8. Movchan, A., Shliakhovskyi, O., Kozii, V., & Fedchak, I. (2023). Investigating cryptocurrency financing crimes terrorism and armed aggression. Social and Legal Studios, 6(4), 123–131. https://doi.org/10.32518/sals4.2023.123 [in English].

9. FATF. (2023). Tsilove Onovlennia v Konteksti Implementatsii Standartiv FATF shchodo Virtualnykh Aktyviv ta Postachal′nykiv Posluh z Virtual′nymy Aktyvamy [Targeted update on the implementation of FATF standards on virtual assets and virtual asset service providers]. FATF, Paris. Retrieved from https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html [in Ukrainian].

10. Budnyk, L. A., & Budnyk, V. I. (2023). Pravove rehuliuvannia rynku tsyfrovykh aktyviv [Legal regulation of the digital asset market]. In Proceedings of the III International Scientific and Practical Conference "Suchasne upravlinnia orhanizatsiiamy: kontseptsii, tsyfrovi transformatsii, modeli innovatsiinoho rozvytku" (pp. 56–59). Kharkiv. Retrieved from https://ekhnuir.karazin.ua/server/api/core/bitstreams/6c453407-c526-4016-80c1-beb2e5b79fae/content [in Ukrainian].

11. Lukinchuk, R., & Penkina, A. (n.d.). Dovedennia faktu volodinnia kryptovaliutoiu u kryminalnomu protsesi: dzherela ta instrumenty [Proving cryptocurrency ownership in criminal proceedings: sources and tools]. Retrieved from https://advanq.ua/dovedennya-faktu-volodinnya-kriptovalyutoyu-u-kriminalnomu-proczesi-dzherela-ta-instrumenti/ [in Ukrainian].

Стаття надійшла до редакції: 10.11.2025

УДК 343.13:004
DOI: 10.36550/2522-9230-2025-19-147-151

Мехеда Владислав Дмитрович,
кандидат юридичних наук,
заступник начальника кафедри соціально-гуманітарних дисциплін
Військового інституту танкових військ
Національного технічного університету «Харківський політехнічний інститут»
mekhedavd@ukr.net
ORCID ID: 0000-0002-2160-3738

ДОКАЗУВАННЯ У КРИМІНАЛЬНОМУ ПРОЦЕСІ В УМОВАХ ЦИФРОВІЗАЦІЇ: ЄВРОПЕЙСЬКІ СТАНДАРТИ ТА УКРАЇНСЬКІ РЕАЛІЇ

У статті досліджено сучасний стан доказування у кримінальному процесі України в умовах цифрової трансформації суспільства. Підкреслюється, що доказування є фундаментальною складовою реалізації принципів верховенства права, презумпції невинуватості та справедливого суду. З появою нових технологій традиційна система доказів доповнюється електронними даними, цифровими документами, записами з мережі Інтернет та іншими інформаційними джерелами, що суттєво змінює підходи до оцінки доказів.

Актуальність теми зумовлена необхідністю гармонізації національного кримінального процесуального законодавства з європейськими стандартами та міжнародними практиками у сфері збирання, збереження й перевірки електронних доказів. Відсутність чітких критеріїв автентичності, процедур «ланцюга збереження» (chain of custody) та механізмів верифікації цифрових даних створює ризики для дотримання прав людини та справедливості судового розгляду.

У роботі проаналізовано положення чинного Кримінального процесуального кодексу України, міжнародні акти Європейського Союзу, а також практику Європейського суду з прав людини щодо допустимості доказів. Наголошено, що ключовим критерієм залишається не формальна відповідність доказу процесуальним вимогам, а забезпечення «справедливості в цілому».

Визначено перспективні напрями вдосконалення доказового процесу: нормативне закріплення поняття «електронний доказ» і процедур його перевірки, розроблення методичних рекомендацій щодо роботи з цифровими слідами, розвиток підготовки фахівців у сфері цифрової криміналістики та OSINT.

Додатково підкреслено, що успішне впровадження таких реформ потребує комплексного підходу, який включає не лише зміни законодавства та методичні рекомендації, а й розвиток сучасної матеріально-технічної бази, створення спеціалізованих лабораторій цифрової криміналістики та міжвідомчу координацію правоохоронних органів, судів і наукових установ. Такий підхід дозволить забезпечити ефективність доказового процесу в умовах цифрової трансформації, гарантувати дотримання прав людини та сприятиме формуванню високого рівня професійної компетентності фахівців у сфері сучасного кримінального провадження.

