УДК 347.73
DOI https://doi.org/10.32782/2521-6473.2025-3.11

Ю. Р. Кардашевський, доктор філософії у галузі права,
керівник відділу внутрішнього контролю
Національного агентства з питань запобігання корупції

МЕТОДОЛОГІЧНІ ПІДХОДИ У ФОРМУВАННІ РОЗВІДУВАЛЬНОЇ АНАЛІТИКИ В СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ

У статті досліджено методологічні основи розвідувальної аналітики в контексті національної та економічної безпеки. Автор аналізує чотири ключові підходи до аналітичної діяльності: системний, діяльнісний, інформаційно-правовий та ризик-орієнтований. Системний підхід розглядає розвідувальну аналітику як елемент складної структури національної безпеки, де важливою є взаємодія між інституціями та інформаційними потоками. Діяльнісний підхід акцентує на ролі суб'єктів, етапах аналітичного циклу та стандартах аналітичної роботи. Інформаційно-правовий фокусує увагу на законності використання інформації, захисті персональних даних і викликах цифровізації. Ризик-орієнтований підхід дозволяє оцінювати загрози, моделювати їх вплив та приймати обґрунтовані управлінські рішення. У роботі використано міждисциплінарний підхід та проаналізовано наукові праці вітчизняних і зарубіжних дослідників. Автор доводить, що саме поєднання зазначених методологій забезпечує ефективне функціонування аналітичних підрозділів у сучасному динамічному середовищі загроз. Особливу увагу приділено практиці впровадження таких підходів в Україні в умовах гібридної війни, а також у сфері протидії економічним злочинам, корупції та кіберзагрозам. Акцентовано на тому, що ефективність аналітичної діяльності визначається здатністю інтегрувати кілька методологічних підходів – системний, діяльнісний, інформаційно-правовий та ризик-орієнтований – у єдину аналітичну модель. Зроблено висновок про необхідність подальшої інтеграції технологій, удосконалення правового регулювання й професіоналізації аналітичної діяльності.

Ключові слова: *розвідувальна аналітика, економічна безпека, методологія, системний підхід, діяльнісний підхід, ризик-орієнтований підхід, інформаційно-правовий підхід.*

Yu. R. Kardashevskyy. Methodological approaches to the formation of intelligence in the economic security system

The article explores the methodological foundations of intelligence analytics in the context of national and economic security. The author examines four key approaches to analytical activity: systemic, activity-based, legal-informational, and risk-oriented. The systemic approach considers intelligence analytics as an integral part of a complex national security structure, emphasizing the interaction between institutions and information flows. The activity-based approach focuses on the roles of actors, stages of the analytical cycle, and professional standards. The legal-informational approach addresses the legality of information use, data protection, and digitalization challenges. The risk-oriented approach enables the assessment and modeling of threats to support evidence-based decision-making. The study applies an interdisciplinary methodology and draws on domestic and international research. The author argues that the integration of these approaches is essential for the effective functioning of analytical units in a rapidly evolving threat environment. Particular attention is given to the implementation of these approaches in Ukraine under conditions of hybrid warfare, as well as in combating economic crimes, corruption, and cyber threats. The author emphasizes that the effectiveness of analytical activities is determined by the ability to integrate several methodological approaches – systemic, activity-based, information and legal, and risk-oriented – into a single analytical model. The article concludes by emphasizing the need for further integration of technologies, legal regulation improvements, and the professionalization of analytical practices.

Key words: *intelligence, national security, economic security, methodology, risk-oriented approach, legal-informational approach, systematic approach, activity-based approach.*

Постановка проблеми. У сучасних умовах зростання складності загроз національній безпеці та динамічних трансформацій безпекового середовища виникає потреба у методологічному обґрунтуванні розвідувальної аналітичної діяльності як основного інструменту системи економічної, інформаційної, кібер- та загальнодержавної безпеки. Методологія повинна забезпечувати комплексний підхід до аналізу, поєднуючи теоретичні основи з прикладними аспектами.

Ключовим завданням є визначення методології, яка не лише гарантує наукову валідність дослідження, але й відповідає потребам безпекових інституцій у інтегрованому підході до аналізу інформації, прогнозування загроз і підтримки прийняття рішень. Це вимагає врахування загальнонаукових, правових та міждисциплінарних підходів.

