

ISSN 2311-8040

НАУКОВИЙ ВІСНИК

ЛЬВІВСЬКОГО
ДЕРЖАВНОГО УНІВЕРСИТЕТУ
ВНУТРІШНІХ СПРАВ

Серія правоохоронна

Випуск 2



Видавничий дім
«Гельветика»
2026

УДК 34(05)
НЗ4

Науковий вісник Львівського державного університету внутрішніх справ. Серія правоохоронна: збірник наукових праць / головний редактор І. Федчак. Львів: ЛьвДУВС, 2026. Вип. 2. 120 с.

Виходить чотири рази на рік. Мова видання: українська, англійська.

Засновник – Львівський державний університет внутрішніх справ.

Рішення Національної ради України з питань телебачення і радіомовлення від 11 квітня 2024 року № 1191 (Ідентифікатор медіа в Реєстрі суб'єктів у сфері медіа R30-04394)

Суб'єкт у сфері друкованих медіа – Львівський державний університет внутрішніх справ (вул. Городоцька, буд. 26, м. Львів, 79007, vdzr@lvduvs.edu.ua, тел. (032) 258-63-25)

Рекомендовано Вченою радою Львівського державного університету внутрішніх справ до друку та поширення через мережу Інтернет (протокол № 3 від 24.09.2026).

РЕДАКЦІЙНА КОЛЕГІЯ

Головний редактор – **ФЕДЧАК Ігор Андрійович**, доктор юридичних наук, доцент, декан факультету № 1 (з підготовки фахівців для органів досудового розслідування Національної поліції України), Львівський державний університет внутрішніх справ, Україна

Заступник головного редактора – **ПАСЕКА Олексій Федорович**, кандидат юридичних наук, доцент, директор навчально-наукового інституту з підготовки фахівців для підрозділів кримінальної поліції, Львівський державний університет внутрішніх справ, Україна

Відповідальний секретар – **ШЕХАВЦОВ Руслан Миколайович**, кандидат юридичних наук, професор, професор кафедри кримінального процесу та криміналістики факультету № 1 (з підготовки фахівців для органів досудового розслідування Національної поліції України), Львівський державний університет внутрішніх справ, Україна

Члени редколегії:

ДАНИЛЕВСЬКИЙ Андрій Олександрович, кандидат юридичних наук, доцент, заступник начальника відділу розвитку освітньої та спортивної інфраструктури Департаменту освіти, науки та спорту, Міністерство внутрішніх справ України, Україна;

КОЗИЧ Ігор Васильович, доктор юридичних наук, професор, завідувач кафедри політики в сфері боротьби зі злочинністю та кримінального права навчально-наукового юридичного інституту, Карпатський національний університет імені Василя Стефаника, Україна;

МАРІН Олександр Костянтинович, кандидат юридичних наук, доцент, помічник ректора, Львівський державний університет внутрішніх справ, Україна;

МОВЧАН Анатолій Васильович, доктор юридичних наук, професор, професор кафедри оперативно-розшукової діяльності навчально-наукового інституту з підготовки фахівців для підрозділів кримінальної поліції, Львівський державний інститут внутрішніх справ, Україна;

ПИСЬМЕНСЬКИЙ Євген Олександрович, доктор юридичних наук, професор, проректор з наукової роботи, ЗВО «Університет Короля Данила», Україна;

ХАНЬКЕВИЧ Андрій Миколайович, кандидат юридичних наук, професор, старший викладач, Національний юридичний університет імені Ярослава Мудрого, Україна;

Ярослав КОСТРУБЕЦ (Jarosław Kostrubiec), доктор, професор, декан факультету права та адміністрації, Університет Марії Кюрі-Склодовської, Республіка Польща;

Магдалена БУДИН-КУЛІК (Magdalena Budyn-Kulik), доктор, професор, професор кафедри кримінального права і кримінології, Університет Марії Кюрі-Склодовської, Республіка Польща.

Єва ЯСЮК (Ewa Jasiuk), кандидат наук, професор, доцент, Інститут журналістики та міжнародних відносин, Університет національної комісії з питань освіти, Республіка Польща.

У публікаціях висвітлено результати досліджень у галузі права, здійснених фахівцями у теоретичних і практичних напрямках.

У статтях висловлено позицію авторів, яку не завжди підтримує редакційна колегія.

За достовірність фактів, статистичних даних, точність викладеного матеріалу відповідають автори і рецензенти. Під час передруку матеріалів посилання на Науковий вісник обов'язкове.

Статті у виданні перевірені на наявність плагіату за допомогою програмного забезпечення StrikePlagiarism.com від польської компанії Plagiat.pl

На підставі Наказу МОН України № 928 від 11 червня 2026 року (додаток 1) видання включено до Переліку наукових фахових видань України категорії «Б» у галузі юридичних наук (К9 «Правоохоронна діяльність»).

Офіційний сайт видання: <https://journals.lvduvs.lviv.ua/index.php/law>

© Львівський державний університет внутрішніх справ, 2026

© Оформлення «Видавничий дім «Гельветика», 2026

УДК 342.951:004.8:656.61:347.77/.78

DOI <https://doi.org/10.32782/2311-8040/2026-2-1>**Барабаш Ольга Олегівна,**

доктор юридичних наук, професор,

заступник директора Навчально-наукового інституту права, психології та безпекознавства;

голова Ради молодих вчених,

Львівський державний університет внутрішніх справ,

вулиця Городоцька, 26, Львів, 79000, Україна

ORCID: <https://orcid.org/0000-0003-2666-9696>

КОНЦЕПТУАЛЬНІ ЗАСАДИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ПРОФЕСІЙНОЇ ТАЄМНИЦІ ПРИ ВИКОРИСТАННІ ШТУЧНОГО ІНТЕЛЕКТУ ПІД ЧАС КВАЛІФІКАЦІЙНИХ ІСПИТІВ ЧЛЕНІВ ЕКІПАЖІВ: СТАНДАРТИ НАТО ТА ПЕРСПЕКТИВИ ІМПЛЕМЕНТАЦІЇ В УКРАЇНІ

Анотація. Статтю присвячено дослідженню концептуальних засад правового забезпечення професійної таємниці під час адміністративно-правового регулювання використання систем контролю на основі штучного інтелекту при проведенні кваліфікаційних іспитів членів екіпажів. Актуальність обраної тематики обумовлена цифровою трансформацією адміністративних процедур у сфері підтвердження професійної компетентності моряків, поширенням технологій «AI-proctoring», необхідністю забезпечення належного рівня захисту професійної таємниці, персональних даних та інформаційної безпеки, а також виконанням Україною міжнародних зобов'язань у процесі європейської та євроатлантичної інтеграції.

На основі аналізу законодавства України, міжнародно-правових актів, документів Європейського Союзу, НАТО, Міжнародної морської організації, практики держав – членів НАТО та сучасних доктринальних джерел здійснено критичний перегляд чинної моделі адміністративно-правового регулювання використання систем штучного інтелекту під час кваліфікаційного оцінювання членів екіпажів.

Авторкою обґрунтовано, що усталене в доктрині розуміння поняття професійної таємниці як різновиду інформації з обмеженим доступом наразі не забезпечує належного рівня правового захисту в умовах алгоритмічної обробки інформації. Доведено, що використання систем штучного інтелекту у процедурах кваліфікаційного оцінювання змінює зміст професійної таємниці, поширюючи її на алгоритмічно сформовані результати, журнали функціонування інформаційних систем, поведінкові та біометричні характеристики кандидатів, цифрові докази й інші відомості, які безпосередньо впливають на прийняття адміністративних рішень. Запропоновано авторське визначення професійної таємниці в умовах використання систем штучного інтелекту та сформульовано концепцію алгоритмічно сформованої службово-професійної інформації як самостійного об'єкта адміністративно-правової охорони.

На підставі порівняльно-правового аналізу встановлено, що нормативні моделі держав – членів НАТО ґрунтуються на принципах людиноцентричності, людського контролю, прозорості, пояснюваності алгоритмів, підзвітності, кіберстійкості та юридичної відповідальності людини за остаточне адміністративне рішення. Аргументовано доцільність імплементації зазначених стандартів у національне законодавство з урахуванням особливостей адміністративної процедури проведення кваліфікаційних іспитів членів екіпажів.

Крім того, запропоновано напрями вдосконалення адміністративно-правового регулювання, які передбачають нормативне закріплення обов'язкової алгоритмічної оцінки ризиків, незалежного аудиту систем штучного інтелекту, спеціального правового режиму алгоритмічно сформованої службово-професійної інформації, права кандидата на отримання мотивованого пояснення результатів автоматизованого оцінювання та гарантій ефективного адміністративного і судового оскарження.

Наприкінці зроблено висновок, що адаптація українського законодавства до європейських і євроатлантичних стандартів використання високоризикових систем штучного інтелекту є необхідною передумовою забезпечення законності адміністративних процедур, належного захисту професійної таємниці, зміцнення довіри до процедур підтвердження кваліфікації членів екіпажів і підвищення міжнародного авторитету української системи підготовки та сертифікації моряків.

Ключові слова: професійна таємниця, адміністративно-правове регулювання, штучний інтелект, кваліфікаційний іспит, член екіпажу, моряк, алгоритмічне прийняття рішень, персональні дані, інформаційна

безпека, кібербезпека, пояснюваність алгоритмів, людський контроль, алгоритмічний аудит, стандарти НАТО, морський транспорт.

Barabash Olha. CONCEPTUAL FOUNDATIONS OF THE LEGAL PROTECTION OF PROFESSIONAL SECRECY IN THE USE OF ARTIFICIAL INTELLIGENCE DURING CREW MEMBERS' QUALIFICATION EXAMINATIONS: NATO STANDARDS AND PROSPECTS FOR IMPLEMENTATION IN UKRAINE

Abstract. *This article examines the conceptual foundations of the legal protection of professional secrecy in the context of administrative regulation governing the use of artificial intelligence-based monitoring systems during qualification examinations for crew members. The relevance of this topic stems from the digital transformation of administrative procedures in the field of certifying seafarers' professional competence, the widespread adoption of "AI-proctoring" technologies, the need to ensure an adequate level of protection for professional secrecy, personal data, and information security, as well as Ukraine's fulfillment of its international obligations in the process of European and Euro-Atlantic integration.*

Based on an analysis of Ukrainian legislation, international legal instruments, documents of the European Union, NATO, and the International Maritime Organization, the practices of NATO member states, and contemporary doctrinal sources, a critical review of the current model of administrative and legal regulation governing the use of artificial intelligence systems during the qualification assessment of crew members has been conducted.

The author argues that the established doctrinal understanding of the concept of professional secrecy as a type of restricted-access information currently does not provide an adequate level of legal protection in the context of algorithmic information processing. It is demonstrated that the use of artificial intelligence systems in qualification assessment procedures alters the meaning of professional secrecy, extending it to algorithmically generated results, logs of information system operations, behavioral and biometric characteristics of candidates, digital evidence, and other information that directly influences administrative decision-making. The author proposes a definition of professional secrecy in the context of artificial intelligence systems and formulates the concept of algorithmically generated official and professional information as an independent object of administrative and legal protection.

Based on a comparative legal analysis, it has been established that the regulatory models of NATO member states are grounded in the principles of human-centeredness, human oversight, transparency, algorithmic explainability, accountability, cyber resilience, and human legal responsibility for the final administrative decision. The author argues for the advisability of implementing these standards into national legislation, taking into account the specific features of the administrative procedure for conducting qualification exams for crew members.

In addition, the author proposes directions for improving administrative and legal regulation, which include the normative establishment of mandatory algorithmic risk assessment, an independent audit of artificial intelligence systems, a special legal regime for algorithmically generated official and professional information, a candidate's right to receive a reasoned explanation of the results of automated assessment, and guarantees for effective administrative and judicial appeals.

The paper concludes that adapting Ukrainian legislation to European and Euro-Atlantic standards for the use of high-risk artificial intelligence systems is a necessary prerequisite for ensuring the legality of administrative procedures, adequate protection of professional secrecy, strengthening confidence in procedures for verifying the qualifications of crew members, and enhancing the international standing of the Ukrainian system for training and certifying seafarers.

Key words: *professional secrecy, administrative and legal regulation, artificial intelligence, qualification exam, crew member, seafarer, algorithmic decision-making, personal data, information security, cybersecurity, algorithmic explainability, human oversight, algorithmic audit, NATO standards, maritime transport.*

Вступ. Достатньо стрімка цифровізація публічного управління істотно змінила адміністративно-правові процедури, безпосередньо пов'язані із здійсненням державного контролю, наданням адміністративних послуг та реалізацією дозвільних функцій. Зазначені процеси привертають особливу увагу тоді, коли прийняття адміністративних рішень впливає на безпеку особи, функціонування критичної інфраструктури та виконання міжнародних

зобов'язань держави. До таких сфер, беззаперечно, належить система підтвердження професійної компетентності членів екіпажів морських суден та суден внутрішнього водного транспорту, оскільки результат кваліфікаційного оцінювання визначає можливість набуття чи підтвердження права на здійснення професійної діяльності, яка характеризується підвищеним рівнем відповідальності та міжнародної мобільності.

Останніми роками адміністративна практика багатьох держав свідчить про впровадження автоматизованих систем контролю із застосуванням технологій штучного інтелекту (далі – ШІ) під час проведення теоретичних і практичних іспитів. Власне кажучи, застосування «AI-proctoring» сьогодні перестало бути винятком для освітньої сфери та професійної сертифікації, перетворившись на один із механізмів мінімізації корупційних ризиків, протидії шахрайству, дистанційної ідентифікації кандидатів, верифікації їхньої поведінки та автоматизованої фіксації можливих порушень процедури оцінювання [1]. Одночасно із цим виникає абсолютно новий масив інформації, що формується алгоритмами машинного навчання: біометричні характеристики, поведінкові профілі, аудіовізуальні записи, результати автоматичного аналізу міміки, напрямку погляду, особливостей голосу, швидкості реакції, цифрових слідів користувача та інших параметрів, які раніше взагалі не розглядалися законодавцем як самостійний об'єкт правового регулювання.

З огляду на вищевказане, окрему увагу варто приділити питанню визначення правового режиму інформації, сформованої такими системами. У вітчизняному законодавстві України відсутня цілісна концепція, яка дозволяла б встановити співвідношення між професійною таємницею, конфіденційною інформацією, персональними даними, службовою інформацією та цифровими результатами функціонування алгоритмів ШІ. Як наслідок виникає низка адміністративно-правових ризиків, пов'язаних із доступом до відповідної інформації, порядком її зберігання, міжнародною передачею, використанням під час адміністративного чи судового оскарження результатів іспиту, а також відповідальністю суб'єктів владних повноважень за порушення режиму її охорони.

Проблематика значно ускладнюється міжнародним характером морського судноплавства. Кваліфікаційні документи українських моряків визнаються відповідно до вимог Міжнародної конвенції про підготовку і дипломування моряків та несення вахти 1978 р. [2],

тоді як цифрові технології контролю все частіше розробляються приватними транснаціональними компаніями, програмне забезпечення яких функціонує із використанням хмарних сервісів, розташованих у різних юрисдикціях. Відповідно інформація, що виникає під час кваліфікаційного оцінювання, виходить за межі виключно національного правового простору, стаючи об'єктом міжнародного інформаційного обігу.

Щоправда, наукова література переважно зосереджена на питаннях цифровізації адміністративних процедур [3], правового регулювання ШІ [4], захисту персональних даних [5] чи кібербезпеки [6]. В той же час, професійна таємниця у процедурі автоматизованого контролю під час проведення кваліфікаційних іспитів членів екіпажів практично не досліджувалася як самостійний адміністративно-правовий інститут. Не отримали належного доктринального осмислення критерії віднесення результатів алгоритмічного аналізу до професійної таємниці, адміністративно-правовий статус суб'єктів, які здійснюють обробку відповідної інформації, правова природа автоматично сформованих висновків систем ШІ, а також їх співвідношення із принципами законності, пропорційності, належного врядування, інформаційної безпеки та права на справедливу адміністративну процедуру.

Доволі прикметно, що після набуття Україною статусу держави-кандидата на вступ до ЄС та поглиблення співробітництва з НАТО питання нормативного забезпечення використання систем ШІ вже не може оцінюватися виключно крізь призму внутрішнього законодавства. Регламент (ЄС) 2024/1689 про ШІ («AI Act» [7]), Загальний регламент про захист даних [8], Конвенція Ради Європи №108+ [9], Директива (ЄС) 2022/2555 (NIS2) [10] та низка стандартів Альянсу у сфері інформаційної безпеки формують нову нормативну парадигму, у межах якої будь-які системи автоматизованого контролю мають відповідати вимогам пояснюваності алгоритмів, підзвітності, людського контролю, кіберстійкості та захисту фундаментальних прав людини. Отож імплементація зазначених стандартів повинна супроводжува-

тися критичним переосмисленням вже існуючих адміністративно-правових конструкцій.

Науковий інтерес до окресленої проблематики визначається також відсутністю у вітчизняній юридичній доктрині єдиного розуміння професійної таємниці в умовах функціонування алгоритмічних систем прийняття рішень. На переконання автора, професійна таємниця під час проведення кваліфікаційних іспитів із використанням систем ІІІ має розглядатися не як сукупність окремих відомостей, доступ до яких обмежується законом, а як самостійний адміністративно-правовий режим інформації, що виникає у процесі автоматизованої реалізації владних повноважень, містить результати інтелектуального аналізу поведінки кандидата та потребує спеціального порядку збирання, використання, передачі, зберігання, аудиту і судового контролю. Власне перевірка даної наукової гіпотези визначає загальну концепцію пропонованого дослідження.

Метою статті є формування концептуальних засад адміністративно-правового забезпечення професійної таємниці під час використання систем контролю на основі ІІІ при проведенні кваліфікаційних іспитів членів екіпажів шляхом переосмислення існуючих доктринальних конструкцій, дослідження національного та міжнародного нормативного регулювання, правових стандартів ЄС і НАТО, визначення юридичної природи інформації, що формується алгоритмами ІІІ, обґрунтування її самостійного адміністративно-правового режиму, а також розроблення пропозицій щодо вдосконалення законодавства України.

Матеріали та методи. При цьому науковий пошук не обмежується аналізом чинних нормативних приписів, а спрямовується на виявлення закономірностей зміни адміністративно-правових відносин під впливом алгоритмічних технологій, оцінку достатності існуючих юридичних гарантій охорони професійної таємниці та вироблення критеріїв, за якими результати функціонування систем ІІІ можуть бути віднесені до інформації з обмеженим доступом. Окрему увагу приділено встановленню меж дискреційних повноважень суб'єктів владних повноважень при використанні авто-

матизованих систем контролю, визначенню співвідношення людського контролю та алгоритмічного оцінювання, а також формуванню пропозицій щодо нормативного закріплення процедур алгоритмічного аудиту, пояснюваності рішень ІІІ та адміністративно-правових гарантій судового захисту осіб, стосовно яких такі системи застосовуються.

Однак досягнення окресленої мети неможливе без з'ясування ступеня наукового опрацювання відповідної проблематики, оскільки адміністративно-правове регулювання використання систем ІІІ у процедурах кваліфікаційного оцінювання членів екіпажів перебуває на перетині кількох самостійних напрямів юридичної науки: доктрини професійної таємниці, адміністративного права, інформаційного права, права ЄС, міжнародного морського права, правового регулювання ІІІ та кібербезпеки. Беручи до уваги зазначене, слід звернутися до аналізу останніх досліджень і публікацій, у яких започатковано вирішення окремих аспектів порушеної проблеми, визначити напрями наукової дискусії, оцінити ступінь їх теоретичної розробленості та окреслити ті питання, що залишаються недостатньо дослідженими й потребують подальшого доктринального вивчення.