Зроблено висновок, що інтеграція європейських стандартів та запровадження єдиних правил поводження з електронними доказами підвищить ефективність досудового розслідування, забезпечить прозорість судового процесу й зміцнить довіру суспільства до правосуддя.

Ключові слова: доказування, кримінальний процес, електронні докази, цифрові технології, допустимість

доказів, справедливий суд, презумпція невинуватості, автентичність доказів, ланцюг збереження, процесуальні гарантії, гармонізація законодавства, європейські стандарти.

Meheda V. EVIDENCE IN CRIMINAL PROCEEDINGS IN THE CONDITIONS OF DIGITALIZATION: EUROPEAN STANDARDS AND UKRAINIAN REALITIES

The article examines the current state of evidence in the criminal process of Ukraine in the context of the digital transformation of society. It is emphasized that evidence is a fundamental component of the implementation of the principles of the rule of law, the presumption of innocence and a fair trial. With the advent of new technologies, the traditional system of evidence is supplemented by electronic data, digital documents, records from the Internet and other information sources, which significantly changes approaches to the assessment of evidence.

The relevance of the topic is due to the need to harmonize national criminal procedural legislation with European standards and international practices in the field of collection, preservation and verification of electronic evidence. The lack of clear authenticity criteria, chain of custody procedures and verification mechanisms for digital data creates risks for respect for human rights and the fairness of the trial.

The paper analyzes the provisions of the current Criminal Procedure Code of Ukraine, international acts of the European Union, as well as the practice of the European Court of Human Rights on the admissibility of evidence. It is emphasized that the key criterion remains not the formal compliance of the evidence with procedural requirements, but the provision of «justice as a whole».

Promising directions for improving the evidentiary process were identified: regulatory consolidation of the concept of "electronic evidence" and procedures for its verification, development of methodological recommendations for working with digital traces, development of training of specialists in the field of digital forensics and OSINT.

It was additionally emphasized that the successful implementation of such reforms requires a comprehensive approach, which includes not only changes in legislation and methodological recommendations, but also the development of a modern material and technical base, the creation of specialized digital forensics laboratories and interdepartmental coordination of law enforcement agencies, courts and scientific institutions. Such an approach will ensure the effectiveness of the evidentiary process in the context of digital transformation, guarantee compliance with human rights and contribute to the formation of a high level of professional competence of specialists in the field of modern criminal proceedings.

It was concluded that the integration of European standards and the introduction of uniform rules for handling electronic evidence will increase the effectiveness of pre-trial investigation, ensure transparency of the judicial process and strengthen public trust in justice.

Keywords: evidentiary, criminal process, electronic evidence, digital technologies, admissibility of evidence, fair trial, presumption of innocence, authenticity of evidence, chain of custody, procedural guarantees, harmonization of legislation, European standards.

Постановка проблеми. Доказування у кримінальному процесі є основою встановлення істини у справі та реалізації принципів верховенства права, презумпції невинуватості й справедливого суду. В умовах цифрової трансформації суспільства цей процес набуває нових рис, адже поряд із традиційними доказами все більшого значення набувають електронні дані, інформація з мережі Інтернет, цифрові документи та записи.

Актуальність теми зумовлена потребою адаптації національної системи доказування до сучасних технологічних реалій і забезпечення балансу між ефективністю розслідування та дотриманням прав людини. Водночас відсутність чітких стандартів щодо збирання, перевірки та оцінки електронних доказів створює ризики порушення процесуальних гарантій і неоднаковості судової практики.