Системний підхід дозволяє розглядати розвідувальну аналітику як частину більшої системи національної безпеки, вивчаючи взаємозв'язки елементів (інституцій, процедур, суб'єктів, технологій) та інформаційні потоки між ними.

Діяльнісний підхід фокусується на суб'єктах, цілях, інструментах і результатах розвідувальної аналітики як професійної діяльності, що дозволяє досліджувати алгоритми аналітичної роботи, її організаційну структуру та зв'язок між аналітичними продуктами й рішеннями органів влади.

Інформаційно-правовий підхід вивчає правовий режим інформації, що використовується в аналітичній діяльності, зокрема в контексті персональних даних, державної таємниці та службової інформації, визначаючи межі законності використання різних джерел інформації.

Ризик-орієнтований підхід дозволяє оцінювати й ранжувати загрози, прогнозувати ймовірність подій та їх вплив, що є важливим для політики безпеки та побудови систем раннього попередження. В аналітиці цей підхід включає структурування оцінок ризиків, використовуючи цифрові формати та автоматизовані системи.

Цілісне застосування цих підходів дозволяє створити науково обґрунтовану модель розвідувальної аналітики, що має ключове значення для формування ефективної та правомірної системи реагування на загрози національній безпеці.

У сучасних умовах розвідувальна аналітика розглядається як міждисциплінарна галузь, що інтегрує правові, організаційні, інформаційні та технологічні компоненти національної безпеки. У загальнонауковому плані ця проблематика розвивається як частина прикладної безпеки та кіберполітики, із фокусом на моделі Intelligence-Led Policing (ILP), стратегічну аналітику та ризик-менеджмент [1; 2]. Такі зарубіжні дослідники як Тер'є Авен [3], Сандра Вахтер, Брент Міттельштадт [4], Даніель Солове [5] аналізують як ризик-орієнтовані, так і правові аспекти аналітики.

Українські дослідники активно розробляють методологічні підходи до оцінки та управління загрозами в умовах гібридної війни, а також підкреслюють значущість системного підходу, що передбачає інтеграцію аналітики у структуру безпеки держави. Зокрема, наголошується на важливості системного підходу до розвідувальної аналітики як частини більшої системи національної безпеки, де важливо забезпечити ефективну взаємодію між різними підсистемами (сили оборони, поліція, кіберзахист). Водночас в працях вітчизняних вчених аналізується діяльнісний підхід, при цьому вивчається роль. аналітиків, процеси прийняття рішень і стандарти професійної роботи Окрім того, в умовах війни практичне застосування розвідувальної аналітики знайшло відображення в підготовленій українськими вченими та практиками монографії «Реалізація філософії «Intelligence-led Policing» в системі кримінального аналізу Національної поліції України» [6]. В даному аспекті викликають зацікавленість також роботи авторів під керівництвом Користіна О.Є., що зосереджуються на методології оцінювання гібридних загроз та їх аналізі, виявленні ключових ризиків та аналізі стратегічних комунікацій і пропозицій щодо підвищення стійкості системи безпеки, моделі ILP та ризик-менеджменті в безпековій сфері [7; 8; 9; 10].

Таким чином, сучасна наукова думка формує концептуальне підґрунтя для побудови адаптивної, правомірної та високотехнологічної системи розвідувальної аналітики в умовах сучасних загроз.

Метою статті є аналіз методологічних підходів до розвідувальної аналітики з урахуванням вітчизняного та міжнародного досвіду дозволяє зрозуміти не лише теоретичні засади цього феномену, а й його практичне застосування в системі національної безпеки. Поглиблений аналіз основних підходів, таких як системний, діяльнісний, ризик-орієнтований та інформаційно-правовий, дає змогу сформувати комплексне уявлення про роль аналітичної діяльності в умовах сучасних загроз. Тепер, на основі вищезгаданих досліджень та методологій, доцільно зосередитися на більш детальному розгляді кожного з цих підходів, їх взаємозв'язку та впливі на ефективність розвідувальної аналітики, зокрема в контексті національної безпеки.