Результати. Окремі аспекти цифровізації публічного адміністрування та її впливу на реалізацію адміністративних процедур досліджували А. Краковська та М. Бабики, які акцентували увагу на трансформації механізмів надання адміністративних послуг, в той же час залишивши поза науковою увагою питання використання систем ІІІ під час кваліфікаційного оцінювання осіб. Значний внесок у розвиток доктрини правового регулювання ІІІ зробила О. Кожухар, яка обґрунтувала визначальне значення принципу прозорості алгоритмічних систем для забезпечення законності адміністративної діяльності, проте специфіка захисту професійної таємниці у процедурах автоматизованого контролю предметом її дослідження не була.

Теоретичні засади права на приватність ґрунтовно висвітлено у працях О. Панкевича, який розглядає приватність як самостійну

сферу автономії особи, що потребує належних юридичних гарантій у процесі обробки інформації. Своєю чергою, М. Менджул та О. Мулеса дослідили окремі питання забезпечення кібербезпеки під час цифрової взаємодії суб'єктів публічного управління, звернувши увагу на нові виклики інформаційної безпеки в умовах воєнного стану.

Міжнародно-правові аспекти доступу систем ІІІ до професійної таємниці проаналізовано у праці Т. Пашука, де обґрунтовано потребу встановлення спеціальних правових обмежень щодо використання алгоритмів під час обробки конфіденційної професійної інформації. Водночас Д. Кертін та Т. Фіа, досліджуючи проблему алгоритмічної закритості діяльності публічної адміністрації Європейського Союзу, звернули увагу на ризики надмірної секретності функціонування систем ІІІ, яка істотно ускладнює реалізацію принципів прозорості, підзвітності та ефективного контролю за адміністративними рішеннями.

Беручи до уваги вищенаведені наукові напрацювання, слідуює констатувати, що питання адміністративно-правового забезпечення професійної таємниці під час використання систем контролю на основі ІІІ при проведенні кваліфікаційних іспитів членів екіпажів, з урахуванням стандартів НАТО, міжнародних вимог до підготовки моряків та особливостей адміністративної процедури підтвердження кваліфікації, дотепер не отримало самостійного концептуального дослідження. Зокрема, поза належною увагою залишаються правова природа алгоритмічно сформованої інформації, межі поширення режиму професійної таємниці на результати функціонування систем ІІІ, а також засади імплементації міжнародних стандартів у національне адміністративне законодавство, що й зумовлює актуальність та наукову новизну цієї статті.

Правове регулювання професійної таємниці традиційно розвивалося як інститут, покликаний забезпечити баланс між публічним інтересом держави у належному функціонуванні окремих сфер професійної діяльності та приватним інтересом особи щодо нерозголошення відомостей, доступ до яких обумовлений ви-

конанням професійних обов'язків. Історично відповідна категорія формувалася крізь призму медичної, адвокатської, нотаріальної, банківської, аудиторської та інших різновидів професійної таємниці, для яких характерною була наявність спеціального суб'єкта, нормативно визначеного предмета охорони та юридичного обов'язку щодо нерозголошення отриманої інформації. Проте цифровізація адміністративних процедур та активне використання систем ІІІ засвідчили, що усталене в доктрині розуміння професійної таємниці більше не відображає реального змісту інформаційних відносин, які виникають між суб'єктами владних повноважень, розробниками програмного забезпечення, адміністраторами інформаційно-комунікаційних систем та особами, щодо яких здійснюються автоматизовані контрольні процедури.

З огляду на вищенаведене, привертає увагу одна обставина, яка тривалий час залишалася поза межами наукової дискусії. Зокрема, переважна більшість законодавчих конструкцій виходить із презумпції, що *інформація створюється людиною, накопичується людиною та використовується людиною*. Проте сучасні системи контролю із застосуванням ІІІ генерують якісно новий різновид інформації, який виникає без безпосереднього волевиявлення посадової особи. Алгоритми машинного навчання здійснюють оцінювання поведінкових характеристик кандидата, аналізують рухи очей, тембр голосу, тривалість концентрації уваги, зміну освітлення приміщення, цифрову активність користувача, швидкість виконання тестових завдань та десятки інших параметрів, результатом чого стає формування висновку про наявність чи відсутність ознак порушення процедури складання кваліфікаційного іспиту. Дана інформація має істотне юридичне значення, оскільки безпосередньо впливає на прийняття адміністративного рішення про видачу, відмову у видачі або підтвердження кваліфікаційного документа.

У зазначеному аспекті виникає питання, яке, гадаємо, ще не отримало належного доктринального опрацювання: чи можна результати алгоритмічного аналізу вважати різно-

видом професійної таємниці, якщо вони не були сформовані людиною, проте використовуються суб'єктом владних повноважень під час реалізації адміністративної компетенції? Власне кажучи, традиційні критерії професійної таємниці, що ґрунтуються виключно на професійному статусі носія інформації, вже не дозволяють надати переконливу відповідь. Натомість цифрове середовище демонструє іншу модель інформаційного обігу, в якій суб'єкт владних повноважень виконує функцію адміністратора інформації, а її первинним «автором» стає програмний алгоритм.

Конституція України від 28.06.1996 р. №254к/96-ВР, закріплюючи у ст. 32 гарантії невтручання в особисте і сімейне життя та заборону збирання, зберігання, використання і поширення конфіденційної інформації про особу без її згоди [11], фактично встановлює імперативну конституційну вимогу захисту інформаційної приватності. Проте наведена норма була прийнята тоді, коли цифрові технології ще не здійснювали самостійного аналізу поведінки людини. Вочевидь тому буквально тлумачення конституційних приписів сьогодні не забезпечує належного правового регулювання випадків, за яких автоматизовані системи формують нові інформаційні масиви, які раніше взагалі не існували як об'єкт юридичної охорони.

Аналогічні висновки впливають із положень Закону України «Про інформацію» від 02.10.1992 р. №2657-ХІІ [12]. Законодавець класифікує інформацію залежно від режиму доступу, визначаючи відкриту інформацію та інформацію з обмеженим доступом, до якої належать конфіденційна, таємна і службова інформація. Разом із тим Закон не містить критеріїв віднесення до конфіденційної інформації результатів автоматизованого поведінкового аналізу особи, здійсненого системами ШІ. Втім, відсутність відповідної регламентації не можна розглядати як випадкову законодавчу прогалину, оскільки на момент прийняття зазначеного нормативного акта технології «AI-proctoring» фактично не використовувалися в адміністративній діяльності. А отже, сформовані законодавцем класифікаційні критерії вже

не відповідають сучасному стану цифрових правовідносин.

Не менш показовим є зміст Закону України «Про захист персональних даних» від 01.06.2010 р. №2297-VI [13]. Закон визначає персональні дані як «...відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована» (абз. 8 ст. 2 Закону). Водночас алгоритмічний аналіз поведінки кандидата під час складання кваліфікаційного іспиту очевидно виходить за межі усталеного розуміння персональних даних. Система ШІ не обмежується встановленням особи кандидата, а здійснює оцінювання його поведінкових патернів, прогнозує можливі ризики недоброчесної поведінки, визначає статистичні відхилення від типової моделі проходження тестування та формує інтегральний цифровий профіль.

Для дослідження заявленої проблематики варто звернутися до права ЄС. Вищезгаданий Загальний регламент про захист даних, запровадивши категорію профайлінгу та автоматизованого прийняття рішень, фактично визнав, що алгоритмічно сформована інформація може суттєво впливати на права людини. Важливе значення має ст. 22 GDPR, яка гарантує особі право не бути об'єктом рішення, що ґрунтується винятково на автоматизованій обробці, якщо таке рішення породжує юридичні наслідки або іншим чином істотно впливає на її права чи законні інтереси [8]. Вважаємо, саме ця конструкція має стати відправною точкою для формування української моделі адміністративно-правового забезпечення професійної таємниці у процедурах кваліфікаційного оцінювання членів екіпажів.

Ще більшої актуальності зазначене питання набуло після набрання чинності Регламентом (ЄС) 2024/1689 про ШІ [7]. Законодавець ЄС вперше запропонував ризик-орієнтовану модель правового регулювання систем ШІ, віднісши окремі системи оцінювання осіб до категорії високого ризику. Прикметно, що правове значення у даному випадку має вже не характер інформації як такої, а можливість алгоритму впливати на реалізацію прав людини, доступ до професії та здійснення еконо-

мічної діяльності. Отож професійна таємниця у сфері AI-контролю повинна оцінюватися крізь призму потенційних юридичних наслідків використання алгоритмічно сформованої інформації, а не виключно через критерій її конфіденційності.

Припустимо, що під час дистанційного складання кваліфікаційного іспиту моряком система «AI-proctoring» зафіксувала багаторазове відведення погляду від монітора, після чого автоматично сформувала повідомлення про високий рівень ймовірності використання сторонньої допомоги. На підставі такого повідомлення екзаменаційна комісія ухвалює рішення про припинення іспиту та відмову у видачі кваліфікаційного документа. Під час судового оскарження кандидат вимагає надати технічні параметри функціонування алгоритму, дані машинного навчання, критерії оцінювання ризику та математичну модель, відповідно до якої система сформувала негативний висновок. Адміністратор інформаційної системи відмовляє, посилаючись на комерційну таємницю розробника програмного забезпечення. Відповідно виникає конфлікт між правом особи на ефективний судовий захист, необхідністю забезпечення прозорості адміністративної процедури, охороною інтелектуальної власності розробника та обов'язком держави гарантувати конфіденційність інформації, отриманої під час кваліфікаційного оцінювання.

Саме з огляду на зазначене є підстави підтримати наукову позицію, відповідно до якої професійна таємниця в умовах використання систем ШІ має розглядатися значно ширше, ніж традиційний інститут інформації з обмеженим доступом [див. 14; 15]. На нашу думку, **професійною таємницею** у сфері проведення кваліфікаційних іспитів членів екіпажів слід розуміти встановлений адміністративним законодавством правовий режим інформації, яка формується, накопичується, аналізується або використовується суб'єктами владних повноважень та автоматизованими системами контролю під час реалізації адміністративної процедури підтвердження професійної компетентності, розголошення чи неправомірне

використання якої здатне вплинути на права особи, безпеку судноплавства, довіру до результатів кваліфікаційного оцінювання чи виконання міжнародних зобов'язань України.

Не менш важливо, що додаткові гарантії встановлює модернізована Конвенція Ради Європи №108+, яка вперше закріпила принципи *пропорційності*, мінімізації обсягу оброблюваних даних, прозорості алгоритмічної обробки та відповідальності контролера даних. В порівнянні з окремими національними моделями, Конвенція поширює відповідні вимоги незалежно від місця фізичного розташування серверів чи інформаційної системи [9]. Вбачається, окреслений підхід має вагоме значення і для України, адже більшість комерційних платформ «AI-proctoring» використовує хмарні дата-центри, розміщені за межами держави.

У сфері кібербезпеки визначальне місце посідає Директива (ЄС) 2022/2555 (NIS2), яка значно посилила вимоги до управління кіберризиками, реагування на інциденти та захисту цифрової інфраструктури [10]. Так, хоча вона безпосередньо не регулює проведення кваліфікаційних іспитів, її положення формують єдиний стандарт захисту інформаційних систем, що використовуються суб'єктами публічної влади. Для України, своєю чергою, імплементація підходів NIS2 – це беззаперечна потреба законодавчого закріплення обов'язкового аудиту інформаційної безпеки платформ «AI-proctoring», періодичного тестування їхньої стійкості до кібератак та визначення адміністративної відповідальності операторів за неналежний рівень кіберзахисту.

Вагомий науковий інтерес становить нормативна політика НАТО щодо використання ШІ. Зокрема, у NATO Artificial Intelligence Strategy 2021 р. Альянс визначив, що застосування ШІ повинно відповідати принципам законності, відповідальності, пояснюваності, надійності, можливості відстеження функціонування алгоритмів та керованості людиною [16]. Подальший розвиток ці положення отримали у документі NATO Responsible Use of Artificial Intelligence, схваленому у 2024 році, де державам рекомендовано забезпечити постійний людський контроль за функціонуванням ви-

сокоризикових AI-систем, здійснювати незалежний аудит алгоритмів, гарантувати їхню кіберстійкість та запобігати алгоритмічній дискримінації [17]. При цьому, незважаючи на військову спрямованість зазначених документів, сформульовані принципи мають універсальний характер і можуть бути застосовані до адміністративних процедур професійної сертифікації. Передусім це стосується обов'язку пояснюваності алгоритмів, адже кандидат повинен мати можливість зрозуміти, з яких причин система сформувала негативний висновок.

З точки зору практики, варто звернути увагу на положення NATO Digital Transformation Implementation Strategy, відповідно до якої цифрові системи, що використовуються органами державної влади, повинні відповідати принципам «...interoperability, cyber resilience, secure-by-design, data governance...» [18]. У контексті проведення кваліфікаційних іспитів членів екіпажів зазначені положення означають потребу нормативного закріплення вимог до захищеного обміну інформацією між Морською адміністрацією, державними реєстрами, інформаційними системами підготовки моряків та міжнародними базами даних. До слова, українське законодавство наразі не встановлює спеціальних критеріїв сертифікації програмного забезпечення, що використовується під час автоматизованого оцінювання кандидатів, тоді як підходи НАТО виходять із необхідності попередньої перевірки цифрових платформ на відповідність визначеним вимогам безпеки.

Досвід держав – членів НАТО підтверджує, що нормативне регулювання «AI-proctoring» формується за єдиною концепцією, хоча способи її реалізації різняться. Так, у Великій Британії Office of Qualifications and Examinations Regulation після пандемії COVID-19 сформував окремий напрям правового регулювання дистанційного контролю за перебігом кваліфікаційних іспитів, а згодом оприлюднив політику щодо використання ШІ у сфері кваліфікацій. Регулятор виходить із необхідності забезпечення справедливості оцінювання, пропорційного використання ШІ, обов'язкового людського контролю за висо-

коризиковими процедурами та недопустимості використання ШІ як єдиного механізму ухвалення рішень щодо результатів кандидатів [19; 20]. Очевидно, дана модель заслуговує на підтримку, оскільки мінімізує ризик помилкових рішень, спричинених технічними помилками чи недосконалістю алгоритмів.

У Нідерландах питання використання систем автоматизованого прокторингу (автоматизованого спостереження та контролю за дотриманням встановленої процедури під час дистанційного складання іспитів) стало актуальним після судових спорів, пов'язаних із використанням програмного забезпечення «Proctorio» у закладах вищої освіти. Національний орган із захисту персональних даних (Autoriteit Persoonsgegevens), а також нідерландська судова практика акцентували увагу на потребі дотримання принципу пропорційності під час втручання у приватне життя, проведення попередньої оцінки впливу на захист персональних даних відповідно до ст. 35 GDPR [8] та належного обґрунтування неможливості застосування менш інтенсивних засобів контролю. За відсутності такого обґрунтування використання автоматизованих систем прокторингу може розглядатися як *непропорційне обмеження права на повагу до приватного життя* [21]. Думається, саме критерій *пропорційності* повинен стати обов'язковою складовою адміністративної процедури запровадження AI-контролю в Україні.

Норвегія та Данія, які активно цифровізують публічне управління, використовують дещо іншу модель [22, 23]. Замість максимальної автоматизації вони зберігають вирішальну роль екзаменатора, тоді як ШІ виконує допоміжну функцію з аналізу потенційних ризиків. Вочевидь, практика названих країн відповідає принципам НАТО щодо «human oversight» і видається більш прийнятною для адміністративно-правової системи України, ніж моделі повністю автоматизованого прийняття рішень.

Свою чергою, у Сполучених Штатах Америки нормативне регулювання здійснюється переважно на рівні окремих штатів, федеральних рекомендацій та технічних стандартів, що

обумовлює певну децентралізацію відповідної правової політики. Водночас NIST AI Risk Management Framework сформував універсальну модель управління ризиками, засновану на принципах пояснюваності, достовірності, безпечності та підзвітності алгоритмів [24; 25]. Втім, незважаючи на відсутність спеціального федерального закону про ШІ, американська модель привертає увагу насамперед розвитком процедур незалежного аудиту алгоритмів, що доцільно використати під час вдосконалення положень українського законодавства.

Висновки. Підсумовуючи викладене, слід констатувати, що жодна з розглянутих іноземних моделей не допускає використання систем ШІ як повністю автономного суб'єкта прийняття адміністративного рішення. У центрі європейської та євроатлантичної нормативної парадигми перебуває *людина*, тоді як алгоритм розглядається винятково як інструмент підтримки управлінської діяльності. Власне ця концепція, на нашу думку, пови-

нна бути покладена в основу майбутнього адміністративно-правового регулювання використання систем контролю на основі ШІ під час проведення кваліфікаційних іспитів членів екіпажів в Україні. Більш того, її імплементація має передбачати законодавче визначення правового статусу «AI-proctoring», обов'язковості алгоритмічного аудиту, нормативне закріплення права кандидата на отримання мотивованого пояснення результатів автоматизованого оцінювання, проведення оцінки впливу на права людини до введення відповідної системи в експлуатацію, а також спеціальний режим охорони професійної таємниці щодо інформації, сформованої алгоритмами ШІ. Вважаємо, що тільки за таких умов можливо досягти належного балансу між інтересами держави у забезпеченні об'єктивності кваліфікаційного оцінювання, міжнародними зобов'язаннями України та гарантіями захисту основоположних прав людини.