Аналіз останніх досліджень та публікацій. У кримінально-процесуальній доктрині питаннями доказування, допустимості та оцінки доказів зверталися Р.Ш. Бабанли, А.М. Безносюк, С.Л. Будилін, В.В. Вапнярчук, Н.В. Глинська, І.В. Гловюк, В.П. Гмирко, М.Є. Громова, Ю.М. Грошевий, В.М. Іщенко, К.Б. Калиновський, О.В. Капліна, Р.О. Куйбіда, А.А. Кухта, Л.М. Лобойко, Н.О. Марчук, М.М. Михеєнко, В.Т. Нор, П.М. Рабінович, Б.П. Ратушна, Г.М. Рєзнік, І.В. Решетнікова, М.В. Сіроткіна, А.С. Степаненко, В.Д. Титов, І.А. Тітко, О.М. Толочко, Т.І. Фулей, М.І. Хавронюк, О.Г. Шило, М.Є. Шумило, Г.Ю. Юдківська та інші. Їхні праці заклали методологічні та теоретичні основи для подальшого вивчення проблем допустимості електронних доказів, однак існуючі розробки потребують оновлення з урахуванням сучасних стандартів e-evidence, OSINT-практик та технічних настанов щодо збереження цифрових слідів.

Мета статті полягає у комплексному аналізі сучасних тенденцій розвитку доказування у кримінальному процесі України в умовах цифрової трансформації суспільства, виявленні проблем нормативного регулювання електронних доказів, визначенні шляхів гармонізації національного законодавства.

Виклад основного матеріалу дослідження. Згідно зі статтями 84–94 Кримінального процесуального кодексу України, доказами у кримінальному провадженні є фактичні дані, отримані в передбаченому законом порядку, на підставі яких встановлюються наявність чи відсутність обставин, що мають значення для кримінального провадження. Система доказів охоплює показання, речові докази, документи, висновки експертів, результати негласних слідчих (розшукових) дій та інші передбачені законом джерела [1]. Водночас розвиток інформаційних технологій розширює традиційні категорії доказів, зумовлюючи появу цифрових об’єктів, які за своєю природою є менш стабільними, легше модифікуються та потребують спеціальних правил фіксації й транспортування. Це ставить перед законодавцем нові завдання щодо формулювання чітких, уніфікованих вимог до роботи з такими даними.

Сучасний етап розвитку процесуального доказування в Україні характеризується поєднанням двох тенденцій – інтеграцією європейських стандартів прав людини та адаптацією кримінального процесу до умов цифровізації. Конвенція про захист прав людини і основоположних свобод не містить чітко визначених правил допустимості доказів; це обумовлено різноманітністю правових традицій держав – учасниць, що зумовлює переважно національне вирішення зазначених питань [2, с. 177; 4]. Водночас загальноєвропейські стандарти формують орієнтири, яких держави мають дотримуватися у сфері доказування, особливо у питаннях забезпечення конфіденційності, приватності, недоторканності житла та комунікацій.

Практика Європейського суду з прав людини (далі – ЄСПЛ), зокрема рішення у справах Schenk v. Switzerland (1988), Khan v. the United Kingdom (2000), Bykov v. Russia (2009), сформувала концепцію, згідно з якою допустимість доказів не є самодостатнім критерієм справедливості процесу. Ключовим критерієм є «справедливість провадження в цілому» (fairness as a whole) [3]. Саме тому на перший план виходять гарантії захисту від свавільного втручання у приватне життя, забезпечення змагальності, рівності сторін та реальної можливості оскаржити достовірність і походження доказу. У сучасній українській судовій практиці простежується поступове запозичення цих підходів, що зумовлює переорієнтацію з формального аналізу процесуальних порушень на комплексну оцінку впливу таких порушень на права учасників провадження.

Паралельно із європеїзацією кримінального процесу в Україні спостерігається стрімке посилення значення електронних доказів. Згідно з Регламентом 2023/1543, визначення «електронного доказу» охоплює три категорії даних: відомості про абонента, дані трафіку та зміст [5]. До них належать метадані, журнали подій (логи), електронні листування, дані з месенджерів, записи відеоспостереження, геолокаційна інформація, пошукові запити, цифрові сліди у хмарних сховищах тощо. Особливістю їх є нестабільність, залежність від зовнішніх технічних факторів, а також необхідність забезпечення автентичності шляхом фіксації контрольних сум, цифрових підписів або використання спеціалізованих інструментів криміналістичної експертизи.

На міжнародному рівні важливим орієнтиром є Регламент (ЄС) 2023/1543 про Європейські ордери на отримання та збереження електронних доказів і Директива (ЄС) 2023/1544 щодо призначення представників постачальників електронних послуг [5; 6]. Ці акти встановлюють процедури швидкого, захищеного доступу до даних, що зберігаються у транснаціональних цифрових провайдерів, з обов'язковим дотриманням принципів необхідності, пропорційності та мінімізації обсягу доступу. Для України вони мають особливе значення, оскільки визначають напрями подальшої гармонізації законодавства у сфері міжнародного співробітництва та цифрової криміналістики, що є невід'ємною умовою євроінтеграції та участі у спільних механізмах кібербезпеки.