Виклад основного матеріалу. Розвідувальна аналітика, як частина національної безпеки, є багаторівневою та ієрархічною системою, що функціонує в тісному взаємозв'язку з іншими підсистемами безпеки. Вона є не просто сукупністю інституцій та функцій, а саморегульованим об'єктом, здатним до адаптації та розвитку в умовах змінюваних загроз. ***Системний підхід*** дозволяє визначити місце розвідувальної аналітики в структурі державного управління безпекою та її взаємодію з іншими компонентами, такими як поліція, розвідка та кіберзахист.

Розвідувальна аналітика включає підсистеми: (1) інформаційне забезпечення, (2) аналітична обробка, (3) прогнозування, (4) експертна оцінка, (5) прийняття рішень. Ці етапи взаємопов'язані в циклічному процесі – від збору даних до ухвалення управлінських рішень [2]. Системний підхід також передбачає постійну адаптацію аналітичних функцій до реальних загроз, що забезпечує гнучкість і оперативність у кризових ситуаціях, зокрема в умовах гібридної війни, як зазначено у Стратегії воєнної безпеки України [11].

Важливу роль у цьому процесі відіграє інтеграція даних з різних джерел, таких як розвідка (HUMINT, SIGINT, OSINT), поліція, фінансовий моніторинг та кібербезпека. Ці потоки інформації взаємодіють в межах єдиного аналітичного процесу. Водночас, міжвідомча координація є необхідною для ефективного обміну інформацією між органами, такими як МВС, СБУ, РНБО, та іншими структурами, що забезпечують безпеку.

Моделювання аналітичних процесів на базі новітніх технологій, зокрема Big Data, штучного інтелекту та машинного навчання, дозволяє підвищити точність прогнозування загроз та підтримку прийняття рішень. Системний підхід також передбачає можливість трансформації та вдосконалення структури розвідувальної аналітики через інновації та стандарти інтероперабельності, що сприяють її ефективності в умовах постійно змінюваних загроз.

У сфері економічної безпеки розвідувальна аналітика дозволяє оцінювати ризики від фінансових потоків, економічної злочинності та інших аспектів, що впливають на стабільність держави. Аналітична система повинна забезпечувати безперервний обмін інформацією та оперативну реакцію на нові виклики [12].

Таким чином, системний підхід до розвідувальної аналітики забезпечує цілісне бачення її функціонування в рамках національної безпеки, акцентуючи увагу на інтеграції, адаптації та інноваціях для підвищення ефективності реагування на сучасні загрози.

Діяльнісний підхід у правовій науці зосереджений на вивченні динаміки та механізмів реалізації суспільно значущих дій, зокрема акцентуючи на функціонуванні суб'єктів і процесів. У контексті розвідувальної аналітики цей підхід орієнтується на аналіз етапів діяльності, ролей учасників, а також регламентів і стандартів, які визначають ефективність і легітимність аналітичного продукту. Згідно з цим підходом, аналіз – не просто обробка даних, а складна інтеракція між тими, хто збирає й обробляє інформацію, і тими, хто ухвалює стратегічні або тактичні рішення. Така взаємодія має критичне значення в ієрархізованій системі безпеки, оскільки вона забезпечує цілісність, адаптивність і своєчасність реакції на загрози [13].

Основним елементом діяльнісного підходу є *характеристика суб'єктів аналітичної діяльності,* що визначаються за рівнем прийняття рішень, доступом до інформації та функціональними задачами. Залежно від цього, аналітика може здійснюватись на трьох рівнях: *стратегічний рівень* – аналітичні підрозділи РНБО, СЗРУ, ГУР МО, МВС, НПУ, ДБР, БЕБ, СБУ, НАБУ, які прогнозують загрози національній безпеці); *оперативний рівень* – аналітичні центри МВС, НПУ, ДПСУ, ДБР, БЕБ, СБУ, НАБУ, що займаються ризик-орієнтованим моніторингом і аналізом інцидентів); *тактичний рівень* (слідчі групи, підрозділи кримінальної поліції та кіберпідрозділи).

Крім того, розвідувальна аналітика може здійснюватись приватними й громадськими організаціями, зокрема аналітичними центрами, науковими установами та журналістами, які працюють з відкритими джерелами (OSINT).