Список використаних джерел

1. Lareo X. Automated proctoring. *European Data Protection Supervisor*. URL: <https://www.edps.europa.eu/data-protection/technology-monitoring/techsonar/automated-proctoring>
2. International Convention on Standards of Training, Certification and Watchkeeping for Seafarers of 1978. URL: <https://www.imo.org/en/ourwork/humanelement/pages/stcw-convention.aspx>
3. Краковська А., Бабик М. Цифровізація адміністративних послуг в Україні: проблеми та перспективи розвитку. *Науковий вісник Ужгородського Національного Університету*. Серія: Право. 2022. Вип. 70. С. 329–334. DOI: <https://doi.org/10.24144/2307-3322.2022.70.52>
4. Кожухар О. Принцип прозорості в контексті правового регулювання систем штучного інтелекту. *Наукові записки НаУКМА*. 2025. Серія: Юридичні науки. Т. 15. С. 78–85. DOI: <https://doi.org/10.18523/2617-2607.2025.15.78-85>
5. Панкевич О.З. Право на приватність: царица незалежності особи. *Науковий вісник Львівського державного університету внутрішніх справ*. Серія юридична. 2017. Вип. 2. С. 47–56. <http://dspace.lvduvs.edu.ua/handle/1234567890/1761>
6. Менджул М., Мулеса О. Проблеми гарантування кібербезпеки у процесі транскордонного співробітництва під час воєнного стану. *Кібербезпека в транскордонному співробітництві*. Наукове видання (Збірник тез доповідей) Закарпатського угорського інституту імені Ференца Ракоці II / Редактори: Степан Черничко, Маріанна Марусинець, Єлизавета Молнар Д, Ганна Мелегачич та Оксана Мулеса. Берегове: ЗУІ ім. Ференца Ракоці II, 2024. (українською, англійською та угорською мовами). С. 35–37. <https://dspace.kme.org.ua/items/f7d61419-1539-45fe-a1e9-fde130074868>
7. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>
8. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>

9. Convention 108+. Convention for the protection of individuals with regard to the processing of personal data of 2018. URL: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf
10. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). URL: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>
11. Конституція України від 28.06.1996 №254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>
12. Про інформацію: Закон України від 02.10.1992 №2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
13. Про захист персональних даних: Закон України від 01.06.2010 №2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
14. Pashchuk T. Regulatory limits on Artificial Intelligence access to professional secrets in the digital age: an international legal perspective. *Legal, Economic Science and Praxis*. 2025. №16. P. 11-18. https://lesp.hu/wp-content/uploads/2026/02/2-Taras-Pashchuk_16_2025_p-11-18.pdf
15. Curtin D., Fia T. Cracking AI secrecy: (beyond) EU migration law and governance. *European Law Open*. 2026. P. 1-30. DOI: <https://doi.org/10.1017/elo.2025.10064>
16. Summary of the NATO Artificial Intelligence Strategy. NATO. 2021. URL: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2021/10/22/summary-of-the-nato-artificial-intelligence-strategy>
17. Summary of NATO's revised Artificial Intelligence (AI) strategy. NATO. 2024. URL: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy>
18. NATO's Digital Transformation Implementation Strategy 2.0. NATO. 2026. URL: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/05/26/natos-digital-transformation-implementation-strategy>
19. Remote invigilation in vocational and technical qualifications. 2023. URL: <https://www.gov.uk/government/publications/remote-invigilation-in-vocational-and-technical-qualifications>
20. Ofqual's approach to regulating the use of artificial intelligence in the qualifications sector. 2024. URL: <https://www.gov.uk/government/publications/ofquals-approach-to-regulating-the-use-of-artificial-intelligence-in-the-qualifications-sector>
21. Data protection impact assessment (DPIA). Autoriteit Persoonsgegevens. URL: <https://www.autoriteitpersoonsgegevens.nl/en/themes/basic-gdpr/gdpr-in-practice/data-protection-impact-assessment-dpia>
22. The National Strategy for Artificial Intelligence. 2020. URL: <https://www.regjeringen.no/en/documents/nasjonal-strategi-for-kunstig-intelligens/id2685594/>
23. Danish strategies for artificial intelligence. URL: <https://en.digst.dk/digital-governance/new-technologies/danish-strategies-for-artificial-intelligence/>
24. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST. 2023. URL: <https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf>
25. AI Risk Management Framework. NIST. 2026. URL: <https://www.nist.gov/itl/ai-risk-management-framework>

References:

1. Lareo X. Automated proctoring. European Data Protection Supervisor. URL: <https://www.edps.europa.eu/data-protection/technology-monitoring/techsonar/automated-proctoring> [In English].
2. International Convention on Standards of Training, Certification and Watchkeeping for Seafarers of 1978. URL: <https://www.imo.org/en/ourwork/humanelement/pages/stcw-convention.aspx> [In English].
3. Krakovska A., Babyk M. (2022). Tsyfrovizatsiia administratyvnykh posluh v Ukraini: problemy ta perspektyvy rozvytku [Digitalization of administrative services in Ukraine: challenges and development prospects]. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu. Seriya: Pravo (Scientific Bulletin of Uzhhorod National University. Series: Law)*. Vyp. 70. S. 329–334. DOI: <https://doi.org/10.24144/2307-3322.2022.70.52> [In Ukrainian].
4. Kozhukhar O. (2025). Pryntsyp prozorosti v konteksti pravovoho rehuliuвання system shtuchnoho intelektu [The Principle of Transparency in the Context of the Legal Regulation of Artificial Intelligence Sys-

tems]. Naukovi zapysky NaUKMA . Serii: Yurydychni nauky (NaUKMA Research Papers. Legal Sciences Series). T. 15. S. 78–85. DOI: <https://doi.org/10.18523/2617-2607.2025.15.78-85> [In Ukrainian].

5. Pankevych O.Z. (2017). Pravo na pryvatnist: tsaryna nezalezhnosti osoby [The Right to Privacy: The Realm of Personal Independence]. Naukovyi visnyk Lvivskoho derzhavnogo universytetu vnutrishnikh sprav. Serii: yurydychna (Scientific Bulletin of Lviv State University of Internal Affairs. Legal Series). Vyp. 2. S. 47–56. <http://dspace.lvduvs.edu.ua/handle/1234567890/1761> [In Ukrainian].

6. Mendzhul M., Mulesa O. (2024). Problemy harantuvannya kiberbezpeky u protsesi transkordonnoho spivrobitnytstva pid chas voiennoho stanu [Challenges of Ensuring Cybersecurity in Cross-Border Cooperation under Martial Law. Cybersecurity in Cross-Border Cooperation. Scientific Publication (Collection of Abstracts) Ferenc Rákóczi II Transcarpathian Hungarian Institute]. Kiberbezpeka v transkordonnomu spivrobitnytstvi. Naukove vydannia (Zbirnyk tez dopovidei)

Zakarpatskoho uhorskoho instytutu imeni Ferentsa Rakotsi II (Cybersecurity in Cross-Border Cooperation. Scientific Publication (Collection of Abstracts) Ferenc Rákóczi II Transcarpathian Hungarian Institute)/ Redaktery: Stepan Chernychko, Marianna Marusynets, Yelyzaveta Molnar D, Hanna Melehanych ta Oksana Mulesa. Berehove: ZUI im. Ferentsa Rakotsi II. (ukrainskoiiu, anhliiskoiu ta uhorskoiiu movamy). S. 35–37. <https://dspace.kme.org.ua/items/f7d61419-1539-45fe-a1e9-fde130074868> [In Ukrainian, English, Hungarian].

7. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> [In English].

8. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> [In English].

9. Convention 108 +. Convention for the protection of individuals with regard to the processing of personal data of 2018. URL: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf [In English].

10. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). URL: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng> [In English].

11. Konstytutsiia Ukrainy [Constitution of Ukraine] vid 28.06.1996 №254k/96-VR. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text> [In Ukrainian].

12. Pro informatsiiu: Zakon Ukrainy [On Information: Law of Ukraine] vid 02.10.1992 №2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> [In Ukrainian].

13. Pro zakhyst personalnykh danykh: Zakon Ukrainy [On Personal Data Protection: Law of Ukraine] vid 01.06.2010 №2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> [In Ukrainian].

14. Pashchuk T. Regulatory limits on Artificial Intelligence access to professional secrets in the digital age: an international legal perspective. Legal, Economic Science and Praxis. 2025. № 16. P. 11–18. https://lesp.hu/wp-content/uploads/2026/02/2-Taras-Pashchuk_16_2025_p-11-18.pdf [In English].

15. Curtin D., Fia T. (2026). Cracking AI secrecy: (beyond) EU migration law and governance. *European Law Open*. P. 1–30. DOI: <https://doi.org/10.1017/elo.2025.10064> [In English].

16. Summary of the NATO Artificial Intelligence Strategy. NATO. 2021. URL: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2021/10/22/summary-of-the-nato-artificial-intelligence-strategy> [In English].

17. Summary of NATO's revised Artificial Intelligence (AI) strategy. NATO. 2024. URL: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy> [In English].

18. NATO's Digital Transformation Implementation Strategy 2.0. NATO. 2026. URL: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/05/26/natos-digital-transformation-implementation-strategy> [In English].

19. Remote invigilation in vocational and technical qualifications. 2023. URL: <https://www.gov.uk/government/publications/remote-invigilation-in-vocational-and-technical-qualifications> [In English].

20. Ofqual's approach to regulating the use of artificial intelligence in the qualifications sector. 2024. URL: <https://www.gov.uk/government/publications/ofqual-approach-to-regulating-the-use-of-artificial-intelligence-in-the-qualifications-sector> [In English].
21. Data protection impact assessment (DPIA). Autoriteit Persoonsgegevens. URL: <https://www.autoriteitpersoonsgegevens.nl/en/themes/basic-gdpr/gdpr-in-practice/data-protection-impact-assessment-dpia> [In English].
22. The National Strategy for Artificial Intelligence. 2020. URL: <https://www.regjeringen.no/en/documents/nasjonal-strategi-for-kunstig-intelligens/id2685594/> [In English].
23. Danish strategies for artificial intelligence. URL: <https://en.digst.dk/digital-governance/new-technologies/danish-strategies-for-artificial-intelligence/> [In English].
24. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST. 2023. URL: <https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf> [In English].
25. AI Risk Management Framework. NIST. 2026. URL: <https://www.nist.gov/itl/ai-risk-management-framework> [In English].

Creative Commons Attribution 4.0
International (CC BY 4.0)



Дата першого надходження статті до видання: 31.07.2026
Дата прийняття статті до друку після рецензування: 03.09.2026
Дата публікації (оприлюднення) статті: 00.00.2026

УДК 343

DOI <https://doi.org/10.32782/2311-8040/2026-2-2>**Боровікова Віталіна Станіславівна,**

старший науковий співробітник відділу організації наукової діяльності,
Львівський державний університет внутрішніх справ,
вулиця Городоцька, 26, Львів, 79000, Україна
ORCID: <https://orcid.org/0000-0003-4401-4562>

Баб'як Андрій Васильович,

кандидат юридичних наук, доцент,
завідувач кафедри оперативно-розшукової діяльності,
Львівський державний університет внутрішніх справ,
вулиця Городоцька, 26, Львів, 79000, Україна
ORCID: <https://orcid.org/0000-0002-2284-3864>

ІНФОРМАЦІЙНО-АНАЛІТИЧНА ДІЯЛЬНІСТЬ У ПРАВООХОРОННИХ ОРГАНАХ УКРАЇНИ: ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ТА НОРМАТИВНЕ ЗАБЕЗПЕЧЕННЯ

Анотація. У статті досліджено теоретико-правові засади інформаційно-аналітичної діяльності правоохоронних органів України та особливості її нормативно-правового забезпечення в умовах цифрової трансформації суспільства. Обґрунтовано актуальність дослідження з огляду на зростання ролі інформації як стратегічного ресурсу у сфері забезпечення правопорядку, протидії злочинності та прийняття ефективних управлінських рішень. Визначено, що інформаційно-аналітична діяльність є комплексним процесом, який охоплює збір, накопичення, систематизацію, обробку, аналіз та інтерпретацію інформації з метою формування об'єктивного уявлення про стан криміногенної ситуації та вироблення оптимальних заходів реагування.

Проаналізовано основні наукові підходи до розуміння сутності інформаційно-аналітичного забезпечення правоохоронної діяльності, розкрито його функціональне призначення та значення для підвищення ефективності діяльності правоохоронних органів. Встановлено, що сучасні інформаційно-аналітичні технології сприяють своєчасному виявленню кримінальних загроз, прогнозуванню тенденцій злочинності, координації діяльності суб'єктів правоохоронної системи та оптимізації процесів прийняття управлінських рішень.

Особливу увагу приділено дослідженню нормативно-правової бази, що регламентує інформаційно-аналітичну діяльність в Україні. Розглянуто положення Конституції України, законів України «Про Національну поліцію», «Про оперативно-розшукову діяльність», «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про захист персональних даних» та інших нормативно-правових актів. Визначено їхню роль у формуванні правових засад збору, обробки, використання та захисту інформації у правоохоронній сфері. Наголошено на необхідності забезпечення балансу між ефективністю інформаційно-аналітичної діяльності та дотриманням конституційних прав людини, насамперед права на приватність і захист персональних даних.

Зроблено висновок, що чинна система нормативно-правового регулювання створює належні передумови для функціонування інформаційно-аналітичного забезпечення правоохоронних органів, однак потребує подальшого вдосконалення в контексті розвитку цифрових технологій, інтеграції інформаційних ресурсів та гармонізації національного законодавства із європейськими стандартами. Перспективним напрямом розвитку визначено впровадження сучасних аналітичних інструментів, технологій штучного інтелекту та прогнозової аналітики у практику правоохоронної діяльності.

Ключові слова: інформаційно-аналітична діяльність, правоохоронні органи, інформаційно-аналітичне забезпечення, нормативно-правове регулювання, Національна поліція України, інформаційна безпека, персональні дані, кримінальний аналіз, правоохоронна діяльність, цифровізація, аналітичні системи, штучний інтелект.

Borovikova Vitalina, Babiak Andrii. INFORMATION AND ANALYTICAL ACTIVITIES IN THE LAW ENFORCEMENT AGENCIES OF UKRAINE: THEORETICAL AND LEGAL FOUNDATIONS AND REGULATORY FRAMEWORK

Abstract. *The article examines the theoretical and legal foundations of information and analytical activities within the system of Ukrainian law enforcement agencies and analyzes the specific features of their legal and regulatory framework in the context of the ongoing digital transformation of society. The relevance of the study is substantiated by the growing role of information as a strategic resource for maintaining public order, combating crime, and supporting effective managerial decision-making.*

It is established that information and analytical activity constitutes a comprehensive process involving the collection, accumulation, systematization, processing, analysis, and interpretation of information aimed at developing an objective understanding of the criminogenic situation and formulating appropriate response measures. The article analyzes the principal scholarly approaches to the concept of information and analytical support for law enforcement activities, revealing its functional purpose and significance in enhancing the effectiveness of law enforcement agencies.

The study demonstrates that modern information and analytical technologies facilitate the timely identification of criminal threats, forecasting of crime trends, coordination among law enforcement entities, and optimization of decision-making processes. Particular attention is paid to the analysis of the regulatory framework governing information and analytical activities in Ukraine. The provisions of the Constitution of Ukraine, the Laws of Ukraine "On the National Police," "On Operational and Investigative Activities," "On Information," "On the Protection of Information in Information and Communication Systems," and "On Personal Data Protection," as well as other relevant legal acts, are examined. Their role in establishing the legal foundations for the collection, processing, use, and protection of information in the law enforcement sphere is determined.

The article emphasizes the necessity of maintaining a balance between the effectiveness of information and analytical activities and the protection of fundamental human rights, particularly the right to privacy and personal data protection. It is concluded that the existing legal framework provides an adequate basis for the functioning of information and analytical support within law enforcement agencies; however, it requires further improvement in light of technological advancements, integration of information resources, and harmonization of national legislation with European standards. The implementation of advanced analytical tools, artificial intelligence technologies, and predictive analytics is identified as a promising direction for the further development of law enforcement practice.

Key words: *information and analytical activity, law enforcement agencies, information and analytical support, legal regulation, National Police of Ukraine, information security, personal data, criminal analysis, law enforcement activity, digitalization, analytical systems, artificial intelligence.*

Вступ. В умовах стрімкої цифровізації суспільства, зростання обсягів інформації та ускладнення криміногенної ситуації особливого значення набуває ефективне інформаційно-аналітичне забезпечення діяльності правоохоронних органів. Сучасна правоохоронна діяльність потребує не лише своєчасного отримання інформації, а й її комплексного аналізу, оцінювання та прогнозування з метою прийняття обґрунтованих управлінських і процесуальних рішень. Саме інформаційно-аналітична діяльність виступає важливим інструментом виявлення закономірностей злочинності, визначення криміногенних ризиків, координації роботи правоохоронних органів та підвищення ефективності протидії правопорушенням.

Актуальність дослідження зумовлена необхідністю вдосконалення механізмів обробки та використання інформації в умовах розвитку

сучасних інформаційних технологій, а також потребою забезпечення балансу між інтересами держави у сфері безпеки та дотриманням прав і свобод людини під час здійснення аналітичної діяльності. Водночас інтеграція України до європейського правового простору потребує адаптації національного законодавства до міжнародних стандартів у сфері інформаційної безпеки, захисту персональних даних та правоохоронної діяльності.

Проблематика інформаційно-аналітичного забезпечення правоохоронної діяльності знайшла відображення у працях вітчизняних і зарубіжних науковців, зокрема А. В. Кубасенка, П. П. Латковського, В. Терехова, О. В. Лисенка, Дж. Реткліффа та інших дослідників. Однак динамічний розвиток інформаційних технологій і постійне оновлення нормативно-правової бази обумовлюють необхідність подальшого наукового осмислення теоретичних

і правових засад інформаційно-аналітичної діяльності правоохоронних органів.

Метою статті є дослідження сутності та значення інформаційно-аналітичної діяльності в системі правоохоронних органів України, а також аналіз сучасного стану її нормативно-правового забезпечення та визначення перспектив його вдосконалення.

Матеріали та методи. Матеріальну основу дослідження становлять нормативно-правові акти України, що регулюють інформаційно-аналітичну діяльність правоохоронних органів, зокрема Конституція України, закони України «Про Національну поліцію», «Про оперативно-розшукову діяльність», «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про захист персональних даних», а також наукові праці вітчизняних і зарубіжних учених, присвячені питанням інформаційно-аналітичного забезпечення правоохоронної діяльності.

Методологічну основу дослідження становить комплекс загальнонаукових і спеціально-юридичних методів пізнання. Діалектичний метод використано для дослідження сутності та закономірностей розвитку інформаційно-аналітичної діяльності в правоохоронній сфері. Формально-юридичний метод застосовано під час аналізу нормативно-правових актів, що регламентують порядок збору, обробки, використання та захисту інформації. За допомогою системно-структурного методу визначено місце інформаційно-аналітичної діяльності в системі забезпечення правоохоронної функції держави та встановлено взаємозв'язок її окремих елементів.

Порівняльно-правовий метод використано для оцінки сучасних тенденцій розвитку правового регулювання інформаційно-аналітичної діяльності та визначення перспектив його гармонізації з європейськими стандартами. Метод аналізу й синтезу дав змогу узагальнити наукові підходи до розуміння сутності інформаційно-аналітичного забезпечення та сформулювати висновки щодо напрямів удосконалення нормативно-правової бази у цій сфері.

Результати. Аналітичне забезпечення правоохоронної діяльності доцільно розглядати як

комплексну систему організаційних, інформаційних та методологічних заходів, спрямованих на збір, обробку, аналіз та інтерпретацію даних із метою формування обґрунтованих управлінських і процесуальних рішень у сфері протидії злочинності. У сучасних умовах воно виступає не лише допоміжним інструментом, а й самостійною функціональною підсистемою правоохоронної діяльності, що забезпечує її ефективність та проактивність. У науковій літературі підкреслюється, що інформаційно-аналітичний компонент є ключовим елементом управління правоохоронними органами, оскільки дозволяє трансформувати первинні дані у знання, необхідні для прийняття рішень [1, с. 204].

Зміст аналітичного забезпечення охоплює послідовний процес: первинний збір інформації з різних джерел (оперативних, відкритих, статистичних, цифрових), її систематизацію, подальшу обробку із застосуванням аналітичних методів (структурний, порівняльний, мережевий аналіз), а також інтерпретацію результатів у вигляді аналітичних продуктів. Такий підхід забезпечує можливість не лише фіксації кримінальних явищ, але й виявлення прихованих закономірностей, прогнозування ризиків та моделювання потенційного розвитку криміногенної ситуації. Як зазначається у наукових дослідженнях, інформаційно-аналітична діяльність у правоохоронній сфері є складовою управлінського механізму, що охоплює як соціальну, так і безпекову функції держави [2, с. 87].

Важливим аспектом є відмежування аналітичного забезпечення від суміжних категорій. Насамперед, інформаційна робота має більш загальний характер і включає збір та поширення інформації без обов'язкового її глибинного аналізу. Натомість аналітичне забезпечення передбачає інтерпретаційний рівень обробки даних, що завершується формуванням висновків для прийняття рішень. Кримінальний аналіз є складовою аналітичного забезпечення, однак він має більш прикладний характер і спрямований на виявлення закономірностей злочинної діяльності, географії злочинів та профілювання злочинців. Кримінальна роз-

відка натомість орієнтована на отримання випереджувальної інформації про злочинні наміри та структури, часто із використанням оперативних методів і конфіденційних джерел.