Крім того, цифрова трансформація породжує нові виклики, пов'язані з використанням алгоритмічних систем та штучного інтелекту у доказуванні. У міжнародній практиці вже обговорюються питання прозорості алгоритмів, ризиків упередженості, надійності результатів автоматичних розпізнавальних систем. В Україні на законодавчому рівні такі інструменти ще не врегульовані, однак фактично вони застосовуються в оперативно-розшуковій діяльності, що потребує нормативної конкретизації та визначення меж їх допустимості як доказів у кримінальному процесі.

Верховний Суд України у своїй практиці останніх років неодноразово підкреслював необхідність фіксації «ланцюга збереження» цифрових доказів (chain of custody) – послідовного документування кожного етапу їх здобуття, передання та дослідження. Відсутність підтвердження автентичності електронного доказу або належного процесуального оформлення його отримання є підставою для визнання такого доказу недопустимим відповідно до частини другої статті 86 КПК [1].

Проблемним залишається питання розкриття матеріалів стороною обвинувачення (ст. 290 КПК) [1]. Судова практика засвідчує, що неповне відкриття доказів – наприклад, надання лише результатів негласних слідчих дій без їх процесуальної підстави (ухвали суду, постанови слідчого, технічних протоколів) – істотно порушує право на захист та зумовлює виключення таких матеріалів із доказової бази. Верховний Суд неодноразово наголошував, що сторони повинні забезпечувати повноту розкриття та можливість перевірки джерел інформації, включно з технічними даними про походження файлів.

Суттєвим викликом для українського процесуального законодавства є робота з відкритими джерелами OSINT.

OSINT в основному використовується у функціях національної безпеки, правоохоронних органів та бізнес-розвідки, а також має цінність для аналітиків, які використовують неконфіденційні розвідувальні дані, що відповідають на секретні, несекретні або власні розвідувальні запити в рамках попередніх розвідувальних дисциплін.

Джерела OSINT можна розділити на шість різних категорій інформаційних потоків:

- ЗМІ, друковані газети, журнали, радіо і телебачення в різних країнах і між країнами; інтернет, онлайнові публікації, блоги, дискусійні групи, громадські медіа (наприклад, відео з мобільних телефонів і контент, створений користувачами), YouTube та інші соціальні мережі (наприклад, Facebook, Twitter, Instagram тощо). Це джерело також випереджає низку інших джерел завдяки своїй оперативності та простоті доступу;
- державні дані, державні звіти, бюджети, слухання, телефонні довідники, прес-конференції, веб-

сайти та промови. Хоча ці джерела походять з офіційних джерел, вони є загальнодоступними і можуть використовуватися відкрито і вільно;

- професійні та академічні публікації, інформація, отримана з журналів, конференцій, симпозіумів, наукових робіт, дисертацій та тез; комерційні дані, комерційні зображення, фінансові та промислові оцінки та бази даних;

- сіра література, технічні звіти, препринти, патенти, робочі документи, ділові документи, неопубліковані роботи та інформаційні бюлетені [7].

Такі матеріали можуть мати доказове значення у справах про воєнні злочини, злочини проти людяності та кіберзлочини, однак їхня автентичність потребує спеціальної архівації з фіксацією контрольних сум і збереженням метаданих. Нині це питання не має детального нормативного врегулювання в КПК, що створює ризик довільного тлумачення судами критеріїв допустимості.

Актуальним напрямом удосконалення кримінального процесуального законодавства є нормативне закріплення поняття «електронний доказ», а також процедур «ідентифікації», «ланцюга збереження» та «верифікації» цифрових даних. Доцільно також доповнити КПК окремою статтею, що визначатиме вимоги до електронного формату подання доказів, умови автентифікації, можливість перевірки контрольних сум і залучення спеціалістів-цифрових експертів. Аналогічні положення містяться у кримінально-процесуальних кодексах держав-членів ЄС, зокрема Німеччини, Франції, Польщі, де розроблено алгоритми поводження з e-evidence.

