

УДК 343.98:004.9:343.132:355.01(477)(045)

DOI <https://doi.org/10.32782/cuj-2026-2-14>**Ковальова Ольга Вікторівна**

доктор юридичних наук, доцент,

помічник ректора

Донецького державного університету внутрішніх справ

ORCID: 0000-0003-4555-0172



## ОРГАНІЗАЦІЯ ТА ОСОБЛИВОСТІ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ДОСУДОВОГО РОЗСЛІДУВАННЯ В УМОВАХ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ ТА У ПІСЛЯВОЄННИЙ ПЕРІОД: КРИМІНАЛІСТИЧНИЙ АСПЕКТ

У статті комплексно узагальнено сучасні наукові підходи до організації інформаційного забезпечення досудового розслідування в умовах правового режиму воєнного стану та з урахуванням викликів післявоєнного періоду. Розкрито криміналістичний зміст інформаційного забезпечення як системи збирання, фіксації, обробки, аналізу, збереження та використання доказової інформації для прийняття процесуальних рішень і формування належної доказової бази. Проаналізовано ключові проблеми функціонування електронного кримінального провадження, зокрема обмежений доступ до інформаційних ресурсів у зоні бойових дій, пошкодження інфраструктури, затримки у проведенні слідчих дій та ризики втрати доказів. Окрему увагу приділено використанню цифрових доказів, OSINT-інструментів і технологій штучного інтелекту, які забезпечують можливість документування воєнних злочинів, аналізу великих масивів даних, ідентифікації осіб та встановлення причинно-наслідкових зв'язків. Визначено основні ризики щодо допустимості, достовірності та цілісності доказової інформації, зокрема пов'язані з порушенням «ланцюга збереження», маніпуляціями з цифровими даними та недостатнім нормативним врегулюванням застосування новітніх технологій. Обґрунтовано необхідність формування цілісної багаторівневої моделі інформаційного забезпечення, яка включає організаційний, інформаційно-технологічний, криміналістичний і правовий компоненти. Підкреслено відсутність системного науково-прикладного опрацювання післявоєнного етапу, зокрема питань відновлення інформаційної інфраструктури, систематизації та процесуальної легалізації матеріалів, зібраних у період воєнного стану, а також їх інтеграції у національні та міжнародні механізми правосуддя. Зроблено висновок про необхідність розроблення комплексної стратегії цифровізації та стандартизації інформаційного забезпечення досудового розслідування, що забезпечить підвищення його ефективності, стійкості та відповідності сучасним криміналістичним і правовим вимогам.

**Ключові слова:** інформаційне забезпечення, досудове розслідування, криміналістика, воєнний стан, післявоєнний період, OSINT, цифрові технології, незаконний обіг зброї.

### **Kovalova O. V. Organization and features of information support of pre-trial investigation under conditions of martial law and in the post-war period: forensic approach**

This article is a study of the organization of information support for pre-trial investigations under conditions of martial law and in the post-war period. Contemporary research emphasizes that such support is a critical factor for the effectiveness of forensic procedures and the reliability of evidence in complex and high-risk investigative environments. Scholars identify multiple challenges, including limited or intermittent access to information in conflict zones, damage to electronic databases, delays in conducting investigative actions, and heightened risks of violating human rights. Open-source intelligence (OSINT) is increasingly recognized as a crucial tool for documenting war crimes, crimes against humanity, and violations of international humanitarian law, provided that strict procedures for verification, metadata recording, and preservation of digital evidence are applied. The application of artificial intelligence in network monitoring, analysis of digital evidence, biometric identification, and predictive modeling of criminal behavior offers new possibilities for pre-trial investigations, while requiring careful regulatory oversight, algorithmic transparency, and standardized operational procedures to prevent errors or misuse. Legal, procedural,