Таким чином, аналітичне забезпечення виступає інтегруючою категорією, що об'єднує інформаційну роботу, кримінальний аналіз і кримінальну розвідку в єдину систему підтримки прийняття рішень у правоохоронній діяльності. Його сутність полягає у трансформації даних у знання, здатні забезпечити стратегічне та тактичне управління у сфері протидії злочинності, особливо в умовах цифровізації та зростання складності кримінальних процесів.

Аналітичне забезпечення посідає центральне місце в сучасній системі протидії злочинності, виступаючи ключовим механізмом переходу від реактивної моделі правоохоронної діяльності до проактивної. У межах концепції *intelligence-led policing* (далі – ILP) саме аналітика визначає пріоритети діяльності правоохоронних органів, формує основу для розподілу ресурсів та забезпечує прийняття рішень, орієнтованих на випередження злочинних загроз. Як підкреслюється у класичних дослідженнях Дж. Раткліффа, ILP передбачає системне використання аналітичних продуктів для стратегічного управління поліцією та концентрації зусиль на найбільш небезпечних кримінальних явищах [3].

У межах цієї моделі аналітичне забезпечення виконує функцію інтелектуального ядра системи протидії злочинності, забезпечуючи безперервний цикл «дані – аналіз – рішення – дія – оцінка». Такий підхід дозволяє не лише реагувати на вже вчинені кримінальні правопорушення, але й ідентифікувати потенційні загрози, прогнозувати їх розвиток та формувати превентивні стратегії. У науковій літературі наголошується, що ефективність ILP безпосередньо залежить від якості аналітичних даних та рівня інтеграції інформаційних систем правоохоронних органів.

Важливим аспектом є вплив аналітичного забезпечення на стратегічне планування діяльності правоохоронних органів. На стратегічному рівні аналітика забезпечує формування

довгострокових пріоритетів у сфері протидії злочинності, визначення криміногенних тенденцій та розробку політик безпеки. Зокрема, аналіз великих масивів даних дозволяє виявляти структурні зміни у злочинності, включаючи зростання кіберзлочинів, транснаціональних злочинних мереж та гібридних загроз. Це створює підґрунтя для прийняття управлінських рішень на рівні державної політики у сфері внутрішньої безпеки [4, с. 162–167].

На тактичному рівні аналітичне забезпечення використовується для підтримки оперативної діяльності підрозділів поліції та інших правоохоронних органів. Воно дозволяє визначати “гарячі точки” злочинності (*hot spots policing*), оптимізувати патрулювання, розподіляти ресурси та підвищувати ефективність реагування на конкретні події. Дослідження в галузі *predictive policing* свідчать, що застосування аналітичних моделей значно підвищує точність прогнозування місць і часу ймовірного вчинення злочинів, що, у свою чергу, сприяє зниженню рівня злочинності [5, с. 27].

Таким чином, аналітичне забезпечення виступає системоутворюючим елементом сучасної правоохоронної діяльності, який інтегрує стратегічний і тактичний рівні управління. Його впровадження забезпечує не лише підвищення ефективності реагування на злочинність, але й формування превентивної моделі безпеки, орієнтованої на прогнозування та попередження кримінальних загроз.

Аналітичне забезпечення правоохоронної діяльності являє собою складну багаторівневу систему, що охоплює сукупність організаційних, інформаційних, методичних і технологічних компонентів, спрямованих на забезпечення ефективного функціонування правоохоронних органів. Його структура формується відповідно до логіки аналітичного циклу, який включає збір інформації, її обробку та аналіз, підготовку аналітичних продуктів і використання отриманих результатів у процесі прийняття управлінських та процесуальних рішень. У сучасних умовах цифровізації суспільства аналітичне забезпечення перетворюється на один із ключових інструментів

підвищення ефективності діяльності правоохоронних органів, оскільки дозволяє оперативно реагувати на криміногенні загрози та прогнозувати їх подальший розвиток [6, с. 454; 7, с. 103–105].

Першим структурним елементом аналітичного забезпечення виступає збір даних з різних джерел. Ефективність подальшого аналізу безпосередньо залежить від повноти, достовірності та актуальності інформації, що надходить до аналітичних підрозділів. Джерелами таких даних можуть бути відомчі інформаційні системи, державні реєстри, матеріали кримінальних проваджень, результати оперативно-розшукової діяльності, статистична інформація, відкриті джерела (OSINT), повідомлення громадян, а також дані міжнародного інформаційного обміну. Науковці підкреслюють, що сучасна інформаційно-аналітична діяльність правоохоронних органів характеризується інтеграцією великої кількості різно-рідних інформаційних ресурсів, що дозволяє формувати комплексне уявлення про криміногенну ситуацію та фактори, які впливають на її розвиток [6, 456; 8, с. 282].

Наступним етапом є аналітична обробка інформації, яка становить змістовне ядро всієї системи аналітичного забезпечення. На цьому рівні здійснюється перевірка, систематизація, узагальнення та інтерпретація отриманих даних. Аналітична діяльність передбачає використання різноманітних методів, серед яких особливе значення мають аналіз і синтез, порівняння, класифікація, статистичне моделювання, мережевий аналіз, кримінологічне прогнозування та сценарне планування. Завдяки таким методам відбувається виявлення закономірностей, тенденцій і взаємозв'язків між окремими подіями та явищами. У сучасних умовах дедалі більшого значення набувають технології Big Data та штучного інтелекту, які дозволяють обробляти значні масиви інформації та автоматично виявляти приховані кореляції між даними. У результаті аналітична обробка забезпечує трансформацію первинної інформації у нові знання, придатні для практичного використання правоохоронними органами [2, с. 87; 7, с. 105–107].

Важливою функцією аналітичного забезпечення є формування аналітичних продуктів. Під аналітичними продуктами розуміють результати аналітичної діяльності, оформлені у вигляді документів, звітів, довідок, прогнозів, інформаційних бюлетенів, карт криміногенної обстановки, ризик-аналізів та інших матеріалів, призначених для використання керівництвом або оперативними підрозділами. Саме аналітичні продукти виступають основною формою передачі знань від аналітичних підрозділів до суб'єктів прийняття рішень. Їхня якість визначається не лише точністю викладених даних, але й здатністю надавати практично значущі рекомендації щодо реагування на конкретні загрози. Дослідники зазначають, що формування якісного аналітичного продукту передбачає не просте накопичення інформації, а її комплексну оцінку та вироблення обґрунтованих висновків щодо розвитку криміногенної ситуації [7, с. 107].

Завершальним елементом структури аналітичного забезпечення є підтримка управлінських рішень. Саме на цьому етапі реалізується практична цінність аналітичної діяльності, оскільки результати аналізу використовуються для визначення пріоритетів правоохоронної політики, розподілу ресурсів, планування оперативно-службової діяльності та оцінки ефективності вже вжитих заходів. Аналітичне забезпечення сприяє прийняттю рішень як на стратегічному, так і на тактичному рівнях управління. На стратегічному рівні воно допомагає визначати основні напрями боротьби зі злочинністю та прогнозувати перспективи її розвитку, тоді як на тактичному рівні забезпечує оперативне реагування на конкретні кримінальні загрози. У науковій літературі наголошується, що інформаційно-аналітичне забезпечення є невід'ємним елементом сучасного управління правоохоронною системою, оскільки забезпечує науково обґрунтований характер управлінських рішень та підвищує їх ефективність [2, с. 87].

Таким чином, структура аналітичного забезпечення правоохоронної діяльності охоплює взаємопов'язані елементи – збір даних, їх аналітичну обробку, формування аналі-

тичних продуктів та підтримку прийняття управлінських рішень. Лише комплексне функціонування всіх зазначених компонентів забезпечує ефективне виконання аналітичної функції правоохоронних органів та створює передумови для переходу до сучасної моделі управління, заснованої на знаннях, прогнозуванні та випереджувальному реагуванні на кримінальні загрози.

Методологічні основи аналітичної діяльності становлять сукупність наукових підходів, принципів і методів, за допомогою яких здійснюється отримання, обробка, інтерпретація та використання інформації у сфері правоохоронної діяльності. Ефективність аналітичного забезпечення значною мірою залежить від правильного вибору методологічного інструментарію, який дозволяє не лише фіксувати наявний стан злочинності, але й виявляти закономірності її розвитку, прогнозувати майбутні тенденції та формувати науково обґрунтовані рекомендації для прийняття управлінських рішень. У сучасних умовах аналітична діяльність ґрунтується на поєднанні загальнонаукових і спеціальних методів дослідження, що забезпечує комплексність вивчення криміногенних процесів та явищ [9, с. 141].

Основу методології аналітичної діяльності складають загальнонаукові методи пізнання. Одним із найважливіших серед них є аналіз, який передбачає розчленування складного явища на окремі складові елементи з метою їх детального вивчення. У правоохоронній практиці аналіз використовується для дослідження структури злочинності, причин та умов вчинення кримінальних правопорушень, характеристик осіб правопорушників, особливостей кримінальних зв'язків та інших факторів, що мають значення для протидії злочинності. Завдяки аналітичним процедурам правоохоронні органи отримують можливість виявляти приховані закономірності та встановлювати причинно-наслідкові зв'язки між окремими кримінальними подіями.

Невід'ємним доповненням аналізу виступає синтез, який полягає в об'єднанні окремих фактів, показників та результатів дослідження в єдину систему знань. Якщо аналіз дозволяє

розкрити структуру досліджуваного явища, то синтез забезпечує формування цілісного уявлення про криміногенну ситуацію та її тенденції. Саме поєднання аналізу і синтезу створює передумови для вироблення комплексних висновків щодо стану злочинності та визначення оптимальних шляхів реагування на існуючі загрози.

Важливе значення у процесі аналітичної діяльності має метод індукції, який передбачає перехід від окремих фактів до загальних висновків. У правоохоронній сфері індуктивний підхід застосовується під час узагальнення результатів оперативно-службової діяльності, аналізу статистичних даних та виявлення типових закономірностей злочинної поведінки. На основі накопичених емпіричних даних формуються узагальнення щодо динаміки злочинності, ефективності діяльності правоохоронних органів та перспектив розвитку криміногенної ситуації.

Поряд із загальнонауковими методами особливе місце в системі аналітичної діяльності займають спеціальні методи, насамперед кримінальний аналіз. У сучасній науковій літературі кримінальний аналіз розглядається як один із ключових інструментів інформаційно-аналітичного забезпечення правоохоронної діяльності, спрямований на виявлення закономірностей злочинної активності, аналіз кримінальних зв'язків та підтримку процесу прийняття рішень [10, с. 353]. Кримінальний аналіз забезпечує перетворення значних обсягів інформації на практично корисні знання шляхом використання статистичних, логічних, математичних і візуалізаційних методів. Його застосування дозволяє встановлювати осіб, причетних до злочинної діяльності, визначати характер їхніх взаємозв'язків, виявляти осередки злочинності та прогнозувати подальший розвиток кримінальних процесів [9, с. 143–144].

Суттєвого значення набуває також мережевий аналіз, який активно використовується для дослідження організованих злочинних груп, терористичних організацій, корупційних схем та інших складних соціальних мереж. Методологія мережевого аналізу базується на вивчен-

ні взаємозв'язків між окремими суб'єктами, що дозволяє виявляти центральних учасників злочинних мереж, визначати канали передачі інформації та встановлювати структуру кримінальних організацій. Застосування цього методу значно підвищує ефективність протидії організованій злочинності, оскільки дає можливість правоохоронним органам концентрувати зусилля на найбільш значущих елементах злочинної мережі [11, с. 22].

Одним із найважливіших напрямів сучасної аналітичної діяльності є прогнозування злочинності. Прогностичні методи дозволяють оцінювати ймовірність виникнення певних кримінальних загроз, прогнозувати зміни рівня злочинності та визначати найбільш вразливі сфери суспільних відносин. Для цього використовуються статистичні моделі, математичне моделювання, сценарний аналіз, геоінформаційні технології та інструменти штучного інтелекту. У результаті прогнозування формується науково обґрунтована база для стратегічного та тактичного планування діяльності правоохоронних органів, що відповідає сучасним концепціям *intelligence-led policing* та *risk-based policing* [9, с. 145; 10, с. 355–356].

Отже, методологічні основи аналітичної діяльності формуються шляхом поєднання загальнонаукових методів пізнання та спеціальних інструментів кримінального аналізу. Аналіз, синтез та індукція забезпечують теоретичну основу дослідження криміногенних процесів, тоді як кримінальний аналіз, мережевий аналіз і прогнозування злочинності дозволяють трансформувати інформацію у практичні знання, необхідні для ефективного функціонування правоохоронної системи. Комплексне використання зазначених методів створює підґрунтя для прийняття обґрунтованих управлінських рішень та підвищення результативності протидії сучасним формам злочинності.

Нормативно-правова база України, що регулює інформаційно-аналітичну діяльність у правоохоронній сфері, формує комплексну систему правових норм, які визначають повноваження суб'єктів, порядок обробки інформації та гарантії захисту даних. Її ядро

становлять закони загального та спеціального характеру, що регламентують діяльність Національної поліції, оперативно-розшукову діяльність, захист інформації та персональних даних. У сукупності ці акти забезпечують правові передумови функціонування аналітичних систем у сфері протидії злочинності та формують баланс між інтересами безпеки держави та правами людини.

Ключове значення має Закон України «Про Національну поліцію» від 02.07.2015 № 580-VIII, який прямо закріплює повноваження поліції щодо здійснення інформаційно-аналітичної діяльності. Відповідно до статті 25 цього Закону, поліція має право формувати та використовувати інформаційні ресурси, здійснювати обробку даних, а також створювати аналітичні системи для виконання покладених на неї функцій. При цьому законодавець підкреслює, що така діяльність здійснюється виключно в межах реалізації законодавчо визначених повноважень, що забезпечує її легітимність і контрольованість. Це положення є базовим для розуміння місця аналітичного забезпечення у структурі правоохоронної діяльності.

Важливим елементом нормативного регулювання виступає Закон України «Про оперативно-розшукову діяльність» від 18.02.1992 № 2135-XII, який визначає правові засади отримання та використання інформації про злочинні прояви. Саме в межах оперативно-розшукової діяльності формується значна частина інформаційної бази для подальшого аналітичного опрацювання. Закон передбачає можливість використання спеціальних засобів і методів для виявлення та документування злочинної діяльності, що створює підґрунтя для подальшого кримінального аналізу та прогнозування криміногенних процесів.

Не менш важливу роль відіграє законодавство у сфері інформаційної безпеки та захисту даних. Закони України «Про інформацію» від 02.10.1992 № 2657-XII, «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 № 80/94-ВР та «Про захист персональних даних» від 01.06.2010 № 2297-VI визначають правовий режим інформації, порядок її збору, збері-

гання, обробки та захисту. У контексті аналітичної діяльності ці нормативні акти встановлюють принципи законності, цільового використання та мінімізації даних, що є особливо важливим при роботі з великими масивами персональної та оперативної інформації. Таким чином, правове регулювання забезпечує запобігання зловживанням та гарантує дотримання прав людини під час здійснення аналітичних процедур.

Окрему групу становлять підзаконні нормативно-правові акти, що деталізують порядок функціонування інформаційних систем Національної поліції, ведення обліків та обміну інформацією між правоохоронними органами. Вони забезпечують практичну реалізацію законодавчих положень і визначають технічні та організаційні аспекти аналітичної діяльності. У наукових дослідженнях підкреслюється, що саме рівень інтеграції інформаційних систем та якість нормативного регулювання визначають ефективність аналітичного забезпечення правоохоронної діяльності в сучасних умовах цифровізації.

Отже, нормативно-правова база України у сфері інформаційно-аналітичної діяльності є багаторівневою та комплексною. Вона охоплює як загальні принципи функціонування правоохоронних органів, так і спеціальні норми щодо обробки інформації та захисту даних. Її подальший розвиток має бути спрямований на гармонізацію з європейськими стандартами, цифровізацію процедур обробки інформації та підвищення ефективності аналітичного забезпечення у сфері протидії злочинності.

Висновки. У результаті проведеного дослідження встановлено, що інформаційно-аналітична діяльність є невід'ємною складовою сучасної правоохоронної діяльності та важливим інструментом забезпечення ефективного виявлення, попередження і розслідування правопорушень. Її зміст полягає у систематичному зборі, обробці, аналізі та використанні інформації для прийняття обґрунтованих управлінських і процесуальних рішень.

З'ясовано, що нормативно-правове регулювання інформаційно-аналітичної діяльності в Україні має комплексний характер і охоплює норми Конституції України, спеціального законодавства у сфері правоохоронної діяльності, інформаційної безпеки та захисту персональних даних. Чинна правова база створює необхідні передумови для функціонування інформаційно-аналітичних систем, однак потребує подальшого вдосконалення з урахуванням сучасних викликів цифровізації та європейських стандартів захисту інформації.

Встановлено, що підвищення ефективності інформаційно-аналітичного забезпечення правоохоронних органів безпосередньо залежить від рівня інтеграції інформаційних ресурсів, впровадження сучасних аналітичних технологій та належного нормативного врегулювання процесів обробки інформації.

Перспективи подальших досліджень вбачаються у вивченні можливостей застосування технологій штучного інтелекту, великих даних та прогнозної аналітики в діяльності правоохоронних органів України, а також у розробленні механізмів їх правового регулювання відповідно до європейських стандартів.

Список використаних джерел:

1. Кубасенко, А. В. Інформаційно-аналітичне забезпечення оцінки ефективності діяльності правоохоронних органів: погляд на проблему. *Київський часопис права*. 2023. № 1. С. 202–208. <https://doi.org/10.32782/klj/2023.1.30>
2. Захожай В.Б. Інформаційно-аналітичне забезпечення управління правоохоронною та соціально-економічною діяльністю (на засадах методології та практики прикладної статистики). *Статистика України*. 2023. № 100(1). С. 86–91. [https://doi.org/10.31767/su.1\(100\)2023.01.08](https://doi.org/10.31767/su.1(100)2023.01.08)
3. Jerry H. Ratcliffe. *Intelligence-led Policing*. Routledge, 2012. URL: https://books.google.com.ua/books/about/Intelligence_led_Policing.html?hl=lv&id=LXEQBAABQBAJ&redir_esc=y
4. Alraggad M.M., Almahasneh A.A.A.A., Borovikova V., Zhyvko Z., Komissarchuk Y. The policy of rethinking the criminal process in the national security system: The impact of digitalisation on working with electronic evidence. *Social and Legal Studios*. 2024. № 7(2). P. 162–170. <https://doi.org/10.32518/sals2.2024.162>

5. Christopher S. Koper, Weiwei Liu, Bruce G. Taylor, Xiaoyun Wu, William D. Johnson, Jackie Sheridan. The Effects of Hot Spot Policing on Community Experiences and Perceptions in a Time of COVID-19 and Calls for Police Reform. *Police Quarterly*. 2023. P. 1-43. URL: <https://nij.ojp.gov/library/publications/effects-hot-spot-policing-community-experiences-and-perceptions-time-covid-19>

6. Латковський П.П. Інформаційно-аналітичне забезпечення правоохоронної діяльності. *Науковий вісник Ужгородського Національного Університету, Серія право*. Вип. 90. Ч. 5. 2025. С. 453–458. <https://doi.org/10.24144/2307-3322.2025.90.5.61>

7. Терехов В. Питання інформаційно-аналітичних досліджень у сфері правоохоронної діяльності. *Актуальні проблеми правознавства*. № 3 (27). 2021. С. 103–109. DOI:10.35774/app2021.03.103

8. Lysenko O.V., Lunhol O.M., Haborets O.A. Law enforcement information and analytical support. *Актуальні питання у сучасній науці*. Iss. № 3(9). 2023. P. 281–291. DOI: [https://doi.org/10.52058/2786-6300-2023-3\(9\)-281-291](https://doi.org/10.52058/2786-6300-2023-3(9)-281-291)

9. Моца В.В. Теоретико-методологічні засади використання кримінального аналізу оперативними підрозділами правоохоронних органів України. *Науковий вісник Ужгородського Національного Університету*. 2022. № 2. С. 141–147. <https://doi.org/10.24144/2307-3322.2022.73.53>

10. Різвано В., Свистун І., Копилов, Е. Кримінальний аналіз: сутність та аналітичні основи. *UNIVERSUM*. 2025. № (27). С. 352–359. URL: <https://archive.liga.science/index.php/universum/article/view/2565>

11. Овсянюк Д. І. Методологічні засади тактичного аналізу та аналізу оперативних даних під час розслідування злочинів, пов'язаних з незаконним обігом наркотиків : метод. рек. Київ : НАВС, 2024. 50 с. URL: <https://elar.navs.edu.ua/server/api/core/bitstreams/9f693faf-930e-4f40-9127-87d4be005233/content>

References:

1. Kubaienko, A. V. (2023). Informatsiino-analitychne zabezpechennia otsinky efektyvnosti diialnosti pravookhoronnykh orhaniv: pohliad na problemu [Information and analytical support for assessing the effectiveness of law enforcement agencies: a view on the problem]. *Kyivskiy chasopys prava – Kyiv Journal of Law*, 1, 202–208. <https://doi.org/10.32782/kj/2023.1.30> [in Ukrainian].

