування політики безпеки на основі глобальних трендів; *оперативна аналітика* фокусується на середньострокових викликах, забезпечує ухвалення рішень у реальному часі, особливо для спецслужб і правоохоронних органів; *тактична аналітика* забезпечує короткострокові дії підрозділів, спираючись на поточну ситуацію і оперативну інформацію [1; 2; 11; 21; 22]. Ця триступенева модель класифікації є загальноприйнятою в теорії і практиці розвідувальної діяльності, що відображає ієрархію прийняття рішень і розподіл відповідальності у сфері безпеки.

Другий підхід фокусується на тематичній спрямованості аналітичної діяльності та відповідає специфіці інформаційних потоків та об'єктів дослідження: *політична аналітика* аналізує політичні процеси та загрози стабільності; *економічна аналітика* вивчає фінансові ризики,

енергетичну безпеку, санкції; *кібераналітика* охоплює оцінку кіберзагроз, атак на ІТ-інфраструктуру; *соціальна аналітика* вивчає ризики внутрішніх конфліктів, громадську думку. Кожен із цих напрямів формує окремі аналітичні продукти, що в комплексі забезпечують багатовимірний аналіз ситуації та дозволяють розробляти комплексні заходи безпеки.

Третій підхід аналітичної діяльності у розвідці та правоохоронних органах базується на різноманітних джерелах інформації, які також служать підставою для класифікації: *відкрита аналітика (OSINT)* базується на ЗМІ, базах даних, соцмережах; *технічна аналітика (SIGINT)* базується на перехопленні, супутниковій розвідці, кібермоніторингу; *соціальна аналітика (HUMINT)* базується на агентурній інформації, зв'язках із суб'єктами загроз. Ефективна розвідувальна аналітика інтегрує ці джерела, комбінуючи відкриті та закриті дані для побудови повної інформаційної картини.

Четвертий підхід – це класифікація за метою, яка визначає цільові функції аналітики у контексті безпекових викликів: *превентивна аналітика* прогнозує загрози і формує стратегії запобігання; *реактивна аналітика* оцінює події, що відбулись, та їх наслідки; *адаптаційна аналітика* забезпечує гнучке коригування стратегій залежно від змін. Класифікація за метою допомагає розмежувати аналітичні продукти за часовою орієнтацією і функціональним навантаженням, що сприяє більш точному плануванню ресурсів і визначенню пріоритетів у діяльності розвідувальних структур.

Ця багатовимірна класифікація дозволяє інтегрувати аналітичні продукти в систему національної безпеки, забезпечуючи ефективне використання інформації у стратегічному, оперативному та тактичному управлінні.

Правове регулювання обробки інформації є ключовим для ефективної аналітичної розвідки, забезпечуючи баланс між доступом до даних і захистом інтересів держави, організацій та особи. В умовах інформаційної відкритості особливо актуальним є чітке розмежування правових режимів інформації в аналітичній діяльності. У правовій системі України і багатьох інших країн виділяють кілька основних режимів: *режим відкритих даних (Open Data); режим обмеженого доступу; режим державної таємниці; режим службової інформації.* Кожен з цих режимів має свої специфічні ознаки, вимоги до обробки та механізми контролю, що необхідно враховувати в аналітичній діяльності.

Відкриті дані (Open Data). Це публічна інформація, доступна без обмежень. В аналітичній практиці використовуються джерела OSINT – ЗМІ, соцмережі, відкриті бази, що регламентуються Законом України «Про доступ до публічної інформації». Їхнє використання дає змогу оперативно аналізувати події та тенденції, але вимагає перевірки достовірності.

Інформація обмеженого доступу. Містить відомості, які не є державною таємницею, але потребують захисту (персональні дані, комерційна таємниця тощо). Регулюється законами «Про захист персональних даних» та «Про захист інформації в інформаційно-телекомунікаційних системах». У сфері аналітики такий режим є поширеним, зокрема в кібербезпеці та фінансовому моніторингу.

Державна таємниця. Це інформація, розголошення якої може завдати шкоди національній безпеці, в Україні регулюється Законом «Про державну таємницю». Аналітична діяльність у цій сфері вимагає спеціального доступу, шифрування даних і високого рівня контролю.

Службова інформація. Не є державною таємницею, але має обмеження для уникнення шкоди інтересам служби. Регулюється внутрішніми положеннями та загальними нормами інформаційного законодавства. В аналітиці використовується у діяльності правоохоронних органів, держструктур тощо.

У практичній діяльності аналітиків постає питання чіткого визначення режиму, до якого належить інформація на кожному етапі обробки. Помилки в класифікації можуть призвести до порушення законодавства, витоку важливої інформації або, навпаки, необґрунтованого обмеження доступу.