*and forensic frameworks are emphasized as essential for ensuring the admissibility, reliability, and integrity of evidence. In the context of these challenges, the study proposes a comprehensive approach that integrates organizational, technological, forensic, and legal levels of information support. The author suggests measures such as coordinated management of investigators, prosecutors, and operational units, standardized procedures for data collection, processing, and storage, cybersecurity measures, integration of national and international information systems, and post-war restoration, systematization, and legalization of collected materials. Overall, the research underlines the necessity of a holistic, multidimensional strategy that ensures resilience, efficiency, and evidentiary integrity in pre-trial investigations both during wartime and in the post-war period, while also addressing emerging technological, legal, and methodological challenges inherent in modern investigative practice.*

**Key words:** *information support, pre-trial investigation, forensic science, martial law, post-war period, OSINT, digital technologies, illegal arms trafficking.*

**Вступ.** В умовах сучасного розвитку суспільства, зростання рівня злочинності та ускладнення способів вчинення кримінальних правопорушень особливого значення набуває ефективність досудового розслідування. Одним із ключових елементів успішного розкриття та розслідування кримінальних правопорушень є належне інформаційне забезпечення діяльності слідчого. Саме інформація є основою для прийняття процесуальних рішень, висунення слідчих версій, планування розслідування, проведення слідчих (розшукових) дій та доведення вини особи.

Криміналістичний аспект інформаційного забезпечення досудового розслідування полягає у застосуванні спеціальних криміналістичних методів, засобів і прийомів збирання, фіксації, дослідження, аналізу та використання інформації, що має значення для кримінального провадження. Важливу роль у цьому процесі відіграють сучасні інформаційні технології, криміналістичні обліки, експертні дослідження, а також взаємодія слідчого з оперативними підрозділами та іншими органами.

Актуальність теми зумовлена тим, що своєчасне отримання, правильна обробка та ефективно використання інформації безпосередньо впливають на повноту, об'єктивність і неупередженість досудового розслідування. Недостатність або несвоєчасність інформаційного забезпечення може призвести до втрати доказів, помилок у розслідуванні та, як наслідок, до ухвалення неправомірних процесуальних рішень.

**Матеріали та методи.** Проблематика інформаційного забезпечення досудового розслідування в умовах воєнного стану є відносно новою для вітчизняної криміналістики, проте

вже сформувала помітний масив наукових публікацій. Так, нами сформульовано теоретичні та правові засади інформаційного забезпечення досудового розслідування кримінальних правопорушень, що стало фундаментом для розуміння загальних принципів збирання, обробки та використання інформації [1]; М.М. Погорецьким проаналізовано проблемні питання криміналістичного забезпечення досудового розслідування кримінальних правопорушень проти основ національної безпеки України в умовах воєнного стану, акцентувавши увагу на процесуальних та тактичних аспектах [2]; В.А. Шкелебеєм та співавторами виявлено проблеми законодавчого врегулювання використання штучного інтелекту під час досудового розслідування в умовах воєнного стану, що стало важливим кроком до розуміння ризиків і потенціалу цифрових технологій [3].

Ліндсі Фрімен (Lindsay Freeman) у працях щодо використання відкритих джерел та цифрових доказів у розслідуваннях воєнних злочинів (зокрема, «Prosecuting Atrocity Crimes with Open Source Evidence») [4] продемонструвала ефективність OSINT для документування злочинів у зонах конфліктів, де традиційні методи недоступні; Алекс Кеніг (Alexa Koenig) разом із колегами (Sam Dubberley, Daragh Murray) досліджувала правові, етичні та практичні аспекти OSINT в озброєних конфліктах, підкреслюючи його роль у забезпеченні доказування та уникненні шкоди [5].

**Метою роботи** є дослідження криміналістичного аспекту інформаційного забезпечення досудового розслідування, визначення основних джерел інформації, особливостей її збирання, фіксації, дослідження та

використання у процесі розслідування кримінальних правопорушень.