2. Zakhozhai, V.B. (2023). Informatsiino-analitychne zabezpechennia upravlinnia pravookhoronnoiu ta sotsialno-ekonomichnoiu diialnistiu (na zasadakh metodolohii ta praktyky prykladnoi statystyky) [Information and Analytical Support for the Management of Law Enforcement and Socio-Economic Activities (on the Basis of Methodologies and Practices of Applied Statistics)]. *Sotsialna statystyka – Social statistics*, 100(1), 86–91. [https://doi.org/10.31767/su.1\(100\)2023.01.08](https://doi.org/10.31767/su.1(100)2023.01.08) [in Ukrainian].

3. Jerry, H. (2012). Ratcliffe. Intelligence-led Policing. Routledge. Retrieved from https://books.google.com.ua/books/about/Intelligence_led_Policing.html?hl=lv&id=LXEQBAAAQBAJ&redir_esc=y [in English].

4. Alraggad, M.M., Almahasneh, A.A.A.A., Borovikova, V., Zhyvko, Z., & Komissarchuk, Y. (2024). The policy of rethinking the criminal process in the national security system: The impact of digitalisation on working with electronic evidence. *Social and Legal Studios*, 7(2), 162–170. <https://doi.org/10.32518/sals2.2024.162> [in English].

5. Christopher S. Koper, Weiwei Liu, Bruce G. Taylor, Xiaoyun Wu, William D. Johnson, Jackie Sheridan. (2023). The Effects of Hot Spot Policing on Community Experiences and Perceptions in a Time of COVID-19 and Calls for Police Reform. *Police Quarterly*. P. 1–43. Retrieved from <https://nij.ojp.gov/library/publications/effects-hot-spot-policing-community-experiences-and-perceptions-time-covid-19> [in English].

6. Latkovskiy, P.P. (2025). Informatsiino-analitychne zabezpechennia pravookhoronnoi diialnosti [Information and analytical support for law enforcement activities]. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu, Seriiia pravo – Scientific Bulletin of the Uzhhorod National University, Law Series*, 90, Ch. 5, 453–458. <https://doi.org/10.24144/2307-3322.2025.90.5.61> [in Ukrainian].

7. Terekhov, V. (2021). Pytannia informatsiino-analitychnykh doslidzhen u sferi pravookhoronnoi diialnosti [Issues of information and analytical research in the field of law enforcement activities]. *Aktualni problemy pravoznavstva – Current problems of jurisprudence*, 3 (27), 103–109. <https://doi.org/10.35774/app2021.03.103> [in Ukrainian].

8. Lysenko, O.V., Lunhol, O.M., & Haborets, O.A. (2023). Law enforcement information and analytical support. *Aktualni pytannia u suchasni nautsi – Current issues in modern science*, Iss. № 3(9), 281–291. [https://doi.org/10.52058/2786-6300-2023-3\(9\)-281-291](https://doi.org/10.52058/2786-6300-2023-3(9)-281-291) [in English].

9. Motsa, V.V. (2022). Teoretyko-metodolohichni zasady vykorystannia kryminalnoho analizu operatyvnymy pidrozdilamy pravookhoronnykh orhaniv Ukpainy [Theoretical and methodological bases for the use of criminal analysis by operative units of law enforcement agencies in Ukraine]. *Naukovyi visnyk Uzhhorodskoho*

Natsionalnoho Universytetu – Uzhhorod National University Herald. Series: Law, 2, 141–147. <https://doi.org/10.24144/2307-3322.2022.73.53> [in Ukrainian].

10. Rizvano, V., Svystun, I., & Kopylov, E. (2025). Kryminalnyi analiz: sutnist ta analitychni osnovy [Criminal analysis: essence and analytical foundations]. *UNIVERSUM*, 27, 352–359. Retrieved from <https://archive.liga.science/index.php/universum/article/view/2565> [in Ukrainian].

11. Ovsianiuk, D. I. (2024). Metodolohichni zasady taktychnoho analizu ta analizu operatyvnykh danykh pid chas rozsliduvannia zlochyniv, poviazanykh z nezakonnym obihom narkotykiv : metod. Rek. [Methodological principles of tactical analysis and analysis of operational data during the investigation of crimes related to illegal drug trafficking: method. rec.]. Kyiv : NAVS, 50 s. Retrieved from <https://elar.navs.edu.ua/server/api/core/bitstreams/9f693faf-930e-4f40-9127-87d4be005233/content> [in Ukrainian].

Creative Commons Attribution 4.0
International (CC BY 4.0)



Дата першого надходження статті до видання: 23.07.2026

Дата прийняття статті до друку після рецензування: 31.08.2026

Дата публікації (оприлюднення) статті: 00.00.2026

УДК 342.9:343.85:364.632.4

DOI <https://doi.org/10.32782/2311-8040/2026-2-3>**Гурковська Катерина Андріївна,**

старша викладачка кафедри адміністративно-правових дисциплін
Навчально-наукового інституту права, психології та безпекознавства,
Львівський державний університет внутрішніх справ,
вулиця Городоцька, 26, Львів, 79000, Україна
ORCID: <https://orcid.org/0000-0001-5026-626X>

АДМІНІСТРАТИВНО-ПРАВОВА ХАРАКТЕРИСТИКА ВЗАЄМОДІЇ СУБ'ЄКТІВ У СФЕРІ ЗАПОБІГАННЯ ТА ПРОТИДІЇ ДОМАШНЬОМУ НАСИЛЬСТВУ

Анотація. У статті здійснено адміністративно-правову характеристику взаємодії суб'єктів у сфері запобігання та протидії домашньому насильству. Проаналізовано та систематизовано наукові підходи до розуміння категорії «взаємодія», що дало змогу виокремити три основні підходи до її трактування: як управлінської категорії, системного процесу та адміністративно-правового механізму.

Обґрунтовано, що взаємодія суб'єктів є ширшим поняттям, ніж міжвідомча взаємодія, оскільки охоплює узгоджену діяльність не лише органів державної влади, а й органів місцевого самоврядування, спеціалізованих служб підтримки постраждалих осіб, закладів охорони здоров'я, освіти, системи безоплатної правничої допомоги, громадських і міжнародних організацій та інших суб'єктів, уповноважених законодавством.

Запропоновано авторське визначення взаємодії суб'єктів у сфері запобігання та протидії домашньому насильству як врегульованого нормами адміністративного права системного процесу узгоджених дій уповноважених суб'єктів, спрямованого на координацію діяльності, інформаційний обмін і реалізацію спільних заходів щодо запобігання, виявлення та припинення домашнього насильства, захисту постраждалих осіб і притягнення кривдників до відповідальності.

Визначено основні ознаки такої взаємодії, до яких віднесено спільність мети, нормативну врегульованість, компетенційну визначеність, узгодженість діяльності, системний характер, сталість інформаційного обміну та комплексний характер.

Підкреслено, що належна організація взаємодії є необхідною передумовою ефективної реалізації державної політики у сфері запобігання та протидії домашньому насильству.

Зроблено висновок, що запропонований підхід поглиблює наукові уявлення про адміністративно-правову природу взаємодії суб'єктів у сфері запобігання та протидії домашньому насильству, сприяє формуванню єдиного теоретичного підходу до розуміння цієї категорії, може бути використаний у подальших наукових дослідженнях, законотворчій діяльності та практиці функціонування суб'єктів, уповноважених реалізовувати державну політику у відповідній сфері.

Ключові слова: взаємодія, суб'єкти запобігання та протидії домашньому насильству, адміністративно-правове регулювання, домашнє насильство, міжвідомча взаємодія, Національна поліція України.

Hurkovska Kateryna. ADMINISTRATIVE AND LEGAL CHARACTERISTICS OF INTERACTION BETWEEN SUBJECTS IN THE FIELD OF PREVENTION AND COUNTERACTION TO DOMESTIC VIOLENCE

Abstract. The article provides an administrative and legal characterisation of interaction between subjects in the field of prevention and counteraction to domestic violence. Scientific approaches to understanding the category of interaction are analysed and systematised, making it possible to distinguish three main approaches to its interpretation: interaction as a managerial category, a systemic process, and an administrative and legal mechanism. It is substantiated that interaction between subjects is a broader concept than interagency interaction, as it encompasses coordinated activities not only of public authorities but also of local self-government bodies, specialised support services for victims, healthcare and educational institutions, the free legal aid system, civil society and international organisations, as well as other entities authorised by law. The author's definition of interaction between subjects in the field of prevention and counteraction to domestic violence is proposed as a systemic process of coordinated actions of authorised entities regulated by the rules of administrative law and aimed at coordinating activities, exchanging information, and implementing joint measures to prevent, detect and stop domestic violence, protect victims, and bring offenders to justice. The essential characteristics of such interaction

are identified, including a common purpose, legal regulation, clearly defined competence, coordinated activities, a systemic nature, continuity of information exchange, and a comprehensive character. It is emphasised that the proper organisation of interaction constitutes a necessary prerequisite for the effective implementation of state policy in the field of prevention and counteraction to domestic violence. It is concluded that the proposed approach deepens the theoretical understanding of the administrative and legal nature of interaction between subjects, contributes to the development of a unified theoretical approach to this category, and may be applied in further academic research, legislative activities, and the practical functioning of entities authorised to implement state policy in the relevant field.

Key words: *interaction, subjects of prevention and counteraction to domestic violence, administrative and legal regulation, domestic violence, interagency interaction, National Police of Ukraine.*

Вступ. Реалізація державної політики у сфері запобігання та протидії домашньому насильству значною мірою залежить від належної взаємодії між суб'єктами, уповноваженими здійснювати відповідні заходи. Незважаючи на законодавче визначення системи таких суб'єктів та їх повноважень, досягнення визначених законом цілей можливе лише за умови узгодженості дій, своєчасного інформаційного обміну, координації управлінських рішень і застосування єдиних алгоритмів реагування. За таких умов взаємодія набуває значення самостійної адміністративно-правової категорії, що потребує комплексного наукового осмислення.

Про актуальність досліджуваної проблематики свідчать також висновки Щорічної доповіді Уповноваженого Верховної Ради України з прав людини за 2025 рік, у якій наголошено на необхідності забезпечення права постраждалих від домашнього насильства на своєчасну та ефективну допомогу й удосконалення державної політики у цій сфері, що безпосередньо пов'язано з належною організацією взаємодії уповноважених суб'єктів [1, с. 383].

Проблематика взаємодії суб'єктів публічної адміністрації тривалий час досліджується представниками адміністративного права, науки державного управління та інших галузей юридичного знання. Попри різноманітність наукових підходів, єдиного розуміння змісту взаємодії у сфері запобігання та протидії домашньому насильству не сформовано, а її адміністративно-правова характеристика залишається недостатньо розробленою.

Особливої актуальності ця проблематика набуває в умовах воєнного стану, коли нові безпекові виклики, масштабне внутрішнє переміщення населення та зростання соціальної

напруги потребують оперативної та скоординованої діяльності всіх уповноважених суб'єктів.

Метою статті є здійснення адміністративно-правової характеристики взаємодії суб'єктів у сфері запобігання та протидії домашньому насильству, визначення її змісту, основних ознак та формулювання авторського визначення поняття взаємодії.

Матеріали та методи. Теоретичну основу дослідження становлять праці вітчизняних учених у галузі адміністративного права, державного управління та правоохоронної діяльності, присвячені проблемам взаємодії суб'єктів публічної адміністрації та адміністративно-правового забезпечення запобігання і протидії домашньому насильству. Під час дослідження використано наукові положення, сформульовані у працях В. Б. Авер'янова, Ю. П. Битяка, О. М. Бандурки, В. В. Галуцька, В. К. Колпакова, Т. О. Коломосьця та Ю. І. Назара та інших науковців.

Нормативну основу дослідження становлять Конституція України [2], Конвенція Ради Європи про запобігання насильству стосовно жінок і домашньому насильству та боротьбу із цими явищами [3], Закон України «Про запобігання та протидію домашньому насильству» [4], Закон України «Про Національну поліцію» [5], Постанова Кабінету Міністрів України від 22 серпня 2018 року № 658 «Про затвердження Порядку взаємодії суб'єктів, що здійснюють заходи у сфері запобігання та протидії домашньому насильству» [6], а також інші законодавчі та підзаконні нормативно-правові акти, що регламентують діяльність суб'єктів у сфері запобігання та протидії домашньому насильству.

Методологічну основу дослідження становить комплекс загальнонаукових і спеціаль-

но-юридичних методів, зокрема діалектичний, формально-юридичний, системно-структурний, порівняльно-правовий та метод узагальнення, використання яких забезпечило аналіз нормативно-правових актів, систематизацію наукових підходів та формулювання авторського визначення взаємодії суб'єктів у сфері запобігання та протидії домашньому насильству.

Результати. Функціонування системи запобігання та протидії домашньому насильству безпосередньо залежить від належної організації взаємодії між суб'єктами, уповноваженими реалізовувати державну політику у цій сфері. Саме завдяки узгодженості їхньої діяльності забезпечуються своєчасне виявлення випадків домашнього насильства, застосування передбачених законодавством заходів реагування, надання комплексної допомоги постраждалим особам та притягнення кримінальників до відповідальності. Водночас аналіз чинного законодавства свідчить, що, незважаючи на широке використання категорії «взаємодія», її легальне визначення відсутнє. Це зумовлює необхідність звернення до наукової доктрини з метою з'ясування змісту зазначеної категорії та формування цілісного адміністративно-правового розуміння цього поняття.

Наукові погляди різняться залежно від предмета дослідження, однак їх систематизація дозволяє виокремити три основні напрями наукового осмислення: розуміння взаємодії як управлінської категорії, як системного процесу та як адміністративно-правового механізму. Такий поділ є умовним, однак він дає можливість простежити еволюцію наукових поглядів і визначити найбільш суттєві характеристики досліджуваного явища.

1. Взаємодія як управлінська категорія. Перший напрям сформувався в межах науки державного управління та адміністративного права, представники якого розглядають взаємодію передусім як різновид управлінської діяльності, спрямованої на забезпечення узгодженого функціонування органів, наділених різною компетенцією. У центрі уваги перебувають питання координації діяльності, раціонального розподілу повноважень, узгодження

управлінських рішень та організації спільного виконання поставлених завдань.

Так, В. К. Колпаков визначає взаємодію як вид управлінської діяльності, що полягає в узгодженні зусиль різних органів для досягнення спільної мети, за якого кожний суб'єкт діє в межах власної компетенції, використовуючи спільні форми та методи роботи [7, с. 10]. На думку науковця, саме координація діяльності забезпечує уникнення дублювання функцій та підвищує ефективність управлінських процесів.

Аналогічної позиції дотримується О. М. Бандурка, який розглядає взаємодію як діяльність, засновану на вимогах законодавства, чіткому розмежуванні повноважень, взаємній відповідальності суб'єктів та постійному інформаційному обміні між ними [8, с. 13]. Науковець підкреслює, що ефективність взаємодії безпосередньо залежить від належного нормативного регулювання та визначення обов'язків кожного учасника управлінських відносин.

Отже, представники зазначеного напрямку розглядають взаємодію насамперед як управлінську категорію, основними ознаками якої є спільність мети, узгодженість діяльності, координація управлінських рішень, розмежування компетенції та інформаційний обмін між суб'єктами.

2. Взаємодія як системний процес. Подальший розвиток адміністративно-правової науки сприяв формуванню ширшого підходу до розуміння взаємодії, відповідно до якого вона розглядається не лише як спосіб координації діяльності суб'єктів, а як системний процес їх взаємозв'язку та взаємовпливу. На відміну від управлінського напрямку, основна увага приділяється не окремим організаційним заходам, а стійким функціональним зв'язкам між учасниками публічного управління, які забезпечують узгоджене функціонування єдиної системи.

Так, В. А. Завгородній характеризує взаємодію через категорії взаємозв'язку та взаємовпливу суб'єктів, наголошуючи, що саме ці елементи забезпечують ефективне функціонування системи публічного управління [9, с. 9]. Такий підхід дозволяє розглядати взаємодію

як безперервний процес, що змінюється під впливом зовнішніх чинників і потребує постійної адаптації організаційних механізмів. У сфері запобігання та протидії домашньому насильству це має особливе значення, оскільки ефективність діяльності окремого суб'єкта безпосередньо залежить від своєчасності та якості виконання повноважень іншими учасниками системи.

Подібний підхід простежується у працях Ю. С. Назара, який розглядає взаємодію як фундаментальну категорію, що відображає загальний взаємозв'язок явищ та процесів [10, с. 8]. У площині адміністративно-правового регулювання це означає, що кожен суб'єкт реалізує власну компетенцію не ізольовано, а як складова цілісної системи, де результати діяльності одного учасника створюють юридичні й організаційні передумови для здійснення повноважень іншими суб'єктами. Саме така послідовність взаємопов'язаних дій забезпечує ефективне функціонування адміністративно-правового механізму запобігання та протидії домашньому насильству.

Водночас і ця концепція не повною мірою враховує особливості адміністративно-правового регулювання, оскільки основний акцент робиться на системних зв'язках між суб'єктами, тоді як нормативна природа взаємодії залишається другорядною.

Наведені напрями сформували загальнотеретичне розуміння взаємодії. Водночас розвиток спеціальних адміністративно-правових досліджень у сфері запобігання та протидії домашньому насильству зумовив формування ще одного напрямку, відповідно до якого взаємодія розглядається як самостійний адміністративно-правовий механізм реалізації державної політики.

3. Взаємодія як адміністративно-правовий механізм. На відміну від попередніх концепцій, у центрі уваги перебувають не лише організаційні чи системні зв'язки між суб'єктами, а й нормативно визначений порядок їхньої спільної діяльності, особливості реалізації компетенції, координації, інформаційного обміну та досягнення спільного результату. Саме такий підхід найбільшою мірою відповідає

сучасним тенденціям розвитку адміністративного права, у якому взаємодія розглядається як необхідна умова ефективного функціонування механізму публічного управління.

Так, Т. Лях, Т. Спіріна та В. Рогожинська визначають міжвідомчу взаємодію як партнерство органів державної влади, органів місцевого самоврядування та інших установ, спрямоване на спільне досягнення цілей у соціальній сфері [11, с. 225]. Запропонований підхід акцентує увагу на партнерському характері відносин між учасниками взаємодії, що передбачає поєднання їхніх ресурсів, компетенцій і можливостей для вирішення суспільно значущих проблем.