У типових аналітичних групах виділяють *data-аналітика* (займається збором і класифікацією даних та інформації, включаючи OSINT, SIGINT, HUMINT); *аналітика-інтерпретатора* (здійснює обробку даних, формує гіпотези та робить висновки); *аналітика моделювання* (використовує алгоритми, програмне забезпечення та прогнозні моделі для побудови ризикових профілів); *аналітика-комунікатора* (відповідає за візуалізацію та адаптацію результатів для управлінців або слідчих органів). [14]

Ці суб'єкти спеціалізуються з урахуванням технічної складності даних та динаміки загроз, орієнтуючись на міжнародні стандарти (наприклад, IACF, розроблений НАТО, EUROPOL, IACP).

Водночас процес аналітичної діяльності включає п'ять основних стадій: *ідентифікація проблеми* (постановка аналітичного запиту, уточнення об'єкта спостереження); *збір даних* (багатоканальний моніторинг відкритих, обмежених та закритих джерел); *обробка даних* (перевірка достовірності та верифікація); *аналіз та інтерпретація* (побудова гіпотез і порівняльний аналіз); *презентація результату* (формування звіту та візуалізація) [2].

Важливою складовою цієї моделі є: виявлення когнітивних упереджень; перевірка альтернативних гіпотез (ACH – Alternative Competing Hypothesis); застосування *структурованих аналітичних технік* [15].

Професійні стандарти аналітичної роботи ґрунтуються на чотирьох основних критеріях: *етичних* (недопущення фальсифікацій, прозорість джерел, об'єктивність); *методологічних* (використання верифікованих методів аналізу, належне посилання на джерела); *формальних* (відповідність структурі звіту та адаптованість до різних рівнів управління); *комунікаційних* (здатність чітко пояснити складні висновки й візуалізувати ризики та сценарії),

Не менш важливо в даному контексті використовувати міжнародний досвід, зокрема рекомендації Міжнародної асоціації для розвідувальної освіти (International Association for Intelligence Education (IAFIE)), що підтверджує необхідність адаптації цих стандартів до юридичних та організаційних реалій держави. В Україні спостерігається перехід від неформалізованих форм аналітики до інституційно оформленої професії в органах правопорядку та безпеки.

Діяльнісний підхід дозволяє не лише виявити внутрішню логіку функціонування розвідувальної аналітики, але й надає інструменти для оцінки якості аналітичного процесу. Цей підхід деталізує функціональні ролі, процеси, методи та стандарти, акцентуючи увагу на професіоналізмі, що є основою успішної аналітичної діяльності.

Інформаційно-правовий підхід у розвідувальній аналітиці зосереджений на нормативному регулюванні обігу інформації, правовому статусі джерел, засобах її обробки та гарантіях дотримання законності, пропорційності і захисту приватності. Аналітична діяльність у цьому контексті є спеціалізованою інформаційною діяльністю, що здійснюється під державним контролем і в межах правових обмежень щодо прав людини та безпеки [5].

Основним елементом інформаційно-правового підходу є визначення *правового режиму інформації*, що використовується в аналітичній діяльності. Законодавство України передбачає кілька типів інформації з різними режимами доступу та використання (публічна, службова, конфіденційна, персональна тощо).

Іншим важливим компонентом є забезпечення дотримання *принципів законності, пропорційності та цільового використання інформації*. В європейському правовому контексті це закріплено в доктринах

«privacy by design» та «necessity and proportionality», що вимагають: *законності* (чітке нормативне обґрунтування збору й обробки даних); *необхідності* (доказ, що використання саме цього обсягу даних необхідне для досягнення аналітичної мети); *пропорційності* (співвідношення між втручанням у права особи та суспільною потребою) [17].

Особливу увагу вимагає проблема *автоматизованої обробки даних* у розвідувальній аналітиці, зокрема використання аналітичних платформ і алгоритмів машинного навчання. Технології прогнозної аналітики здатні формувати профілі ризику, що може призвести до правових наслідків, таких як перевірки чи арешту.

У зв'язку з цим зростає значення таких принципів, як: *транспарентність алгоритмів* (обґрунтованість логіки прийняття рішень); *право на пояснення* (можливість отримати роз'яснення щодо результатів алгоритмічного рішення); *заборона автоматизованого прийняття рішень у кримінальному процесі без участі людини* [4]. Ці принципи закріплені в General Data Protection Regulation (GDPR – Загальний регламент про захист даних). Це регламент Європейського союзу, який набув чинності 25 травня 2018 року, спрямований на посилення захисту персональних даних фізичних осіб у ЄС. Він встановлює правила обробки персональних даних та надає громадянам ЄС більший контроль за їхньою особистою інформацією), хоча й не є обов'язковими для України, вони стають орієнтирами у цифровізації сектору безпеки, зокрема у контексті співпраці з ЄС у сфері кібербезпеки. [18]

Цифровізація та розвиток технологій збору і обробки даних відкривають нові можливості для держави у сфері безпеки, зокрема через обробку великих даних (big data), OSINT та поведінкову аналітику. Однак існує ризик зловживання цими можливостями, що може підривати демократичні засади. Баланс між безпекою та приватністю стає важливим викликом у цьому контексті.