**Результати.** В умовах воєнного стану та у післявоєнний період організація інформаційного забезпечення досудового розслідування набуває особливої актуальності, оскільки від неї залежить ефективність криміналістичних процедур та достовірність отриманих даних. Саме тому доцільним є звернення до наукових праць, що досліджують особливості функціонування цього механізму та сучасні тенденції його розвитку.

Дисертаційне дослідження «Теоретико-правові засади інформаційного забезпечення досудового розслідування кримінальних правопорушень» (2023) наразі є єдиною докторською роботою, безпосередньо присвяченою системному осмисленню інформаційного забезпечення досудового розслідування в умовах воєнного стану [1].

Аналізуючи досвід електронного кримінального провадження, зазначимо, що з 24 лютого 2022 року воєнний стан суттєво загальмував розвиток інформаційно-телекомунікаційної системи досудового розслідування. Серед основних факторів – відсутність доступу до інформації в зоні бойових дій, пошкодження критичної інфраструктури та неможливість своєчасно проводити слідчі дії [1, с. 195].

У межах дисертаційного дослідження нами здійснено аналіз Закону України № 2111-IX від 3 березня 2022 року та змін до ст. 615 КПК [6]. Обґрунтовано, що у разі відсутності технічної можливості доступу до ЄРДР рішення про початок досудового розслідування приймається слідчим або прокурором, а відомості вносяться до реєстру за першої можливості [1, с. 195–196].

Особливу критику викликало доповнення до ст. 236 КПК, яке дозволяє під час обшуку здійснювати пошук комп'ютерних даних на системах, на які не надано дозволу суду. Вважаємо такий підхід недостатньо аргументованим, оскільки він може призвести до втручання у приватне життя осіб, не причетних до злочину [1, с. 232–233]. Загалом законодавчі новели, на думку авторки, є частково позитивними, але розширений доступ до лікарської, банківської таємниці та інформації

про телекомунікаційні послуги створює ризики посягання на персональні дані громадян [1, с. 233].

У межах дослідження нами запропоновано запровадити стратегію «Механізм інформатизації та діджиталізації досудового розслідування», яка передбачає удосконалення нормативно-правового регулювання, створення уніфікованих інформаційних платформ, електронізацію документообігу та інтеграцію міжнародних цифрових проєктів. Також обґрунтовано необхідність упровадження програми «Є-розслідування: електронне кримінальне провадження» [1, с. 264].

Разом з тим дисертація не містить окремої концепції «післявоєнного періоду», а поза увагою залишилися питання опрацювання матеріалів, зібраних в умовах воєнного стану, та міжнародно-правової перспективи використання таких доказів у провадженнях МКС. Через це робота має фундаментальне, водночас залишаючи простір для подальших досліджень післявоєнного періоду.

Значна увага науковців приділяється питанню застосування OSINT-інструментарію. Так, у підручнику О. О. Торбаса акцентується увага на тому, що організація інформаційного забезпечення досудового розслідування в умовах правового режиму воєнного стану вимагає ефективного застосування OSINT-інструментарію для документування воєнних злочинів, зокрема через аналіз відкритих джерел, соціальних мереж та супутникових даних. Криміналістичний аспект такого забезпечення передбачає чітке дотримання етапів OSINT-розслідування відповідно до Протоколу Берклі, з обов'язковим фіксуванням метаданих, хеш-значень та ланцюга забезпечення збереження цифрових доказів для гарантування їх автентичності. Особливістю в умовах воєнного стану є нестабільність інформації в інтернеті, що зумовлює необхідність негайного збереження доказової копії та створення робочих копій для аналізу без ризику компрометації оригіналу. У процесі розслідування воєнних правопорушень OSINT сприяє збору відомостей про порушення міжнародного гуманітарного права, забезпечуючи криміналістичну фіксацію фактів для

подальшого використання в національному та міжнародному правосудді. Важливим елементом є забезпечення належності, допустимості та достовірності електронних доказів, отриманих за допомогою OSINT, що є ключовим для їх визнання в кримінальному. Підготовка слідчих до OSINT-розслідувань у воєнний період включає врахування етичних стандартів, захисту персональних даних та використання сучасних інструментів, таких як штучний інтелект для аналізу зображень та метаданих [7]. Таким чином, OSINT виступає невід'ємною складовою інформаційного забезпечення досудового розслідування, посилюючи його ефективність у криміналістичному аспекті в умовах воєнного стану та сприяючи відновленню справедливості в післявоєнний період.