Подальший розвиток зазначеної концепції знайшов відображення у працях О. Ю. Салманової та І. Д. Казанчук, які досліджували міжвідомчу взаємодію безпосередньо у сфері запобігання та протидії домашньому насильству. Автори пропонують розглядати її у широкому та вузькому значеннях. У широкому розумінні взаємодія охоплює процес узгодження форм, методів і способів реалізації державної політики всіма уповноваженими суб'єктами. У вузькому – характеризується як соціально-правове партнерство органів виконавчої влади, Національної поліції України, органів місцевого самоврядування та інших учасників, які в межах визначеної компетенції здійснюють узгоджені організаційні заходи, забезпечують постійний інформаційний обмін і координують спільні дії щодо запобігання та протидії домашньому насильству [12, с. 318].

Запропоновані підходи мають важливе методологічне значення для дослідження, однак, на нашу думку, категорії «міжвідомча взаємодія» та «взаємодія суб'єктів» не є тотожними. Міжвідомча взаємодія охоплює передусім узгоджену діяльність органів, що належать до різних відомчих систем. Натомість взаємодія суб'єктів у сфері запобігання та протидії домашньому насильству є значно ширшим явищем, оскільки охоплює не лише органи державної влади, а й органи місцевого самоврядування, спеціалізовані служби підтримки постраждалих осіб, заклади охорони здоров'я, освіти, систему безоплатної правничої до-

помоги, громадські об'єднання, міжнародні організації та інших учасників, визначених законодавством. Саме тому для цілей цього дослідження більш коректним є використання категорії «взаємодія суб'єктів», яка повніше відображає структуру та зміст відповідних адміністративно-правових відносин.

Проведений аналіз свідчить, що сучасні умови функціонування системи запобігання та протидії домашньому насильству обумовлюють необхідність ширшого розуміння взаємодії як комплексного адміністративно-правового явища. Це підтверджується і сучасними емпіричними дослідженнями. Зокрема, результати опитування постраждалих осіб та експертів засвідчують, що в умовах воєнного стану результативність реагування значною мірою залежить від належної координації діяльності поліції, соціальних служб, судів, прокуратури та інших уповноважених суб'єктів, а основними перешкодами залишаються кадровий дефіцит, недостатня доступність окремих служб і несвоєчасне реагування [13, с. 9–11].

Важливість належної взаємодії підкріплюється й результатами Національного моніторингу спеціалізованих служб підтримки, серед ключових завдань якого визначено посилення міжвідомчої координації між соціальною, медичною, освітньою та правоохоронною системами як необхідної умови розвитку державної політики у сфері запобігання та протидії домашньому насильству [14, с. 9].

З огляду на це взаємодію суб'єктів у сфері запобігання та протидії домашньому насильству пропонуємо визначати як врегульований нормами адміністративного права системний процес узгоджених дій уповноважених суб'єктів, які, діючи в межах визначеної законодавством компетенції, здійснюють координацію діяльності, інформаційний обмін та реалізацію спільних заходів, спрямованих на запобігання, виявлення і припинення домашнього насильства, захист постраждалих осіб та притягнення кривдників до відповідальності.

Запропоноване визначення відображає загальну сутність взаємодії, однак її зміст найбільш повно розкривається через систему характерних ознак. На підставі проведеного

дослідження пропонуємо виокремити такі основні ознаки взаємодії: 1) спільна мета, яка об'єднує діяльність усіх суб'єктів незалежно від їх організаційної підпорядкованості та обсягу компетенції. Науковці пов'язують мету взаємодії з об'єднанням зусиль усіх суб'єктів для забезпечення постраждалій особі можливості самостійно визначати подальше життя без насильства [15, с. 265]. Як слушно зазначає О. М. Шевчук, обов'язковою ознакою взаємодії є наявність у суб'єктів спільної мети, адже лише за такої умови може відбуватися перетинання їх діяльності. При цьому спільність мети не означає однаковості функцій і завдань, а, навпаки, передбачає їх диференціацію [16, с. 126]. Поділяючи зазначену позицію, вважаємо, що у сфері запобігання та протидії домашньому насильству такою спільною метою є забезпечення своєчасного виявлення випадків домашнього насильства, ефективного захисту постраждалих осіб, припинення протиправної поведінки кривдників і недопущення повторного вчинення насильства. Саме єдина мета забезпечує узгодженість діяльності всіх суб'єктів та визначає зміст їх взаємодії; 2) нормативна врегульованість, яка полягає в тому, що порядок взаємодії, повноваження її учасників, форми співпраці та механізми координації визначаються нормами законодавства. Як зазначає Т. М. Ященко, взаємовідносини органів публічної влади будуються на нормативно-правовій основі [17, с. 20]. Нормативне закріплення забезпечує правову визначеність діяльності суб'єктів, виключає дублювання функцій та створює належні гарантії реалізації державної політики у сфері запобігання та протидії домашньому насильству; 3) компетенційна визначеність означає, що кожний суб'єкт взаємодії реалізує лише ті повноваження, які прямо визначені законодавством. Чітке розмежування компетенції та взаємодоповнюваність функцій забезпечують законність і ефективність взаємодії. О. І. Лавренова відзначає, що компетенція є складною правовою категорією, зміст якої становлять предмети відання, а також права й обов'язки суб'єкта владних повноважень [18, с. 11]; 4) узгодженість діяльності характеризує вза-

ємодію як процес, у межах якого рішення та дії окремих суб'єктів є взаємопов'язаними, послідовними та спрямованими на досягнення спільного результату. Належна взаємодія потребує визначення її учасників, їхніх завдань, обсягу й форм спільної діяльності, розподілу функціональних обов'язків, конкретних виконавців, способів інформаційного обміну та контролю за виконанням погоджених заходів [15, с. 265]; 5) системний характер, оскільки взаємодія здійснюється не епізодично, а як складова єдиного адміністративно-правового механізму реалізації державної політики. Кожний суб'єкт є елементом цілісної системи, а результати його діяльності безпосередньо впливають на ефективність роботи інших учасників взаємодії. Саме системність забезпечує безперервність і комплексність реагування на випадки домашнього насильства; 6) сталість інформаційного обміну, що забезпечує своєчасне отримання, передачу та використання інформації, необхідної для прийняття управлінських рішень. Постійний обмін інформацією між суб'єктами дозволяє оперативно реагувати на випадки домашнього насильства, здійснювати оцінку ризиків та координувати подальші заходи захисту постраждалих осіб. Водночас інформаційний обмін має забезпечуватися не лише між суб'єктами взаємодії, а й бути спрямованим на належне інформування населення, оскільки недостатня обізнаність постраждалих щодо діяльності, місцезнаходження та можливостей суб'єктів, які надають допомогу, істотно ускладнює доступ до відповідних послуг і реалізацію їхніх прав [12, с. 9]; 7) комплексний характер взаємодії, що полягає у поєднанні правових, організаційних, інформаційних, соціальних та інших заходів, що реалізуються різними суб'єктами відповідно до їх компетенції. Законодавчим підтвердженням є положення ст. 15 Закону України «Про запобігання та протидію домашньому насильству», відповідно до

яких взаємодія охоплює не лише реагування на випадки домашнього насильства, а й розроблення та виконання програм для кривдників і програм запобігання та протидії домашньому насильству, обмін досвідом, міжвідомчу підготовку фахівців, здійснення моніторингу та інші взаємопов'язані заходи [4].

Висновки. Проведене дослідження дало змогу встановити, що в адміністративно-правовій науці відсутній єдиний підхід до розуміння взаємодії суб'єктів у сфері запобігання та протидії домашньому насильству. Систематизація наукових поглядів дозволила виокремити три основні концептуальні напрями до її розуміння: як управлінської категорії, як системного процесу та як адміністративно-правового механізму, кожен із яких розкриває окремі аспекти досліджуваного явища.

Обґрунтовано доцільність розгляду взаємодії суб'єктів у досліджуваній сфері як врегульованого нормами адміністративного права системного процесу узгоджених дій уповноважених суб'єктів, спрямованого на координацію діяльності, інформаційний обмін та реалізацію спільних заходів щодо запобігання, виявлення і припинення домашнього насильства, захисту постраждалих осіб і притягнення кривдників до відповідальності.

Встановлено, що зміст взаємодії найбільш повно розкривається через сукупність її основних ознак, до яких віднесено спільність мети, нормативну врегульованість, компетенційну визначеність, узгодженість діяльності, системний характер, сталість інформаційного обміну та комплексний характер. Запропонований підхід розширює наукові уявлення про адміністративно-правову природу взаємодії суб'єктів у сфері запобігання та протидії домашньому насильству та може бути використаний під час подальшого вдосконалення адміністративно-правового регулювання й практичної діяльності уповноважених суб'єктів в умовах воєнного стану та післявоєнного відновлення.

Список використаних джерел:

1. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні у 2025 році. URL: <https://www.ombudsman.gov.ua/storage/app/media/uploaded-files/2-22042026-0951-shchorichna-dopovid-upovnovazhenogo-2025.pdf>

2. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>
3. Конвенція Ради Європи про запобігання насильству стосовно жінок і домашньому насильству та боротьбу із цими явищами (Стамбульська конвенція) : міжнар. док. від 11.05.2011. URL: https://zakon.rada.gov.ua/laws/show/994_001-11#Text
4. Про запобігання та протидію домашньому насильству : Закон України від 07.12.2017 № 2229-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2229-19#Text>
5. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII. URL: <https://zakon.rada.gov.ua/laws/show/580-19#Text>
6. Про затвердження Порядку взаємодії суб'єктів, що здійснюють заходи у сфері запобігання та протидії домашньому насильству: постанова Кабінету Міністрів України від 22.08.2018 № 658. URL: <https://zakon.rada.gov.ua/laws/show/658-2018-%D0%BF#Text>
7. Колпаков В.К. Адміністративне право України : підручник. Київ : Юрінком Інтер, 1999. 736 с.
8. Бандурка О.М. Основи управління в органах внутрішніх справ України : теорія, досвід, шляхи удосконалення. Харків : «Основа», 1996. 398 с.
9. Завгородній В.А. Правове регулювання взаємодії органів Національної поліції та громадських організацій у протидії корупції : навч. посіб. Дніпро : Дніпроп. держ. ун-т внутр. справ; Ліра ЛТД, 2016. 168 с.
10. Назар Ю. С. Взаємодія органів внутрішніх справ із місцевими органами виконавчої влади та органами місцевого самоврядування у профілактиці адміністративних правопорушень: монографія. Львів: Львівський державний університет внутрішніх справ, 2012. 160 с.
11. Лях Т., Спіріна Т., Рогожинська В. Принципи міждисциплінарної взаємодії у соціальній роботі. *Актуальні питання гуманітарних наук*. 2020. Вип. 27. Т. 3. С. 224–228. DOI <https://doi.org/10.24919/2308-4863.3/27.203727>
12. Салманова О. Ю., Казанчук І. Д. Адміністративно-правові засади міжвідомчої взаємодії Національної поліції України з іншими суб'єктами протидії домашньому насильству в умовах сьогодення. *Вісник Кримінологічної асоціації України*. 2025. № 2 (35). Ч. 2. С. 314–329. DOI: <https://doi.org/10.32631/vsa.2025.2.57>
13. Бороздіна К. А., Легенька М. М., Пильо Д. І., Дмитрук Ю. Р., Черехаха К. В. Результати дослідження якості реагування під час воєнного стану відповідних суб'єктів (поліція, суди, прокуратура, соціальні служби тощо), які надають послуги постраждалим від гендерно зумовленого насильства, зокрема домашнього. Київ : ГО «Ла Страда-Україна», 2022. 12 с. URL: <https://la-strada.org.ua/wp-content/uploads/2022/09/la-strada-poll-2.pdf>
14. Національна соціальна сервісна служба України. Національний звіт за підсумками моніторингу спеціалізованих служб підтримки осіб, які постраждали від домашнього насильства та/або насильства за ознакою статі. Київ, 2025. 139 с. URL: <https://nssu.gov.ua/storage/app/sites/22/uploaded-files/national-monitoring-report.pdf>
15. Запобігання та протидія домашньому насильству: підручник / О.В. Ковальова, А.І. Берендєєва. Одеса: ОДУВС. 2022. 368 с.
16. Шевчук О. М. Взаємодія та координація органів державної влади щодо забезпечення державного контролю у сфері обігу наркотичних засобів та психотропних речовин. *Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція*. 2014. № 8. С. 126–129. URL: http://nbuv.gov.ua/UJRN/Nvmgu_jur_2014_8_35
17. Яценко Т. М. Співвідношення понять «взаємодія» та «взаємовідносини» в системі державного управління. *Вісник Національної академії державного управління при Президенті України. Серія : Державне управління*. 2017. № 2. С. 19–25. URL: http://nbuv.gov.ua/UJRN/vnaddy_2017_2_5
18. Лавренова О. І. Адміністративно-правовий статус державної служби як центрального органу виконавчої влади : автореф. дис. ... канд. юрид. наук : 12.00.07. Одеса, 2014. 20 с. URL: <https://dspace.onua.edu.ua/server/api/core/bitstreams/8f0391b4-9ba5-43db-b6e9-b734d623884f/content>

References:

1. Shchorichna dopovid Upovnovazhenoho Verkhovnoi Rady Ukrainy z prav liudyny pro stan doderzhannia ta zakhystu prav i svobod liudyny i hromadianyna v Ukraini u 2025 rotsi (2025). [Annual Report of the Ukrainian Parliament Commissioner for Human Rights on the observance and protection of human and civil rights and freedoms in Ukraine in 2025]. <https://www.ombudsman.gov.ua/storage/app/media/uploaded-files/2-22042026-0951-shchorichna-dopovid-upovnovazhenogo-2025.pdf> [in Ukrainian].

2. Konstytutsiia Ukrainy : Zakon Ukrainy vid 28 chervnia 1996 roku № 254k/96-VR (1996). [Constitution of Ukraine: Law of Ukraine dated 28 June 1996 No. 254k/96-VR]. <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text> [in Ukrainian].
3. Convention on Preventing and Combating Violence against Women and Domestic Violence (Istanbul Convention) vid 11 May 2011 (2011). https://zakon.rada.gov.ua/laws/show/994_001-11#Text [in English].
4. Pro zapobihannia ta protyidii domashnomu nasylstvu : Zakon Ukrainy vid 07 hrudnia 2017 roku № 2229-VIII (2017). [On Prevention and Counteraction to Domestic Violence: Law of Ukraine dated 07 December 2017 No. 2229-VIII]. <https://zakon.rada.gov.ua/laws/show/2229-19#Text> [in Ukrainian].
5. Pro Natsionalnu polit siiu : Zakon Ukrainy vid 02 lypnia 2015 roku № 580-VIII (2015). [On the National Police: Law of Ukraine dated 02 July 2015 No. 580-VIII]. <https://zakon.rada.gov.ua/laws/show/580-19#Text> [in Ukrainian].
6. Pro zatverdzhennia Poriadku vzaiemodii subiektiv, shcho zdiisniuiut zakhody u sferi zapobihannia ta protydii domashnomu nasylstvu : Postanova Kabinetu Ministriv Ukrainy vid 22 serpnia 2018 roku № 658 (2018). [On Approval of the Procedure for Interaction between Entities Implementing Measures in the Field of Prevention and Counteraction to Domestic Violence: Resolution of the Cabinet of Ministers of Ukraine dated 22 August 2018 No. 658]. <https://zakon.rada.gov.ua/laws/show/658-2018-%D0%BF#Text> [in Ukrainian].
7. Kolpakov, V. K. (1999). Administrativne pravo Ukrainy [Administrative Law of Ukraine]. Yurinkom Inter [in Ukrainian].
8. Bandurka, O. M. (1996). Osnovy upravlinnia v orhanakh vnutrishnikh sprav Ukrainy: teoriia, dosvid, shliakhy udoskonalennia [Fundamentals of management in the bodies of internal affairs of Ukraine: Theory, experience, and ways of improvement]. Osnova [in Ukrainian].
9. Zavhorodnii, V. A. (2016). Pravove rehuliuвання vzaiemodii orhaniv Natsionalnoi polit sii ta hromadskykh orhanizatsii u protydii koruptsii [Legal regulation of interaction between the National Police and public organisations in combating corruption]. Lira LTD [in Ukrainian].
10. Nazar, Yu. S. (2012). Vzaiemodiia orhaniv vnutrishnikh sprav iz mistsevymy orhanamy vykonavchoi vlady ta orhanamy mistsevoho samovriaduvannia u profilaktytsi administrativnykh pravoporushen [Interaction of internal affairs bodies with local executive authorities and local self-government bodies in the prevention of administrative offences]. Lviv State University of Internal Affairs [in Ukrainian].
11. Liakh, T., Spirina, T., & Rohozhynska, V. (2020). Pryntsyipy mizhdystsyplinarnoi vzaiemodii u sotsialnii roboti [Principles of interdisciplinary interaction in social work]. *Aktualni pytannia humanitarnykh nauk*, 27(3), 224–228. <https://doi.org/10.24919/2308-4863.3/27.203727> [in Ukrainian].
12. Salmanova, O. Yu., & Kazanchuk, I. D. (2025). Administrativno-pravovi zasady mizhvidomchoi vzaiemodii Natsionalnoi polit sii Ukrainy z inshymy subiektamy protydii domashnomu nasylstvu v umovakh sohodennia [Administrative and legal principles of interagency interaction of the National Police of Ukraine with other entities combating domestic violence under current conditions]. *Visnyk Kryminolohichnoi asotsiatsii Ukrainy*, 2(35), Part 2, 314–329. <https://doi.org/10.32631/vca.2025.2.57> [in Ukrainian].
13. Borozdina, K. A., Lehenka, M. M., Pylo, D. I., Dmytruk, Yu. R., & Cherepakha, K. V. (2022). Rezultaty doslidzhennia yakosti reahuvannia pid chas voiennoho stanu vidpovidnykh subiektiv (politsiia, sudy, prokuratura, sotsialni sluzhby toshcho), yaki nadaiut posluhy postrazhdalym vid genderno zumovlenoho nasylstva, zokrema domashnoho [Results of the study on the quality of response during martial law by relevant entities (police, courts, prosecution, social services, etc.) providing services to victims of gender-based violence, including domestic violence]. *La Strada—Ukraine*. <https://la-strada.org.ua/wp-content/uploads/2022/09/la-strada-poll-2.pdf> [in Ukrainian].
14. Natsionalna sotsialna servisna sluzhba Ukrainy. (2025). Natsionalnyi zvit za pidsumkamy monitorynhu spetsializovanykh sluzhb pidtrymky osib, yaki postrazhdaly vid domashnoho nasylstva ta/abo nasylstva za oznakoiu stati [National report on monitoring specialised support services for persons affected by domestic violence and/or gender-based violence]. <https://nssu.gov.ua/storage/app/sites/22/uploaded-files/national-monitoring-report.pdf> [in Ukrainian].
15. Kovalova, O. V., & Berendieieva, A. I. (2022). Zapobihannia ta protydii domashnomu nasylstvu [Prevention and Counteraction to Domestic Violence]. Odesa State University of Internal Affairs [in Ukrainian].
16. Shevchuk, O. M. (2014). Vzaiemodiia ta koordynatsiia orhaniv derzhavnoi vlady shchodo zabezpechennia derzhavnoho kontroliu u sferi obihu narkotychnykh zasobiv ta psykhotropnykh rehovyn [Interaction and coordination of public authorities in ensuring state control over the circulation of narcotic drugs and psychotropic substances]. *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu. Seriia: Yurytsprudentsiia*, 8, 126–129. http://nbuv.gov.ua/UJRN/Nvmgu_jur_2014_8_35 [in Ukrainian].