Серед основних викликів, які стоять перед розвідувальною аналітикою в інформаційно-правовому вимірі, можна виділити:

– *розмитість правових основ для збору OSINT* (дані з соціальних мереж, месенджерів, де інформація є публічною, але одночасно персональною);

– *відсутність єдиного регламенту для обробки даних* (кожне відомство має власні протоколи, що створює правову невизначеність);

– *нестача інституційного контролю* (парламентський, прокурорський та судовий контроль є обмеженим, зокрема в частині превентивного аналізу).

З метою вирішення вказаних викликів та відповідно до інтернаціональних стандартів IALEIA [19], ISO/IEC 27701 [20], що встановлюють вимоги до компетентності аналітиків, сертифікації аналітиків і етичної відповідальності сертифікації, процедур захисту та управління персональними даними, пропонуються різні моделі правового регулювання аналітичної діяльності такі як: *модель нормативного мандату* (закріплення спеціального статусу аналітичних центрів і їхніх повноважень у законодавстві); *модель процедурної легітимності* (акцент на внутрішніх процедурах оцінки правомірності збору та обробки даних); *модель саморегулювання* (створення етичних кодексів та аудитів якості аналітичної роботи). Автор. Документ встановлює стандарти з професійності.

Таким чином, інформаційно-правовий підхід до розвідувальної аналітики дозволяє не лише розглядати її як інструмент боротьби з загрозами, а й як об'єкт регулювання, де кожна аналітична дія має бути правомірною, пропорційною та контрольованою. Це особливо актуально в умовах цифровізації та посилення державного нагляду, коли необхідно забезпечити баланс між безпекою та правами особи.

Ризик-орієнтований підхід є важливою методологічною основою сучасної розвідувальної аналітики, орієнтованої на ідентифікацію, оцінку та управління потенційними загрозами в системі національної безпеки. Він особливо актуальний у сфері економічної безпеки, де загрози мають багатовимірний характер і потребують інтегрованих аналітичних рішень.

Оцінювання ризиків передбачає визначення ймовірності настання загрозливої події та рівня її впливу. Застосовуються *якісні методи* (експертні оцінки, аналіз сценаріїв, пріоритезація загроз) [21]; *кількісні методи* (математичне моделювання, Монте-Карло, теорія ймовірностей) [3] та *змішані методи* (комбінування якісних і кількісних підходів, рекомендоване ISO 31000) [22].

Аналітичне прогнозування загроз базується на виявленні тенденцій і патернів у розвитку загроз: *трендовий аналіз* (виявлення повторюваних циклів); *метод Delphi* (експертний консенсус [23]); *AI/ML* (обробка великих даних і побудова прогнозів).

Разом з тим інтеграція відкритих, технічних та людських джерел підвищує точність прогнозів, а інформаційні технології дозволяють автоматизувати процеси оцінки ризиків, що сприяє оперативності та точності. Водночас автоматизація вимагає правових рамок для захисту персональних даних.

Ризик-орієнтований підхід забезпечує прогнозне й превентивне управління загрозами у розвідувальній аналітиці. Поєднання сучасних методик, автоматизованих систем і правового забезпечення дозволяє ефективно реагувати на змінне середовище безпеки, особливо в економічному секторі. [8]. Методологічна узгодженість і технічна адаптивність є визначальними чинниками успішного функціонування аналітичних структур.

Водночас розвиток ризик-орієнтованих підходів вимагає постійного вдосконалення нормативно-правової бази, що регулює діяльність аналітичних підрозділів. Законодавство має забезпечувати баланс між

необхідністю збору і обробки інформації та гарантуванням прав і свобод громадян, особливо у питаннях захисту персональних даних і недоторканності приватного життя. Важливим є забезпечення прозорості процедур оцінювання ризиків і контролю за їх дотриманням, що підвищує довіру суспільства до органів безпеки [9].