У своїй статті Д.В. Лісніченко досліджує використання інформації з відкритих джерел (OSINT) та матеріалів ЗМІ як доказів у кримінальному процесі. Автор розглядає як теоретичні основи, так і практичні аспекти застосування таких даних, підкреслюючи їхню значущість у сучасних умовах, коли традиційні методи збору доказів часто стають неможливими через воєнні дії та обмежений доступ до тимчасово окупованих територій.

Особливе значення мають альтернативні джерела інформації: публікації у медіа, відео та фотографії очевидців, супутникові знімки, дані соціальних мереж, блоги та результати журналістських розслідувань. При належній перевірці, підтвердженні автентичності та дотриманні процесуальних вимог така інформація може бути використана як доказ із високою криміналістичною цінністю.

Після початку повномасштабної агресії російської федерації 24 лютого 2022 року документування воєнних злочинів і злочинів проти людяності ускладнилося. У цих умовах дані з відкритих джерел та медіаматеріали стають ключовим інструментом фіксації порушень. Для їхнього ефективного використання необхідне законодавче визначення правил допустимості, фіксації, зберігання та підтвердження достовірності OSINT-даних, включно з дотриманням принципу «ланцюга безперервного володіння» та застосуванням технічних засобів для захисту від маніпуляцій.

Таким чином, інтеграція OSINT та медіаматеріалів у систему доказування набуває особливого значення під час воєнного стану, забезпечуючи можливість ефективного розслідування злочинів та відновлення справедливості [8].

У статті К.В. Волкова, Т.А. Майбороди, Д.О. Єпанчина «Особливості виявлення інформації збуту зброї з відкритих джерел в Національній поліції України» досліджено, що в умовах воєнного стану та загальної мілітаризації суспільства питання оперативного реагування на поширення інформації про обіг зброї набуває особливої актуальності.

Відкриті джерела інформації (OSINT) відіграють важливу роль у встановленні фактів застосування та знищення озброєння, а отримана з них інформація, спеціально оброблена та проаналізована, є важливим елементом для оцінки стану сфери незаконного обігу зброї.

Національна поліція України активно використовує методи OSINT для отримання оперативних даних із соціальних мереж, новинних платформ, відеохостингів, супутникових зображень і відкритих баз. Алгоритми пошуку, фільтрації та перевірки достовірності інформації включають використання спеціалізованих програмних засобів, систем машинного навчання та аналізу візуального контенту з обов'язковою верифікацією.

Важливим аспектом є міжвідомча взаємодія у сфері виявлення та обробки інформації з відкритих джерел, що дозволяє координувати дії з іншими суб'єктами сектору безпеки і оборони [9, с. 362]. Виявлення інформації про збиття озброєння з відкритих джерел є важливим інструментом превентивної та оперативного-розшукової діяльності, що вимагає належного рівня технічної підготовки працівників поліції.