17. Yashchenko, T. M. (2017). Spivvidnoshennia poniat «vzaiemodiiia» ta «vzaiemovidnosyny» v systemi derzhavnoho upravlinnia [Correlation between the concepts «interaction» and «interrelations» in the system of public administration]. *Visnyk Natsionalnoi akademii derzhavnoho upravlinnia pry Prezidentovi Ukrainy. Serii: Derzhavne upravlinnia*, 2, 19–25. http://nbuv.gov.ua/UJRN/vnaddy_2017_2_5 [in Ukrainian].

18. Lavrenova, O. I. (2014). Administratyvno-pravovyi status derzhavnoi sluzhby yak tsentralnoho orhanu vykonavchoi vlady [Administrative and legal status of the civil service as a central executive authority]. Extended abstract of Candidate's thesis. Odesa. <https://dspace.onua.edu.ua/server/api/core/bitstreams/8f0391b4-9ba5-43db-b6e9-b734d623884f/content> [in Ukrainian].

Creative Commons Attribution 4.0
International (CC BY 4.0)



Дата першого надходження статті до видання: 22.07.2026
Дата прийняття статті до друку після рецензування: 21.08.2026
Дата публікації (оприлюднення) статті: 00.00.2026

УДК 343

DOI <https://doi.org/10.32782/2311-8040/2026-2-4>

Кравченко Іван Олександрович,

доктор юридичних наук, професор,
професор кафедри адміністративного та інформаційного права
Сумський національний аграрний університет,
вулиця Герасима Кондратьєва, 160, Суми, 40021, Україна
ORCID: <https://orcid.org/0000-0002-6555-2733>

ТРАНСФОРМАЦІЯ НАЦІОНАЛЬНИХ ПІДХОДІВ ДО КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ЗА НЕЦІЛЬОВЕ ВИКОРИСТАННЯ ГУМАНІТАРНОЇ ДОПОМОГИ: ІМПЛЕМЕНТАЦІЯ СТАНДАРТІВ ЄВРОПЕЙСЬКОГО СОЮЗУ

Анотація. У статті проведений глибокий та критичний кримінально-правовий аналіз інституційних механізмів відповідальності за нецільове використання транснаціональної гуманітарної допомоги в екстремальних умовах воєнного стану крізь призму безапеляційних стандартів Європейського Союзу. Констатовано, що чинна юридична конструкція статті 201-2 Кримінального кодексу України страждає на критичну догматичну обмеженість, оскільки базується на застарілій, вузько-матеріалістичній парадигмі, яка інквізиційно вимагає обов'язкового доведення специфічної мети отримання прибутку та факту фізичної реалізації майна. Доведено, що такий реактивний антропоцентричний підхід прямо суперечить прогресивним європейським принципам захисту фінансових інтересів інституцій-донорів, імперативно закріпленим у Директиві PIF. Обґрунтовано нагальну необхідність концептуальної трансформації об'єкта кримінально-правової охорони, зокрема від захисту абстрактного порядку господарювання до мультиплікативного збереження цільового призначення грантових фондів та глобальної довіри. Аргументовано, що вітчизняна практика тотальної цифровізації та абсолютної публічності реєстрів гуманітарної допомоги є категоричною методологічною помилкою, яка грубо ігнорує європейські стандарти недоторканності персональних даних (GDPR) та фундаментальний принцип «Do No Harm», створюючи екзистенційні безпекові ризики для волонтерів. На основі розгорнутого компаративного аналізу кримінальних доктрин Німеччини та Польщі запропоновано імплементувати інноваційний європейський інститут «субвенційного шахрайства». Ця синергетична євроінтеграційна модель безальтернативно передбачає запровадження виключно формального складу злочину, де справедливій кримінальній репресії підлягає сам умисний факт внесення недостовірних відомостей до електронних реєстрів чи свідомо підробка інвентаризаційних звітів на ранній стадії митного оформлення. Запропонований підхід дозволить стратегічно змістити державний акцент з неефективної боротьби з наслідками на раннє превентивне викорінення транснаціональних фінансових зловживань, забезпечивши остаточну гармонізацію вітчизняного законодавства з *acquis communautaire* ЄС.

Ключові слова: гуманітарна допомога, благодійні пожертви, GDPR, субвенційне шахрайство, євроінтеграція, воєнний стан.

Kravchenko Ivan. TRANSFORMATION OF NATIONAL APPROACHES TO CRIMINAL LIABILITY FOR THE MISUSE OF HUMANITARIAN AID: IMPLEMENTATION OF EUROPEAN UNION STANDARDS

Abstract. The presented article provides an in-depth, multidimensional, and critical criminal-legal analysis of the institutional mechanisms of responsibility for the misuse of transnational humanitarian aid under the extreme conditions of martial law through the prism of the mandatory standards of the European Union. It is indisputably established that the current legal construction of Article 201-2 of the Criminal Code of Ukraine suffers from critical dogmatic limitations, as it is based on an outdated, narrowly materialistic paradigm that inquisitorially requires the mandatory proof of a specific purpose of obtaining profit and the fact of the physical sale of property. It is fundamentally proven that such a reactive anthropocentric approach directly contradicts the progressive European principles of protecting the financial interests of donor institutions, imperatively enshrined in the PIF Directive. The urgent need for a conceptual transformation of the object of criminal-legal protection is substantiated: from protecting an abstract economic order to the multiplicative preservation of the targeted use of grant funds and global trust. It is acutely argued that the domestic practice of total digitalization and absolute publicity of humanitarian aid registries is a categorical methodological error that flagrantly ignores the European standards of personal data

*inviolability (GDPR) and the fundamental “Do No Harm” principle, thereby creating existential security risks for volunteers. Based on an extensive comparative analysis of the criminal doctrines of Germany and Poland, it is proposed to implement the innovative European institution of “subsidy fraud.” This synergistic Euro-integration model unalterably implies the introduction of an exclusively formal composition of the crime, where the intentional fact of entering false information into electronic registers or the deliberate forgery of inventory reports at the early stage of customs clearance is subject to fair criminal repression. The proposed approach will strategically shift the state emphasis from the ineffective fight against consequences to the early preventive eradication of transnational financial abuses, ensuring the ultimate harmonization of domestic legislation with the EU *acquis communautaire*.*

Key words: humanitarian aid, charitable donations, GDPR, subvention fraud, European integration, martial law.

Вступ. Введення в Україні правового режиму воєнного стану у зв'язку з безпрецедентною збройною агресією каталізувало коло-сальний приплив міжнародної гуманітарної допомоги, що, у свою чергу, блискавично оголило кричущу проблему відсутності адекватних та сучасних кримінально-правових механізмів захисту цих ресурсів від злочинних посягань. Законодавець, керуючись екстремним прагненням забезпечити швидке реагування на нові виклики та суспільний резонанс, доповнив Кримінальний кодекс України статтею 201-2, яка встановила відповідальність за незаконне використання гуманітарної допомоги, благодійних пожертв або безоплатної допомоги з метою отримання прибутку. Водночас, ми вважаємо, що ця законодавча стала класичним прикладом інституційної ізоляції, яка не лише штучно дублює існуючі норми про злочини проти власності, але й залишає поза увагою фундаментальні європейські підходи до захисту фінансових інтересів донорів. Набуття Україною статусу кандидата на вступ до Європейського Союзу формує безапеляційні вимоги щодо глибинної гармонізації національного кримінального законодавства з *acquis communautaire*. На наше переконання, проблема нецільового використання гуманітарної допомоги має концептуально розглядатися не як тривіальний локальний майновий злочин, а як комплексна транснаціональна загроза фінансовим інтересам, інституційній довірі міжнародних партнерів та глобальній архітектурі транспарентності. Варто відзначити, що процес європеїзації українського кримінального права не може зводитися до механічної екстраполяції фрагментарних європейських директив, як результат, він вимагає концептуального переосмислення самого об'єкта за-

хисту, де надскладний баланс між публічним контролем за рухом допомоги та строгим дотриманням європейських стандартів захисту персональних даних перетворюється на ключовий лімітуючий фактор ефективності всього правозастосування.

У вітчизняній кримінально-правовій доктрині питання кваліфікації та відповідальності за ст. 201-2 КК України стали предметом гострих наукових дискусій одразу після її імплементації, що засвідчує кричущу нестабільність цієї норми. Фундаментальні дослідження таких провідних вітчизняних науковців, як О. О. Дудоров, Р. О. Мовчан та Д. В. Каменський, переконливо довели штучність та надмірну казуїстичність цієї норми, аргументуючи, що вона є сумнівною законодавчою новелою, яка підміняє традиційні склади майнових злочинів та створює невинуватому конкуренцію кримінально-правових норм [1]. Цю наукову полеміку підтримали й інші авторитетні дослідники, зокрема О. В. Кришевич, О. В. Швидка, А. В. Шевчук, О. М. Бондарук, Г. В. Муляр, В. А. Бабич, М. П. Куцевич, О. С. Кеєр, А. В. Айдинян, які сфокусували увагу на аналізі об'єктивної та суб'єктивної сторони діяння, обґрунтовуючи невідповідність ознаки «мета отримання прибутку» реальним загрозам нецільового використання та виокремлюючи критерії відмежування цього складу від класичного шахрайства. Водночас, аналізуючи ці класичні вітчизняні розвідки, ми вважаємо за необхідне відзначити їхню надмірну зосередженість виключно на внутрішньодогматичних проблемах КК України, тоді як стан опрацювання саме європейського виміру цієї проблеми у вітчизняній науці залишається фрагментарним. Так, наприклад, західні концепції

кримінально-правового захисту фінансових інтересів Європейського Союзу, ретельно розроблені такими дослідниками як В. Ван Баллегуй та Л. Золі, а також фундаментальні принципи безпечної обробки чутливих даних у гуманітарній сфері, зафіксовані в настановах Inter-Agency Standing Committee, практично ніколи не екстраполювалися на український правовий ландшафт [2]. Це створює концептуальний вакуум – національна юридична наука досі намагається оптимізувати пострадянський механізм кримінально-правової охорони власності, тоді як природа об'єкта дослідження безапеляційно вимагає виходу на новий, транснаціональний інституційний рівень європейського праворозуміння.

Мета дослідження полягає у комплексному, критичному переосмисленні вітчизняних кримінально-правових механізмів відповідальності за нецільове використання гуманітарної допомоги крізь призму європейських інституційних стандартів (зокрема Директиви PIF та вимог GDPR) задля формування синергетичної компаративної моделі їх імплементації, що здатна забезпечити фундаментальний захист фінансових інтересів міжнародної спільноти.

Матеріали та методи. Методологічну основу дослідження становить комплекс загальнонаукових та спеціальних методів пізнання правових явищ. Базовим є метод системно-структурного та критичного аналізу, застосований для оцінки діючої юридичної конструкції статті 201-2 Кримінального кодексу України та її співвідношення з європейськими нормами. За допомогою порівняльно-правового (компаративного) методу здійснено ґрунтовне зіставлення вітчизняного кримінального законодавства з передовими кримінальними доктринами країн-членів ЄС (Німеччини та Польщі) у сфері захисту фінансових інтересів та протидії субвенційному шахрайству. Емпіричною та матеріальною базою дослідження слугували норми національного законодавства, стандарти Європейського Союзу (Директива PIF, Загальний регламент про захист даних – GDPR), настанови міжнародних інституцій, а також праці провідних вітчизняних та зарубіжних науковців.

Результати. Історично склалося так, що у загальній національній доктрині кримінального права нецільове використання міжнародної допомоги класично розглядається виключно в межах консервативної парадигми захисту майнових прав або порядку здійснення господарської діяльності. Український законодавець, конструюючи диспозицію ст. 201-2 КК України, визначив об'єктивну сторону цього кримінального правопорушення як «продажем товарів (предметів) гуманітарної допомоги або використанням благодійних пожертв, безоплатної допомоги або укладанням інших правочинів щодо розпорядження таким майном», акцентуючи увагу суто на безпосередньому фізичному відчуженні або привласненні матеріальних цінностей [3]. Цей вітчизняний підхід є глибоко «антропоцентричним» та відверто матеріалістичним: склад злочину констатується лише у тому разі, коли слідством беззаперечно встановлено прямий корисливий мотив суб'єкта – специфічну мету «отримання прибутку», та зафіксовано реальне завдання матеріальної шкоди у значному розмірі. Відповідно, традиційна наука зосереджує свої зусилля на пошуках критеріїв відмежування цього вузького діяння від класичного шахрайства [4].

На наше переконання, жорстка прив'язка кримінальної відповідальності до обов'язкового доведення «мети отримання прибутку» є категоричною методологічною помилкою, яка повністю ігнорує сучасні європейські реалії боротьби з фінансовими зловживаннями. У контексті права Європейського Союзу концептуальний фокус давно зміщений із захисту конкретної «речі» чи міфічного «господарського порядку» на мультиплікативний захист фінансових інтересів та інституційної довіри громадян і донорів. Згідно з безапеляційними вимогами Директиви ЄС 2017/1371 про боротьбу з шахрайством, що зачіпає фінансові інтереси Союзу (PIF Directive), європейський законодавець криміналізує будь-яке умисне використання або надання неправдивої, неточної чи неповної інформації, що безпосередньо призводить до незаконного утримання чи нецільового використання

грантових коштів або гуманітарних ресурсів, незалежно від наявності прямого «прибутку» у кишені зловмисника [5].

Варто зазначити, що фундаментальна обмеженість вітчизняного підходу полягає в тому, що він створює ідеальні умови для уникнення відповідальності тими суб'єктами, які спрямували міжнародну гуманітарну допомогу на власні амбітні політичні проекти, створення позитивного іміджу або покриття інших операційних витрат, формально не отримуючи від цього фінансового «прибутку». Натомість, стала практика Європейського управління з питань запобігання зловживанням та шахрайству (OLAF) недвозначно кваліфікує такі маніпуляції як беззаперечне шахрайство, оскільки вони руйнують цільову європейську архітектуру солідарного фінансування та підривають довіру до інститутів [6].

Варто акцентувати, що об'єкт цього дослідження вимагає негайного впровадження складної, багатовимірної моделі вирішення проблеми. Національне кримінальне право зобов'язане кардинально трансформувати архітектуру ст. 201-2 КК України, повністю імплементувавши філософію та парадигму Директиви PIF. Об'єктом цього кримінального правопорушення має стати не абстрактний порядок господарювання чи власність окремих фондів, а виключно синергетичний інтерес – фінансові інтереси донорів, збереження цільового призначення транснаціональної допомоги та глобальна довіра до волонтерського руху. Ми наголошуємо на необхідності абсолютної декриміналізації вимоги «отримання прибутку» як обов'язкової ознаки суб'єктивної сторони діяння. Замість цього необхідно криміналізувати будь-яке умисне спотворення звітності, приховування конфлікту інтересів або використання допомоги всупереч задекларованим цілям (non-targeted use). На нашу думку, така інноваційна синергія гарантуватиме, що кримінально караним стане вже сам факт підризу довіри європейських інституцій до процесу чесного розподілу грантових та гуманітарних фондів в Україні [7].

В сучасній адміністративно-правовій та кримінологічній практиці класичним мето-

дом превенції будь-яких злочинів у сфері використання гуманітарної допомоги вважається безапеляційна, тотальна цифровізація та абсолютна публічність баз даних. Відповідно до цих догматів, з 1 грудня 2023 року урядом була запущена «Автоматизована система реєстрації гуманітарної допомоги», яка покликана забезпечити публічність даних про отримувачів та рух вантажів [8]. Домінуючий вітчизняний адміністративний наратив базується на наївній ідеї про те, що максимальне розкриття інформації про суб'єктів волонтерської діяльності перед суспільством є бездоганим та достатнім інструментом викорінення корупційних ризиків [9]. Відповідно, будь-які намагання приховати інформацію або обмежити публічний доступ до таких державних реєстрів автоматично трактуються класичною наукою як свідоме створення умов для латентної злочинності та підготовка до шахрайства.

Таким чином наявність проблеми запобігання злочинам виключно до примітивної відкритості електронних реєстрів є фундаментальною методологічною хибністю, яка входить у пряме протиріччя з імперативними стандартами європейського Загального регламенту про захист даних (GDPR). Ми вважаємо, що вимагаючи безумовної та тотальної транспарентності, національний підхід грубо ігнорує європейський концептуальний standard «Data Responsibility in Humanitarian Action», який ставить на перше місце непопушуваний принцип «не нашкодь» (Do No Harm) [10]. В умовах жорстокого збройного конфлікту оприлюднення чутливих персональних даних кінцевих бенефіціарів, детальних адрес транзитних складів або розкриття логістичних ланцюгів створює екзистенційні безпекові ризики для волонтерів. Прогресивна європейська практика чітко розмежовує фінансову звітність організацій та абсолютну недоторканність персональних даних фізичних осіб. Більше того, неконтрольований, хаотичний збір надлишкових чутливих даних, який зараз активно продукується вітчизняними реєстрами під благородним приводом «боротьби з розкраданням», сам по собі створює ідеальний ґрунт для кіберзлочинності,

ворожих диверсій та масштабного витоку інформації.

Водночас, чинна редакція статті 201-2 КК України є класичним продуктом екстреного, рефлекторного правотворення перших місяців воєнного стану. Законодавець, поспіхом конструюючи цю норму, застосував специфічну, але standardну для пострадянського простору кваліфікуючу архітектуру, де тяжкість злочину визначається переважно математичними критеріями. Так, більшість вітчизняних дослідників підтримують логіку, за якою підвищена кримінальна відповідальність настає, якщо діяння вчинено у «значному розмірі» (який прив'язаний до неоподатковуваних мінімумів доходів громадян), або коли злочин вчиняється службовою особою з використанням свого становища [3]. У рамках цієї догми, зусилля науковців спрямовуються переважно на вдосконалення цього механізму шляхом перегляду розмірів завданої шкоди, уточнення статусу службової особи або механічного розширення переліку предметів посягання. Вони залишаються в полоні традиційної парадигми кваліфікації злочинів проти власності, де без встановлення точної грошової суми завданих збитків притягнення до відповідальності вважається неможливим [11].

Аналізуючи ці класичні підходи, ми змушені наголосити, що такий законодавчий механізм є не просто застарілим, а системно дефектним. Компаративний аналіз вітчизняного механізму у порівнянні із кримінальними кодексами передових країн-членів ЄС яскраво підсвічує концептуальну прірву між нашими правовими системами. Наприклад, § 264 Кримінального кодексу Німеччини взагалі не вимагає доведення факту настання матеріальної шкоди державі або факту успішної фізичної реалізації майна на чорному ринку. Злочин вважається закінченим вже з того моменту, коли особа умисно подала неправдиві відомості компетентному органу, що надає субсидію чи допомогу. Ця норма блискуче спрацювала навіть в екстремальних умовах кризового фінансування під час пандемії, де превенція стала ефективнішою за репресію [12]. Аналогічно, ст. 297 Кримінального кодексу Республі-

ки Польща жорстко криміналізує подання підроблених документів або недостовірних заяв для отримання грантів і дотацій як суто формальний склад злочину. Натомість українська стаття 201-2 КК України вимагає складного і часто неможливого доведення факту завершеного «продажу». Це створює колосальні прогалини у правосудді: якщо корумпована особа просто згноїла гуманітарні харчі на складі або нецільово використала грант без прямого продажу, ця норма стає абсолютно безсилою та паралізованою [13].