Отже, ризик-орієнтований підхід є невід'ємною складовою сучасної розвідувальної аналітики, що забезпечує системність, прогнозованість і превентивність у боротьбі з загрозами. Його застосування в секторі економічної безпеки дозволяє підвищити ефективність виявлення і нейтралізації фінансових і кіберзагроз, а також сприяє інтеграції державних та приватних зусиль у сфері безпеки. Майбутні дослідження мають зосередитися на вдосконаленні моделей оцінювання ризиків із урахуванням новітніх технологій і розвитку міжнародної співпраці у цій сфері.

В Україні останніми роками відбувається поступове впровадження ризик-орієнтованих методик у сфері економічної безпеки, особливо в контексті протидії економічним злочинам, корупції, відмиванню коштів і фінансуванню тероризму. Зокрема, Національне агентство з питань запобігання корупції (НАЗК), Державна служба фінансового моніторингу (Держфінмоніторинг) та інші правоохоронні органи почали активно використовувати автоматизовані системи аналізу ризиків, що базуються на методах великих даних (big data) та експертних оцінках.

Значну роль відіграє Система електронного декларування НАЗК, яка дозволяє здійснювати перевірку декларацій посадових осіб із застосуванням алгоритмів ризик-орієнтованого аналізу. Це сприяє виявленню невідповідностей, потенційних корупційних ризиків і формує підґрунтя для глибшого розслідування [24].

Водночас Національний банк України (НБУ) інтегрує ризик-орієнтовані підходи в систему регуляторного контролю фінансових установ. НБУ розробив методики оцінювання фінансових ризиків банківського сектору, які враховують макроекономічні загрози, внутрішні та зовнішні виклики, зокрема у воєнних умовах. Такий підхід дозволяє не лише ідентифікувати ризикові установи, а й розробляти превентивні заходи для підтримання стабільності фінансової системи [25].

Особливості впровадження ризик-орієнтованого підходу в Україні пов'язані з викликами воєнного часу, коли значна частина аналітичної роботи спрямована на підтримку безпеки держави в умовах активної агресії. Водночас це стимулює розвиток нових моделей і методів, орієнтованих на гнучкість, швидкість прийняття рішень і комплексний аналіз загроз.

Отже, Україна поступово наближається до кращих міжнародних практик у сфері ризик-орієнтованої аналітики, особливо в частині економічної безпеки, проте для повноцінного функціонування таких систем необхідна подальша модернізація технологічного забезпечення, законодавчої бази і системи міжвідомчої взаємодії.

Висновки. Розвідувальна аналітика постає як ключовий інструмент сучасної системи національної та економічної безпеки, що функціонує в умовах динамічних загроз, цифровізації та зростання значення відкритих джерел інформації. Означене вище підтвердило, що ефективність аналітичної діяльності визначається здатністю інтегрувати кілька методологічних підходів – системний, діяльнісний, інформаційно-правовий та ризик-орієнтований – у єдину аналітичну модель.

Системний підхід дозволяє осмислити аналітику як багаторівневу підсистему в структурі державного управління безпекою, здатну до адаптації та розвитку. Діяльнісний підхід забезпечує розуміння функціональних ролей аналітиків, етапів роботи, типології аналітичних продуктів і каналів взаємодії з інституціями прийняття рішень. Інформаційно-правовий підхід висвітлює нормативні засади обігу інформації, вказує на необхідність балансу між правом на безпеку й правами людини, зокрема в умовах використання великих даних, автоматизованих систем та OSINT. Ризик-орієнтований підхід сприяє структурованій оцінці загроз, підтримці превентивного управління та формуванню моделей прогнозування, особливо в економічному секторі.

Список використаних джерел:

1. Ratcliffe J. H. Intelligence-Led Policing. Routledge. 2016.

2. Lowenthal M. M. Intelligence: From Secrets to Policy (7th ed.). CQ Press. 2017.

3. Aven T. Risk Assessment and Risk Management: Review of Recent Advances on Their Foundation. *European Journal of Operational Research*. 2016. № 253(1). Pp. 1–13. DOI: 10.1016/j.ejor.2015.12.023.