У своїй статті В.С. Бондар «Інформаційне забезпечення тактичних операцій у досудовому розслідуванні кримінально-протиправної діяльності злочинних спільнот» [10] досліджує, що обов'язковою умовою результативного проведення тактичних операцій у досудовому розслідуванні кримінально-протиправної діяльності злочинних спільнот є належне інформаційне забезпечення. Інформаційне

забезпечення проведення тактичних операцій у досудовому розслідуванні кримінально-протиправної діяльності злочинних спільнот представляє собою розгалужену складну систему, яка охоплює аналіз зібраної органами правопорядку та Офісом Генерального прокурора статистичної інформації про стан, структуру та динаміку кримінальних правопорушень, скоєних злочинними спільнотами (статті 255, 255–1, 255–2, 255–3, 256 КК України). Важливим напрямом є використання відомостей, що містяться в базах даних інших державних органів та недержавних установ і організацій (державна казначейська служба, банківські установи, пенсійний фонд, державна міграційна служба, бази даних послуг зв'язку та провайдерів Інтернет). Під час досудового розслідування кримінальних правопорушень, передбачених ст. ст. 255, 255–1, 255–2, 255–3, 256 КК України, оперативно-аналітична робота має низку особливих властивостей, зокрема специфічність вихідної інформації та необхідність відпрацювання надвеликого масиву різнопланової інформації. Це зумовлює вимушену екстреність оперативно-розшукових заходів, негласних слідчих (розшукових) дій та слідчих (розшукових) дій з метою недопущення настання тяжких наслідків.

Для оптимізації інформаційного забезпечення пропонується формування автоматизованих інформаційних систем на основі методологічних принципів: єдність керівництва процесами формування, ведення та використання інформаційних ресурсів, блочно-ієрархічний принцип побудови баз даних, їх структурованість і типізація, інтеграція обліків у єдине інформаційне поле з можливістю наскрізного пошуку. Таким чином, організація інформаційного забезпечення досудового розслідування набуває особливого криміналістичного значення для ефективної протидії організованим злочинності через створення єдиного інформаційно-правового середовища органів правопорядку та його постійного розвитку на базі сучасних досягнень науки і техніки.

Важливе місце посідає стаття кандидата юридичних наук В.А. Шкелебея, доктора юридичних наук В.І. Галагана та доктора юридичних наук Ж.В. Удовенко «Проблеми

законодавчого врегулювання використання штучного інтелекту під час досудового розслідування в умовах воєнного стану». Автори наголошують, що «збройна агресія РФ спричинила суттєве ускладнення кримінального провадження: зросла кількість кримінальних правопорушень, погіршилися можливості збирання традиційних доказів, знизилася ефективність роботи органів досудового розслідування через обмежені ресурси та значні інформаційні навантаження» [3, с. 355]. Дослідники розкривають функціональні можливості ШІ під час «моніторингу мережі, аналізу цифрових доказів (відео, фото, метаданих, GPS, месенджерів), ідентифікації підозрюваних з використанням біометрії, виявлення шаблонів їхньої поведінки, побудови аналітичних зв'язків між ними, прогнозування злочинної активності». Наводяться приклади впровадження ШІ в Україні: «СРДР-аналітика, системи відеоаналітики, платформи OSINT, модулі на базі GPT, а також інструменти проєктів «Безпечне місто», «СМЕРЕКА», «Copilot»» [3, с. 359]. Автори наполягають на «необхідності невідкладного нормативного врегулювання використання ШІ на досудовому розслідуванні, що охоплює запровадження процесуальних гарантій, прозорість алгоритмів і контроль за діяльністю інтелектуальних систем». Попри технологічну глибину дослідження, організаційна модель впровадження ШІ в конкретні слідчі підрозділи, стандарти верифікації ШІ-доказів у судовій практиці та питання кібербезпеки систем залишилися поза аналізом [3].

У 2026 році доктор юридичних наук, старший дослідник М.М. Погорецький опублікував статтю «Кримінальні правопорушення проти основ національної безпеки України в умовах воєнного стану: проблемні питання криміналістичного забезпечення досудового розслідування». Дослідник обґрунтовує, що «гібридизація» загроз, розосередженість подій і учасників, домінування цифрових комунікацій і транснаціональних каналів формують підвищені ризики втрати доказів, дефектів процесуалізації та подальшої недопустимості доказового масиву». Вчений систематизує проблеми криміналістичного забезпечення за такими блоками: «на старті провадження

(первинна фіксація події та цифрових слідів); у цифровому доказуванні (джерело, спосіб отримання, цілісність, відтворюваність); у легалізації матеріалів ОРД / НСРД (процесуальна перспективність результатів, повнота документування, ризики «провисання»); у застосуванні тактичних операцій та тимчасового доступу; у площині судового контролю та допустимості доказів».