Необхідним видається також розширення змісту статті 246 КПК України щодо негласних слідчих (розшукових) дій шляхом встановлення вимоги індивідуальної санкції суду на кожну дію та епізод, а також обов'язку повного документування процесу зберігання й передачі цифрових матеріалів.

Загальносистемним напрямом удосконалення є запровадження в Україні єдиних методичних рекомендацій для правоохоронців, прокурорів та суддів щодо роботи з цифровими доказами. Такі рекомендації мають базуватися на міжнародних стандартах та практичних настановах Ради Європи й ООН. Вони повинні містити вимоги до процесуальної фіксації, технічних інструментів, документування метаданих, використання контрольних сум і ведення журналів доступу. Паралельно необхідно розвивати спеціалізовану підготовку кадрів у Національній школі суддів України, Офісі Генерального прокурора та органах досудового розслідування з питань цифрової криміналістики, OSINT-архівації та міжнародної правової допомоги.

Поряд із внутрішніми реформами важливим є забезпечення міжнародної співпраці у сфері доступу до електронних доказів. Це особливо актуально в умовах, коли значна частина інформації зберігається на серверах іноземних провайдерів або у хмарних сервісах, підпорядкованих юрисдикції держав-членів ЄС та США.

Висновки. Отже, сучасні тенденції доказування у кримінальному процесі України характеризуються переорієнтацією з формально-легістичного підходу на стандарти гарантійної цифровізації, що забезпечують автентичність, достовірність і прозорість отримання доказів. Подальше вдосконалення національної системи доказування має відбуватися у трьох взаємопов'язаних напрямах: по-перше, оновлення кримінального процесуального законодавства шляхом закріплення термінології та процедур, пов'язаних з електронними доказами; по-друге, розроблення уніфікованих методичних стандартів і навчальних програм для слідчих і суддів; по-третє, активна імплементація міжнародних інструментів співпраці у сфері доступу до цифрових даних. Реалізація цих напрямів дозволить підвищити якість доказового процесу, забезпечити відповідність національної практики європейським стандартам справедливого суду та зміцнити довіру суспільства до правосуддя як інституту захисту прав людини.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Кримінальний процесуальний кодекс України : Закон України від 13 квітня 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/go/4651-17.

2. Вапнярчук В. В. Допустимість доказів (доказування) в практиці Європейського Суду. Публічне право, 2015. № 2. С. 177–183. URL: http://nbuv.gov.ua/UJRN/pp_2015_2_25

3. Європейський суд з прав людини. Рішення у справі Schenk v. Switzerland від 12 липня 1988 р., Series A, № 140; Khan v. the United Kingdom від 12 травня 2000 р., Reports 2000-V; Bykov v. Russia від 10 березня 2009 р., Reports 2009. ЄСПЛ. URL: https://hudoc.echr.coe.int

4. Конвенція про захист прав людини і основоположних свобод (Рим, 1950). URL: https://zakon.rada.gov.ua/go/995_004.

5. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceeding. EUR-Lex. URL: https://eurlex.europa.eu/eli/reg/2023/1543/oj

6. Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 on the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings. EUR-Lex. URL: https://eur-lex.europa.eu/eli/dir/2023/1544/oj.

7. Розвідка з відкритих джерел (Open-source intelligence - OSINT). URL: https://www.maxzosim.com/rozvidka-z-vidkritikh-dzherel-osint/

REFERENCES:

1. Kryminalnyi protsesualnyi kodeks Ukrainy. (2012, April 13). [Criminal Procedure Code of Ukraine]. Zakon Ukrainy №4651-VI. Retrieved from: https://zakon.rada.gov.ua/go/4651-17 [in Ukrainian].
2. Vapniarchuk, V.V. (2015). Dopustymist dokaziv (dokazuvannia) v praktytsi Yevropeiskoho Sudu. [Admissibility of evidence (proving) in the practice of the European Court]. *Publichne pravo. №2.* 177–183. Retrieved from: http://nbuv.gov.ua/UJRN/pp_2015_2_25 [in Ukrainian].
3. Rishennia u spravi Schenk v. Switzerland. (1988, July 12) [Decision in the case of Schenk v. Switzerland]. Yevropeiskyi sud z prav liudyny. Retrieved from: https://hudoc.echr.coe.int [in English].
4. Konventsiia pro zakhyst prav liudyny i osnovopolozhnykh svobod. (1950, November 4). [Convention for the Protection of Human Rights and Fundamental Freedoms]. Retrieved from: https://zakon.rada.gov.ua/go/995_004 [in Ukrainian].
5. Pro yevropeiski ordery na prediavlennia dokaziv ta yevropeiski ordery na zberezhennia elektronnykh dokaziv u kryminalnomu provadzhenni ta dlia vykonannia pokaran, poviazanykh z pozbavlenniam voli, pislia kryminalnoho provadzhennia. (2023, July 12). [On European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceeding]. *Rehlament (IeS) 2023/1543.* Retrieved from: https://eurlex.europa.eu/eli/reg/2023/1543/oj [in English].
6. Pro pryznachennia zakonnykh predstavnykiv z metoiu zboru elektronnykh dokaziv u kryminalnomu provadzhenni. (2023, July 12). [On the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings]. *Dyrektyva 2023/1544.* Retrieved from: https://eur-lex.europa.eu/eli/dir/2023/1544/oj [in English].
7. Rozvidka z vidkrytykh dzherel (Open-source intelligence - OSINT). (2023). [Open-source intelligence (OSINT).]. Retrieved from: https://www.maxzosim.com/rozvidka-z-vidkritikh-dzherel-osint/ [in Ukrainian].

Стаття надійшла до редакції: 12.11.2025

УДК 343.34
DOI: 10.36550/2522-9230-2025-19-151-156

Олійничук Роман Петрович,
кандидат юридичних наук, доцент,
доцент кафедри безпеки та правоохоронної діяльності
Західноукраїнського національного університету
r.oliynychuk@ukr.net
ORCID ID: 0000-0003-4228-1384

АНАЛІТИЧНА ДІЯЛЬНІСТЬ ПОЛІЦІЇ В УМОВАХ ВОЄННОГО СТАНУ: РОЛЬ КРИМІНАЛЬНОГО АНАЛІЗУ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

У статті розглянуто сутність та значення аналітичної діяльності поліції в умовах воєнного стану. Обґрунтовано, що воєнна ситуація вимагає нових підходів до організації інформаційно-аналітичного забезпечення правоохоронної діяльності. Визначено роль кримінального аналізу як основного інструменту прийняття управлінських рішень, прогнозування злочинності та формування ефективних стратегій протидії правопорушенням. Акцентовано на необхідності розвитку методологічних засад аналітичної діяльності, удосконалення інформаційних систем, підготовки висококваліфікованих аналітичних кадрів. Окреслено перспективи впровадження сучасних цифрових технологій, штучного інтелекту та аналітики великих даних у діяльність поліції. Зазначено, що аналітична діяльність у воєнний період стає стратегічним інструментом забезпечення безпеки, координації дій та управління ризиками у сфері правопорядку. Встановлено, що воєнний стан зумовлює суттєві трансформації у структурі злочинності, що, своєю чергою, потребує адаптації аналітичних методів і підходів. З'ясовано, що ефективна аналітична діяльність можлива лише за умови розвитку сучасної інформаційно-аналітичної інфраструктури, удосконалення системи обміну даними між підрозділами, підвищення рівня професійної підготовки аналітичних кадрів та впровадження інноваційних технологій.

Ключові слова: аналітична діяльність, поліція, воєнний стан, кримінальний аналіз, інформаційно-аналітичне забезпечення, прогнозування злочинності, цифровізація, управління безпекою.

Oliynychuk R. ANALYTICAL ACTIVITIES OF THE POLICE UNDER MARTIAL LAW: THE ROLE OF CRIMINAL ANALYSIS AND DEVELOPMENT PROSPECTS

The article examines the essence and significance of police analytical activities under martial law. It substantiates that wartime conditions require new approaches to organizing information and analytical support for law enforcement operations. The role of criminal analysis is defined as a key instrument for decision-making, crime forecasting, and the development of effective crime prevention strategies. The study emphasizes the importance of methodological advancement in police analytics, improvement of information systems, and professional training of analytical personnel. The prospects for implementing modern digital technologies, artificial intelligence, and big data analytics in police work are outlined. It is noted that analytical activity under martial law becomes a strategic tool for ensuring security, coordinating actions, and managing risks within the system of law and order. It has been established that martial law causes significant transformations in the structure of crime, which, in turn,