4. Wachter S., Mittelstadt B. A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. *Columbia Business Law Review.* 2019. №(2). pp. 494–620. URL: https://ssrn.com/abstract=3248829

5. Solove D.J. Understanding Privacy. Harvard University Press, 2008.

6. Реалізація філософії «Intelligence-led Policing» в системі кримінального аналізу Національної поліції України : монографія / Користін О., Швець Д., Бутко Б., Денисенко Б. та ін. ; за заг. ред. Користіна О.Є. Київ : «ВАЙТ», 2024. 444 с.

7. Користін О.Є., Пефтієв Д.О., Пеньков С.В., Некрасов В.А. Довідник керівника поліції–поліцейська діяльність, керована розвідувальною аналітикою. Київ : «Видавництво Людмила», 2019. 120 с.

8. Oleksandr Korystin, Nataliia Svyrydiuk and Olena Mitina. Risk Forecasting of Data Confidentiality Breach Using Linear Regression Algorithm. *International Journal of Computer Network and Information Security,* 2022, 4, 1–13. DOI:10.5815/ijcnis.2022.04.01.

9. Oleksandr Korystin, Nataliia Svyrydiuk, Ganna Sobko, Olena Mitina and Marek Aleksander. Risk assessment of cyberattacks in conditions of hybrid war based on analysis of cybersecurity basic capacity in the civil security sector in Ukraine. *CMiGIN 2022* : 2nd International Conference on Conflict Management in Global Information Networks, November 30, 2022, Kyiv, Ukraine. P. 91–101. URL: https://ceur-ws.org/Vol-3530/paper10.pdf

10. Користін О.Є., Свиридюк Н.П. Formation of security competences in law enforcement activities. *Наука і правоохоронна.* 2021. № 1(51). С. 191–198.

11. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України»: Указ Президента України від 25 березня 2021 року № 121/2021. URL: https://zakon.rada.gov.ua/laws/show/121/2021#Text

12. Carter D. L. Law enforcement intelligence. Department of Homeland Security, Department of Justice, Global Justice Advisory Committee. 2021.

13. Bruce J. B., & George R. Z. (eds.). Intelligence Analysis-The Emergence of a Discipline. In Analyzing Intelligence: Origins, Obstacles, and Innovations (pp. 12–30). Georgetown University Press. 2007. URL: https://ciaotest.cc.columbia.edu/book/gup/0019713/f_0019713_16801.pdf?utm_source=chatgpt.com

14. Clark R. M. Intelligence analysis: A target-centric approach (4th ed.). CQ Press. 2013.

15. Heuer R. J. Psychology of Intelligence Analysis. CIA Center for the Study of Intelligence. 1999. URL: https://surl.li/epqpiy

16. Про захист персональних даних: Закон України від 1 червня 2010 року № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

17. Council of Europe. Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law: Remedies, procedural rights and safeguards. Strasbourg: Council of Europe. 2024. URL: https://surl.lu/zpaskp

18. Загальний регламент про захист даних. Вікіпедія. URL: https://surl.li/dmsyle

19. International Association of Law Enforcement Intelligence Analysts (IALEIA). Law Enforcement Analytic Standards (revised edition). 2012. URL: https://www.ialeia.org/background.php

20. ISO/IEC 27701:2019. Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines. International Organization for Standardization. URL: https://www.iso.org/standard/71670.html

21. Hopkin P. Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management. London: Kogan Page Publishers. 2018. URL: https://surl.li/xhizxi

22. ISO 31000:2018. Risk management – Guidelines. International Organization for Standardization. URL: https://www.iso.org/standard/65694.html

23. Linstone H.A., & Turoff M. The Delphi Method: Techniques and Applications. University of Southern California. 2002. URL: https://www.foresight.pl/assets/downloads/publications/Turoff_Linstone.pdf

24. Національне агентство з питань запобігання корупції (НАЗК). (2023, 22 грудня). Новий підхід до відбору та перевірок декларацій: логічний та арифметичний контроль декларацій. URL: https://surl.li/xiiwcb

25. Національний банк України (НБУ). (2024, 7 лютого). Фінансові установи повинні застосовувати ризик-орієнтований підхід під час роботи з PEP. URL: https://surl.li/rsneos

Дата надходження статті: 11.08.2025
Дата прийняття статті: 01.09.2025
Опубліковано: 01.10.2025