Автором запропонована «узагальнювальна модель криміналістичного забезпечення (виявлення-фіксація-процесуалізація-перевірка-судовий контроль) і комплекс прикладних рішень: алгоритм первинних дій із мінімізацією «доказових прогалин», протоколи цифрового документування (метадані, контроль цілісності, опис середовища отримання, ланцюг збереження)» [2, с. 168]. Важливим є висновок про те, що «визначальними критеріями якості криміналістичного забезпечення у воєнний час мають бути перевірюваність, відтворюваність і допустимість доказів за умови збереження гарантій прав людини».

Синтез наукових праць сучасних дослідників дозволяє визначити сучасний стан розвитку вітчизняної криміналістичної науки щодо інформаційного забезпечення досудового розслідування в умовах воєнного стану. Проведений аналіз свідчить, що наявні дослідження переважно зосереджені на окремих складових цієї проблематики, зокрема на інформаційно-технологічному аспекті (застосування OSINT, цифрових доказів, використання алгоритмів штучного інтелекту), питаннях правового регулювання, а також окремих криміналістичних прийомів і алгоритмах діяльності слідчого.

Водночас відсутній комплексний підхід до дослідження інформаційного забезпечення як цілісної системи, а післявоєнний аспект його функціонування залишається практично недослідженим. У вітчизняній науці наразі відсутня цілісна теоретико-прикладна модель організації інформаційного забезпечення досудового розслідування, яка б системно враховувала:

Організаційний рівень – розподіл функцій між слідчим, прокурором та оперативними підрозділами, планування розслідування, координацію міжвідомчої взаємодії, забезпечення

вертикальної та горизонтальної комунікації в умовах воєнного стану.

Інформаційно-технологічний рівень – стандарти збирання, фіксації, обробки, зберігання та верифікації цифрових даних, отриманих у тому числі із застосуванням технологій штучного інтелекту, а також забезпечення кібербезпеки та інтеграції національних і міжнародних інформаційних систем.

Криміналістичний аспект (тактичний і методичний) – систему криміналістичних засобів, прийомів, методів і алгоритмів роботи з криміналістично значущою інформацією у типових та специфічних слідчих ситуаціях воєнного часу (зокрема документування воєнних злочинів, ідентифікація осіб, проведення дистанційних слідчих дій).

Правовий рівень – нормативне регулювання інформаційного забезпечення, визначення критеріїв допустимості доказів, у тому числі цифрових, а також узгодження національних стандартів доказування з міжнародними (зокрема, у практиці міжнародних судових інституцій).

Часовий (післявоєнний) вимір – відновлення та модернізацію інформаційної інфраструктури, систематизацію й процесуальну легалізацію зібраних матеріалів, а також адаптацію процедур використання доказової інформації у національних і міжнародних кримінальних провадженнях.

**Висновки.** Отже, на основі узагальнення наукових напрацювань інформаційне забезпечення досудового розслідування доцільно визначати як комплексну систему створення, збирання, фіксації, обробки, накопичення, аналізу, передачі та використання інформації, що функціонує на правовому, організаційному та інформаційно-технологічному рівнях. У криміналістичному аспекті воно становить сукупність науково-технічних засобів, тактичних прийомів, методів і алгоритмів роботи з криміналістично значущою інформацією з метою встановлення обставин кримінального правопорушення, прийняття обґрунтованих тактичних рішень і формування належної доказової бази.