Використання відкритих джерел дозволяє оперативно збирати великий масив інформації, але потребує перевірки та критичного аналізу. Обмежені дані та службова інформація вимагають захисту і чіткого регламентування процедур доступу. Для державної таємниці передбачені найжорсткіші заходи контролю, починаючи від спеціальних систем шифрування і закінчуючи кримінальною відповідальністю за розголошення. Водночас кожен режим потребує відповідного програмного, організаційного і правового забезпечення.

Комплексне дотримання норм, що регулюють доступ і обробку інформації, є підґрунтям законної та ефективної аналітики. В умовах розширення OSINT і кіберзагроз важливо постійно оновлювати нормативну

базу та інтегрувати режими у єдину систему інформаційної безпеки.

Разом з тим, розвідувальна аналітика в системі національної безпеки ґрунтується на поєднанні логічних, статистичних, експертних і математичних методів, які забезпечують об'єктивне перетворення даних у знання. Водночас актуальною є проблема правової легітимації цих методів, що забезпечує законність, прозорість та прийнятність результатів для державного управління і правоохоронної практики. Узагальнюючи методи, можемо виділити такі групи:

− ***логічні методи*** *(індукція, дедукція, абдукція)* є основою структурованого аналізу, дозволяючи виявляти причинно-наслідкові зв'язки й будувати аргументовані гіпотези [23];

− ***статистичні методи*** *(регресійний, кореляційний, факторний аналіз)* дозволяють обробляти великі масиви даних, виявляти тренди та закономірності й широко застосовуються у кримінології, кібербезпеці, аналізі економічних ризиків [2; 4];

− ***експертні методи***, *зокрема метод Делфі, групові оцінки й аналітичні інтерв'ю,* важливі при роботі з неповною або суперечливою інформацією, а їх ефективність залежить від стандартизації процедур та запобігання суб'єктивізму [4];

− ***математичні моделі*** *– від теорії ймовірностей і оптимізації до алгоритмів машинного навчання* – забезпечують автоматизацію, точність і глибину аналізу. Їхнє застосування особливо актуальне у сфері фінансового моніторингу, OSINT та кібербезпеки [11].

Правова легітимація методів передбачає їх відповідність законодавству про захист персональних даних, прозорість алгоритмів, сертифікацію моделей. Відсутність нормативного визнання складних методик може обмежити їх використання у правовому процесі.

У контексті національної безпеки, правоохоронних органів і фінансового моніторингу методологічний арсенал варіюється залежно від специфіки завдань, зокрема у різних секторах безпеки застосовуються специфічні підходи:

− у розвідувальних службах застосовуються комплексні методи, включно з автоматизованим аналізом великих обсягів технічної, агентурної і відкритої інформації, а також інтеграція експертних оцінок для формування стратегічних прогнозів;

− у поліції велика увага приділяється аналітиці криміногенних факторів із використанням статистичних моделей, кримінологічних теорій та експертних оцінок, що дозволяє виявляти злочинні угруповання, тенденції злочинності і планувати превентивні заходи;

− у фінансових установах розвідувальна аналітика спрямована на виявлення аномальних операцій, протидію відмиванню коштів і фінансуванню тероризму, застосовуючи математичні алгоритми аналізу транзакцій, класифікаційні моделі, а також статистичні методи для оцінки ризиків.

Методологічна основа розвідувальної аналітики забезпечує її надійність і результативність. Водночас правове регулювання має не відставати від технологічного розвитку. Інтеграція інструментів Big Data, штучного інтелекту та машинного навчання потребує оновлення нормативної бази для забезпечення прозорості, підзвітності та захисту прав людини.

Висновок. Аналітична розвідка посідає ключове місце в системі національної безпеки, трансформуючись у міждисциплінарний механізм оцінки загроз, прогнозування та формування державної політики. Ефективність цієї діяльності залежить від правової визначеності, чітких класифікацій, стандартизованих методів і відповідного інформаційного забезпечення. У статті доведено, що подальший розвиток аналітики потребує уніфікації термінології, законодавчого закріплення її функцій і режимів доступу до інформації. Водночас наголошено на необхідності правової легітимації методологій, що використовуються в аналітичній практиці, з метою підвищення прозорості, достовірності й довіри до результатів. Аналітична розвідка має потенціал стати повноцінною правовою категорією в системі стратегічного управління державою.

Список використаної літератури:

1. Heuer, R. J. (1999). Psychology of Intelligence Analysis. CIA Center for the Study of Intelligence. URL: https://www.cia.gov/resources/csi/static/Pyschology-of-Intelligence-Analysis.pdf
2. Lowenthal, M. (2020). Intelligence: From Secrets to Policy.
3. Treverton, G. F. (2008). Intelligence for an Age of Terror. Cambridge: Cambridge University Press.
4. Ratcliffe, J. H. (2016). Intelligence-Led Policing. Routledge.
5. Користін О. Є. Аналітична розвідка як елемент управління в системі кібербезпеки. *Наука і правоохоронна.* 2024. № 1. С. 10–18.
6. Користін О. Є., & Свиридюк Н. П. Зарубіжний досвід антитерористичного використання OSINT. *Науковий вісник Ужгородського*

національного університету. 2024. (82.2). DOI: 10.24144/2307-3322.2024.82.2.28
7. Користін О. Є., Свиридюк Н. П. Оцінювання гібридних загроз та спроможностей протидії їм при формуванні стратегічних комунікацій. *Науковий вісник Ужгородського університету*. Серія: Право. 2023. Т. 2. Вип. 77. С. 66–74.
8. Мартинюк С. О. Характеристика принципів функціонування OSINT у сфері національної безпеки. *Юридичний науковий електронний журнал.* 2021. № 9. С. 332–334.
9. Тома М. Г., Василова О. В. Інструменти OSINT: фіксація воєнних злочинів в Україні. DOI: https://doi.org/10.24144/2788-6018.2025.02.134
10. Дрижакова Д., Волинець Р. Використання відкритих джерел інформації (OSINT) у сфері безпеки держави: технології та перспективи. *Матеріали конференцій МЦНД*, (28.02.2025; Дніпро, Україна), 138–141. DOI: https://doi.org/10.62731/mcnd-28.02.2025.005
11. Реалізація філософії "Intelligence-led Policing" в системі кримінального аналізу Національної поліції України : монографія / О. Користін, Д. Швець, Б. Бутко, Б. Денисенко та ін. ; за заг. ред. О. Є. Користіна Київ : «ВАЙТ». 2024. 444 с.
12. Міжнародний пакт про громадянські і політичні права. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text
13. Конституція України від 28 червня 1996 року. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text
14. Про розвідку : Закон України від 17 вересня 2020 року № 912-IX. URL: https://zakon.rada.gov.ua/laws/show/912-20#Text
15. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 № 2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text
16. Handbook on European Data Protection Law. European Union Agency for Fundamental Rights. Luxembourg: Publications Office of the European Union, 2018. URL: https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition
17. Кодекс професійної етики та поведінки прокурорів, затверджено на Всеукраїнській конференції прокурорів 27 квітня 2017 року. URL: https://zakon.rada.gov.ua/laws/show/n0001900-17#Text
18. Heuer, R. J., Jr., & Pherson, R. H. (2011). Structured analytic techniques for intelligence analysis. CQ Press.
19. Solove D. J. Understanding Privacy. Harvard University Press, 2008.
20. Про захист персональних даних : Закон України від 1 червня 2010 року № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
21. Joint Chiefs of Staff. Joint Publication 2–0: Joint Intelligence. Washington, D. C. : U. S. Department of Defense, 2013. URL: https://www.jcs.mil/
22. National Security Strategy of the United States of America, 2017. URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf
23. Alexy R. Teorie der Juristischen Argumentation. Die Theorie des rationalen Diskurses als Theorie der Jurischen Begrindung. Franfurt am Main, 1991.

Kardashevskyy Yu. R. Legal and methodological doctrine of intelligence in the security sector

The article explores intelligence as an interdisciplinary phenomenon that integrates legal, informational, and managerial aspects of activity within the context of national and economic security. It is argued that intelligence has evolved beyond an auxiliary function and has become a systemic component of strategic planning, operational management, and law enforcement. The main classification approaches to analytics are analyzed by level (strategic, operational, tactical), focus area (political, economic, cyber, social), information sources (open, technical, human), and purpose (preventive, reactive, adaptive). The legal regimes of information processing are disclosed – from open data to state secrets – as well as the related risks and limitations. Particular attention is given to the methodology of intelligence: logical, statistical, expert, and mathematical methods of analysis, as well as the issues of legal legitimation of analytical models, the need for their standardization and transparency. The author argues that for the effective implementation of intelligence in Ukraine's security sector, modernization of the regulatory framework, unification of terminology, and development of clear standards are required. It is proposed to view analytical activity not only as an informational but also a legal function that requires professional interpretation and regulation in Ukrainian law. Intelligence is seen as a tool for knowledge, risk, and security management in an era of modern informational turbulence.

Key words: *intelligence, national security, information-analytical activity, legal regime of information, OSINT, legal legitimation, strategic analysis, methods of analysis.*

Дата першого надходження рукопису до видання: 24.07.2025
Дата прийнятого до друку рукопису після рецензування: 26.08.2025
Дата публікації: 30.09.2025