У післявоєнний період інформаційне забезпечення має включати відновлення та модернізацію інформаційної інфраструктури,

систематизацію, перевірку та легалізацію національного і міжнародного кримінального зібраних під час воєнного стану матеріалів. судочинства та забезпечити інтеграцію накопичених даних у довгострокову стратегію розвитку правоохоронних органів. Також необхідно адаптувати процедури використання доказової інформації до норм

### Література

1. Ковальова О.В. Теоретико-правові засади інформаційного забезпечення досудового розслідування кримінальних правопорушень : дис. ... д-ра юрид. наук : 12.00.09. Кропивницький. 2023. 318 с.
2. Погорецький М.М. Кримінальні правопорушення проти основ національної безпеки України в умовах воєнного стану: проблемні питання криміналістичного забезпечення досудового розслідування. *Науковий вісник Ужгородського національного університету. Серія : Право*. 2026. Т. 5. № 93. С. 156–174. DOI: <https://doi.org/10.24144/2307-3322.2026.93.5.21>
3. Шкелебей В.А., Галаган В.І., Удовенко Ж.В. Проблеми законодавчого врегулювання використання штучного інтелекту під час досудового розслідування в умовах воєнного стану. *Науковий вісник Ужгородського національного університету. Серія : Право*. 2025. Т. 4. № 90. С. 355–361. DOI: <https://doi.org/10.24144/2307-3322.2025.90.4.51>
4. Freeman L. Prosecuting Atrocity Crimes with Open Source Evidence: Lessons from the International Criminal Court. *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation, and Accountability* / ed. S. Dubberley, A. Koenig, D. Murray. Oxford : Oxford University Press, 2019. P. 48–67.
5. Dubberley S., Koenig A., Murray D. (eds). *Digital witness: using open source information for human rights investigation, documentation, and accountability*. Oxford: Oxford University Press, 2020. 360 p.
6. Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про попереднє ув'язнення» щодо додаткового регулювання забезпечення діяльності правоохоронних органів в умовах воєнного стану : Закон України від 03.03.2022 р. № 2111-IX. URL: <https://zakon.rada.gov.ua/laws/show/2111-20#Text> (дата звернення: 05.04.2026).
7. Торбас О.О. OSINT при розслідуванні кримінальних правопорушень : підручник. Одеса : Юридика, 2024. 180 с.
8. Лісніченко Д.В. Використання даних з медіа та відкритих джерел (OSINT) у процесі доказування у кримінальних провадженнях. *Law and public administration*. 2025. № 1. С. 234–239. DOI: <https://doi.org/10.32782/pdu.2025.1.32> (дата звернення: 05.04.2026).
9. Волков К.В., Майборода Т.А., Спанчин Д.О. Особливості виявлення інформації збуту зброї з відкритих джерел в Національній поліції України. *UNIVERSUM*. 2025. № 21. С. 359–362. URL: <https://archive.liga.science/index.php/universum/article/view/1999/2028>
10. Бондар В.С. Інформаційне забезпечення тактичних операцій у досудовому розслідуванні кримінально-протиправної діяльності злочинних спільнот. *Науковий вісник Львівського державного університету внутрішніх справ (серія юридична)*. 2024. № 1. С. 14–21. DOI: <https://doi.org/10.32782/2311-8040/2024-1-2> (дата звернення: 05.04.2026).

### References

1. Kovalova, O.V. (2023). *Teoretyko-pravovi zasady informatsiinoho zabezpechennia dosudovoho rozsliduvannia kryminalnykh pravoporushen* [Theoretical and legal principles of information support for pre-trial investigation of criminal offenses] (Doctoral dissertation, spetsialnist 12.00.09). Kropyvnytskyi [in Ukrainian].
2. Pohoretskyi, M.M. (2026). *Kryminalni pravoporushennia proty osnov natsionalnoi bezpeky Ukrainy v umovakh voiennoho stanu: problemni pytannia kryminalistychnoho zabezpechennia dosudovoho rozsliduvannia* [Criminal offenses against the foundations of national security of Ukraine under martial law: problematic issues of forensic support of pre-trial investigation]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Serii: Pravo*, 5 (93), 156–174. DOI: <https://doi.org/10.24144/2307-3322.2026.93.5.21> [in Ukrainian].
3. Shkelebei, V.A., Halahan, V.I., & Udoenko, Zh.V. (2025). *Problemy zakonodavchoho vrehuliuvannia vykorystannia shtuchnoho intelektu pid chas dosudovoho rozsliduvannia v umovakh voiennoho stanu* [Problems of legislative regulation of the use of artificial intelligence during pre-trial investigation under martial law]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Serii: Pravo*, 4 (90), 355–361. DOI: <https://doi.org/10.24144/2307-3322.2025.90.4.51> [in Ukrainian].
4. Freeman, L. (2019). *Prosecuting atrocity crimes with open source evidence: Lessons from the International Criminal Court*. In S. Dubberley, A. Koenig, & D. Murray (Eds.), *Digital witness: Using open source information for human rights investigation, documentation, and accountability* (pp. 48–67). Oxford University Press [in English].

5. Dubberley, S., Koenig, A., & Murray, D. (Eds.). (2020). *Digital witness: Using open source information for human rights investigation, documentation, and accountability*. Oxford University Press [in English].
6. Verkhovna Rada Ukrainy. (2022, March 3). Pro vnesennia zmin do Kryminalnogo protsesualnogo kodeksu Ukrainy ta Zakonu Ukrainy "Pro poperednie uviaznennia" shchodo dodatkovoho rehuliuвання zabezpechennia diialnosti pravookhoronnykh orhaniv v umovakh voiennoho stanu [On amendments to the Criminal Procedure Code of Ukraine and the Law of Ukraine "On Pre-trial Detention" regarding additional regulation of ensuring the activities of law enforcement agencies under martial law] (Law No. 2111-IX). URL: <https://zakon.rada.gov.ua/laws/show/2111-20#Text> [in Ukrainian].
7. Torbas, O.O. (2024). OSINT pry rozsliduvanni kryminalnykh pravoporushen [OSINT in the investigation of criminal offenses]. Odesa: Yurydyka [in Ukrainian].
8. Lisnichenko, D.V. (2025). Vykorystannia danykh z media ta vidkrytykh dzherel (OSINT) u protsesi dokazuvannia u kryminalnykh provadzhenniakh [Using media and open source intelligence (OSINT) in the evidentiary process in criminal proceedings]. *Law and Public Administration*, 1, 234–239. DOI: <https://doi.org/10.32782/pdu.2025.1.32> [in Ukrainian].
9. Volkov, K.V., Maiboroda, T.A., & Yepanchyn, D. O. (2025). Osoblyvosti vyjavlennia informat-sii zbutu zbroi z vidkrytykh dzherel v Natsionalnii politsii Ukrainy [Features of detecting information on weapons sales from open sources in the National Police of Ukraine]. *UNIVERSUM*, 21, 359–362. URL: <https://archive.liga.science/index.php/universum/article/view/1999/2028> [in Ukrainian].
10. Bondar, V.S. (2024). Informatsiine zabezpechennia taktychnykh operatsii u dosudovomu rozsliduvanni kryminalno-protypravnoi diialnosti zlochynnykh spilnot [Information support for tactical operations in pre-trial investigation of criminal and illegal activities of criminal communities]. *Naukovyi visnyk Lvivskoho derzhavnogo universytetu vnutrishnikh sprav (seriia yurydychna)*, 1, 14–21. DOI: <https://doi.org/10.32782/2311-8040/2024-1-2> [in Ukrainian].

Дата першого надходження статті до видання: 16.04.2026  
Дата прийняття статті до друку після рецензування: 12.05.2026  
Дата публікації (оприлюднення) статті: 29.05.2026