Цілком поділяючи тривогу суспільства щодо мародерства, вважаємо за абсолютний пріоритет повністю відмовитися від нежиттєздатної юридичної конструкції ст. 201-2 у її нинішньому вигляді на користь імплементації потужного європейського інституту «шахрайства з фінансовою допомогою». Нова кримінально-правова норма повинна отримати виключно формальний склад. Ми наголошуємо: кримінальній репресії має підлягати не лише фізичний продаж гуманітарки на базарі (що є лише ганебним наслідком), а перш за все умисне внесення недостовірних даних до Єдиного реєстру отримувачів гуманітарної допомоги у момент митного оформлення вантажу, а також свідомі підробка інвентаризаційних описів чи звітів для донорів. На нашу думку, таке рішення дозволить стратегічно змістити акцент державної політики з безглуздої боротьби з наслідками на превентивне притягнення до кримінальної відповідальності зловмисників ще на стадії їхнього доступу до ресурсів, що повною мірою відповідатиме бездоганній логіці німецької та польської кримінальних доктрин.

Висновки. Підсумовуючи вище викладене хочемо зазначити, що сліпе збереження існуючої національної парадигми кримінальної відповідальності за нецільове використання гуманітарної допомоги становить кричущу загрозу для стратегічних євроінтеграційних перспектив України. Так, стаття 201-2 КК України, будучи класичним продуктом реактивного та емоційного законотворення періоду війни, швидко продемонструвала свою небезпечну догматичну обмеженість, глибоку антропо-

центричність та абсолютну нездатність правоохоронної системи охопити новітні, складні форми зловживань у сфері транснаціонального фінансування. Системна відсутність формалізації злочинних діянь на ранніх етапах декларування ресурсів та цинічних маніпуляцій з електронними реєстрами де-факто зводить нанівець увесь превентивний потенціал чинного кримінального закону. Ми переконані, що неминуча трансформація цього інституту має відбуватися не через примітивне, точкове коригування розмірів санкцій чи сум збитків, а виключно шляхом фундаментальної синергії національного права з передовими європейськими стандартами. Беззастережна імплементація безапеляційних вимог Директиви PIF вимагає негайного визнання фінансових інтер-

есів міжнародних інституцій-донорів ключовим, мультиплікативним об'єктом кримінально-правової охорони. Водночас, цифрова архітектура антикорупційних механізмів повинна бути радикально переглянута з урахуванням жорстких інституційних вимог GDPR щодо недоторканності та надійного криптографічного захисту персональних даних бенефіціарів у зонах конфлікту. Тільки такий складний, багатовимірний синергетичний підхід, заснований на європейських кримінально-правових традиціях запровадження формальних складів «субвенційного шахрайства», здатен забезпечити абсолютний пріоритет верховенства права, відновити інституційну довіру західних партнерів та бездоганно захистити благородну цілісність світової гуманітарної місії в Україні.

Список використаних джерел:

1. Дудоров О. О., Мовчан Р. О. Кримінально-правова заборона щодо незаконного використання гуманітарної допомоги: сумнівна законодавча новела. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка*. 2022. Вип. 2 (98). С. 99–115. DOI: 10.33766/2524-0323.98.99-115.
2. Van Ballegooij W. Protecting the EU's Financial Interests through Criminal Law: the Implementation of the "PIF Directive". *Eucrim*. 2021. Vol. 16, no. 3. P. 177–181. DOI: 10.30709/eucrim-2021-022.
3. Швидка О. В. Аналіз складу кримінального правопорушення, передбаченого статтею 201-2 Кримінального кодексу України. *Нове українське право*. 2023. Вип. 3. С. 213–219. DOI: 10.51989/NUL.2023.3.30.
4. Кришевич О. В. Кримінальна відповідальність за нецільове використання гуманітарної допомоги чи один з видів шахрайства. *Вісник Асоціації кримінального права України*. 2022. № 1 (17). С. 173–183. DOI: 10.30525/978-9934-26-229-6-58.
5. Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law. *Official Journal of the European Union*. 2017. L 198. P. 29–41. URL: <https://eur-lex.europa.eu/eli/dir/2017/1371/oj>.
6. Zoli L. The Amendment of the PIF Directive by the New Proposal for a Directive on Combating Corruption. *Eucrim*. 2023. Vol. 18, no. 3. P. 279–281. DOI: 10.30709/eucrim-2023-024.
7. Лісовська О. В. Відмінності складу злочину, передбаченого ст. 201-2 кримінального кодексу України від суміжних складів злочину. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2023. Вип. 80 (2). С. 7–12. DOI: 10.24144/2307-3322.2023.80.2.8.
8. З 1 грудня минулого року запрацювала Автоматизована система реєстрації гуманітарної допомоги. URL: <http://plsz.gov.ua/pocss.html>
9. Муляр Г. В., Бабич В. А. Особливості кримінальної відповідальності за розкрадання гуманітарної допомоги під час дії правового режиму воєнного стану в Україні. *Науковий вісник Ужгородського національного університету. Серія ПРАВО*. 2022. Вип. 72. Ч. 2. С. 184–191. DOI: 10.24144/2307-3322.2022.72.63.
10. IASC Operational Guidance on Data Responsibility in Humanitarian Action. Inter-Agency Standing Committee. 2023. 64 p. URL: <https://interagencystandingcommittee.org/sites/default/files/migrated/2023-04/IASC%20Operational%20Guidance%20on%20Data%20Responsibility%20in%20Humanitarian%20Action%20C%202023.pdf>.
11. Дудоров О. О., Каменський Д. В., Савченко А. В., Мовчан Р. О. Кримінальна відповідальність за незаконне використання гуманітарної допомоги: проблеми кваліфікації та вдосконалення законодавства. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2023. № 1. С. 21–37. DOI: 10.31733/2078-3566-2023-1-21-37.

12. Lorenz H., Turhan E. The Pandemic and Criminal Law – A Look at Theory and Practice in Germany. *Białostockie Studia Prawnicze*. 2021. Vol. 26, No. 6. P. 9–26. DOI: 10.15290/bsp.2021.26.06.01.

13. Станіч В. С. К82 Кримінальний кодекс Республіки Польща / під ред. В. Л. Менчинського. Переклад на українську мову В. С. Станіч – К. : ОБК, 2016. – 138 с. URL: https://jurkniga.ua/contents/kriminalniy-kodeks-respubliki-polshcha.pdf?srsId=AfmBOorWR7ZmUsCYxkFcZokrV4L2n85Lm565Tj1x4aIY_sXXBuqnCKOp

References:

1. Dudorov, O.O., & Movchan, R.O. (2022). Kryminalno-pravova zaborona shchodo nezakonnoho vykorystannia humanitarnoi dopomohy: sumnivna zakonodavcha novela [Criminal law prohibition on the illegal use of humanitarian aid: a dubious legislative novelty]. *Visnyk Luhanskoho derzhavnoho universytetu vnutrishnikh sprav imeni E.O. Didorenka – Bulletin of the Luhansk State University of Internal Affairs named after E.O. Didorenko*, Iss. 2(98). Pp. 99–115. DOI: 10.33766/2524-0323.98.99-115 [in Ukrainian].

2. Van Ballegooij, W. (2021). Protecting the EU's Financial Interests through Criminal Law: the Implementation of the "PIF Directive". *eu crim*, Vol. 16, no. 3. Pp. 177–181. DOI: 10.30709/eu crim-2021-022 [in English].

3. Shvydka, O.V. (2023). Analiz skladu kryminalnoho pravoporushennia, peredbachenoho statteiu 201-2 Kryminalnoho kodeksu Ukrainy [Analysis of the corpus delicti of the criminal offense provided for in Article 201-2 of the Criminal Code of Ukraine]. *Nove ukrainske pravo – New Ukrainian Law*, Iss. 3. Pp. 213–219. DOI: 10.51989/NUL.2023.3.30 [in Ukrainian].

4. Kryshevych, O.V. (2022). Kryminalna vidpovidalnist za netsilove vykorystannia humanitarnoi dopomohy chy ody z vydiv shakhraistva [Criminal liability for the misuse of humanitarian aid or one of the types of fraud]. *Visnyk Asotsiatsii kryminalnoho prava Ukrainy – Bulletin of the Criminal Law Association of Ukraine*, No. 1(17). Pp. 173–183. DOI: 10.30525/978-9934-26-229-6-58 [in Ukrainian].

5. European Parliament and the Council. (2017). Directive (EU) 2017/1371 of the European Parliament and of the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law. *Official Journal of the European Union*, L 198. Pp. 29–41. URL: <https://eur-lex.europa.eu/eli/dir/2017/1371/oj> [in English].

6. Zoli, L. (2023). The Amendment of the PIF Directive by the New Proposal for a Directive on Combating Corruption. *eu crim*, Vol. 18, no. 3. Pp. 279–281. DOI: 10.30709/eu crim-2023-024 [in English].

7. Lisovska, O.V. (2023). Vidminnosti skladu zlochynu, peredbachenoho st. 201-2 kryminalnoho kodeksu Ukrainy vid sumizhnykh skladiv zlochynu [Differences between the corpus delicti of the crime provided for in Art. 201-2 of the Criminal Code of Ukraine and related crimes]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Serii: Pravo – Scientific Bulletin of Uzhhorod National University. Series: Law*, Iss. 80(2). Pp. 7–12. DOI: 10.24144/2307-3322.2023.80.2.8 [in Ukrainian].

8. Z 1 hrudnia mynulooho roku zapratsiuvala Avtomatyzovana systema reiestratsii humanitarnoi dopomohy [Since December 1 of last year, the Automated Registration System for Humanitarian Aid has been launched]. (n.d.). URL: <http://plsz.gov.ua/pocss.html> [in Ukrainian].

9. Muliar, H.V., & Babych, V.A. (2022). Osoblyvosti kryminalnoi vidpovidalnosti za rozkradannia humanitarnoi dopomohy pid chas dii pravovoho rezhymu voiennoho stanu v Ukraini [Features of criminal liability for the theft of humanitarian aid during the legal regime of martial law in Ukraine]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Serii: Pravo – Scientific Bulletin of Uzhhorod National University. Series: Law*, Iss. 72, pt. 2. Pp. 184–191. DOI: 10.24144/2307-3322.2022.72.63 [in Ukrainian].

10. Inter-Agency Standing Committee. (2023). IASC Operational Guidance on Data Responsibility in Humanitarian Action. 64 p. URL: <https://interagencystandingcommittee.org/sites/default/files/migrated/2023-04/IASC%20Operational%20Guidance%20on%20Data%20Responsibility%20in%20Humanitarian%20Action%2C%202023.pdf> [in English].

11. Dudorov, O.O., Kamenskyi, D.V., Savchenko, A.V., & Movchan, R.O. (2023). Kryminalna vidpovidalnist za nezakonne vykorystannia humanitarnoi dopomohy: problemy kvalifikatsii ta vdoskonalennia zakonodavstva [Criminal liability for the illegal use of humanitarian aid: problems of qualification and improvement of legislation]. *Naukovyi visnyk Dnipropetrovskoho derzhavnoho universytetu vnutrishnikh sprav – Scientific Bulletin of Dnipropetrovsk State University of Internal Affairs*, No. 1. Pp. 21–37. DOI: 10.31733/2078-3566-2023-1-21-37 [in Ukrainian].

12. Lorenz, H., & Turhan, E. (2021). The Pandemic and Criminal Law – A Look at Theory and Practice in Germany. *Białostockie Studia Prawnicze*, Vol. 26, no. 6. Pp. 9–26. DOI: 10.15290/bsp.2021.26.06.01 [in English].

13. Stanich, V.S. (Trans.). (2016). Kryminalnyi kodeks Respubliky Polshcha [Criminal Code of the Republic of Poland] (V.L. Menchynskyi, Ed.). Kyiv: OVK. 138 p. URL: https://jurkniga.ua/contents/kryminalniy-kodeks-respubliki-polshcha.pdf?srsId=AfmBOorWR7ZmUsCYxkFcZokrV4L2n85Lm565Tj1x4aIY_sXXBuqnCKOp [in Ukrainian].

Creative Commons Attribution 4.0
International (CC BY 4.0)



Дата першого надходження статті до видання: 20.07.2026
Дата прийняття статті до друку після рецензування: 19.08.2026
Дата публікації (оприлюднення) статті: 00.00.2026

УДК 351.862:355.58:351.74

DOI <https://doi.org/10.32782/2311-8040/2026-2-5>

Лиса Марія Олегівна,

кандидат історичних наук, доцент,
доцент кафедри вогневої підготовки,
Львівський державний університет внутрішніх справ,
вулиця Городоцька, 26, Львів, 79000, Україна
ORCID: <https://orcid.org/0000-0001-9585-8007>

Булачек Володимир Романович,

кандидат історичних наук, доцент,
доцент кафедри тактико-спеціальної підготовки,
Львівський державний університет внутрішніх справ,
вулиця Городоцька, 26, Львів, 79000, Україна
ORCID: <https://orcid.org/0000-0003-3067-7955>

Курляк Мар'ян Дмитрович,

кандидат економічних наук, доцент,
завідувач кафедри тактико-спеціальної підготовки,
Львівський державний університет внутрішніх справ,
вулиця Городоцька, 26, Львів, 79007, Україна
ORCID: <https://orcid.org/0000-0001-8062-4806>

Синенький Володимир Михайлович,

кандидат історичних наук,
доцент кафедри тактико-спеціальної підготовки,
Львівський державний університет внутрішніх справ,
вулиця Городоцька, 26, Львів, 79000, Україна
ORCID: <https://orcid.org/0000-0002-9652-2211>

Гречанюк Андрій Олексійович,

старший викладач кафедри тактико-спеціальної підготовки,
Львівський державний університет внутрішніх справ,
вулиця Городоцька, 26, Львів, 79000, Україна
ORCID: <https://orcid.org/0000-0002-7054-4391>

КООРДИНАЦІЯ СИЛ ТА ЗАСОБІВ ПІД ЧАС ЛІКВІДАЦІЇ НАСЛІДКІВ НАДЗВИЧАЙНИХ СИТУАЦІЙ

***Анотація.** У статті досліджуються особливості управління кризовими ситуаціями в умовах воєнного стану, а також механізми взаємодії між органами державної влади, правоохоронними структурами, військовими формуваннями, аварійно-рятувальними службами та органами місцевого самоврядування під час реагування на надзвичайні події. Актуальність теми обумовлена суттєвим зростанням кількості кризових явищ, спричинених збройною агресією проти України, що потребує удосконалення існуючих підходів до координації дій суб'єктів сектору безпеки і цивільного захисту.*

Метою дослідження є аналіз сучасної системи кризового управління в умовах воєнного стану, визначення особливостей міжвідомчої взаємодії під час реагування на кризові ситуації та обґрунтування напрямів підвищення ефективності координації між правоохоронними, рятувальними та військовими структурами. Для досягнення поставленої мети використано комплекс загальнонаукових і спеціальних методів дослідження, зокрема аналіз нормативно-правової бази, системний підхід, порівняльний аналіз, узагальнення наукових джерел та вивчення міжнародного досвіду кризового реагування.

У роботі розглянуто теоретичні засади кризового управління та визначено його місце у системі забезпечення національної безпеки держави. Проаналізовано нормативно-правове регулювання діяльності органів

влади в умовах воєнного стану та надзвичайних ситуацій. Особливу увагу приділено питанням інформаційного обміну, функціонуванню ситуаційних центрів, використанню цифрових платформ управління та організації оперативного інформування населення. Встановлено, що своєчасний обмін достовірною інформацією є одним із ключових факторів ефективного реагування на кризові події.

Досліджено особливості взаємодії між Національною поліцією України, Державною службою України з надзвичайних ситуацій, Національною гвардією України, військовими адміністраціями та іншими суб'єктами кризового реагування. Визначено, що результативність спільних дій залежить від чіткого розподілу повноважень, узгодженості управлінських рішень, наявності єдиних комунікаційних каналів та готовності до оперативного обміну інформацією.

У процесі дослідження виявлено основні проблеми координації в умовах бойових дій, серед яких руйнування комунікаційної інфраструктури, дефіцит матеріально-технічних ресурсів, необхідність одночасного реагування на декілька кризових подій та висока динаміка зміни оперативної обстановки. Обґрунтовано, що зазначені фактори істотно впливають на швидкість прийняття управлінських рішень та ефективність проведення рятувальних, евакуаційних і правоохоронних заходів.

Окрему увагу приділено аналізу зарубіжного досвіду кризового управління. Встановлено, що ефективні міжнародні моделі ґрунтуються на принципах міжвідомчої інтеграції, створенні єдиних координаційних центрів, використанні сучасних інформаційно-комунікаційних технологій та регулярній підготовці персоналу до дій у складних кризових умовах. Доведено доцільність адаптації окремих міжнародних практик до української системи цивільного захисту та безпеки.

За результатами дослідження сформульовано рекомендації щодо вдосконалення механізмів кризового управління в Україні, підвищення рівня міжвідомчої взаємодії, розвитку цифрових інструментів координації та зміцнення спроможностей суб'єктів реагування в умовах воєнного стану.

Ключові слова: кризове управління, воєнний стан, надзвичайні ситуації, міжвідомча взаємодія, цивільний захист, Національна поліція України, ДСНС України, координація сил і засобів, інформаційний обмін, кризове реагування, національна безпека, управління ризиками.

Lysa Mariia, Bulachek Volodymyr, Kurliak Marian, Synenkyi Volodymyr, Grechanuk Andrii.
COORDINATION OF FORCES AND RESOURCES DURING THE ELIMINATION OF THE CONSEQUENCES OF EMERGENCIES

Abstract. The article examines the specific features of crisis management under martial law, as well as the mechanisms of interaction among public authorities, law enforcement agencies, military formations, emergency rescue services, and local self-government bodies in responding to emergency situations. The relevance of the study is determined by the significant increase in crisis situations caused by the armed aggression against Ukraine, which necessitates the improvement of existing approaches to coordinating the activities of actors within the security and civil protection sectors.

The purpose of the study is to analyse the contemporary crisis management system under martial law, identify the specific features of interagency cooperation in responding to crisis situations, and substantiate directions for improving coordination among law enforcement, emergency rescue, and military agencies. To achieve this objective, a comprehensive set of general scientific and special legal research methods was employed, including the analysis of the regulatory and legal framework, the systems approach, comparative analysis, the generalisation of scientific literature, and the examination of international experience in crisis response.

The study explores the theoretical foundations of crisis management and determines its role within the national security system. It analyses the legal and regulatory framework governing the activities of public authorities under martial law and during emergencies. Particular attention is paid to information exchange, the operation of situation centres, the use of digital management platforms, and the organisation of public emergency notification. The findings demonstrate that the timely exchange of reliable information constitutes one of the key prerequisites for an effective response to crisis events.

The article also examines the specific features of cooperation among the National Police of Ukraine, the State Emergency Service of Ukraine, the National Guard of Ukraine, military administrations, and other entities involved in crisis response. It is established that the effectiveness of joint operations depends on a clear distribution of powers and responsibilities, coordinated managerial decision-making, the availability of integrated communication channels, and the capacity for rapid information exchange.

The study identifies the principal challenges affecting coordination during armed conflict, including the destruction of communication infrastructure, shortages of material and technical resources, the simultaneous occurrence of multiple crisis events, and the rapidly changing operational environment. It is substantiated that these factors significantly influence the speed of managerial decision-making and the effectiveness of rescue, evacuation, and law enforcement operations.

Special attention is devoted to the analysis of international experience in crisis management. The study demonstrates that effective international models are based on the principles of interagency integration, unified coordination centres, advanced information and communication technologies, and systematic personnel training for operations in complex crisis environments. The findings confirm the feasibility of adapting selected international best practices to Ukraine's civil protection and security system.

Based on the findings, recommendations are proposed for improving crisis management mechanisms in Ukraine, strengthening interagency cooperation, advancing digital coordination tools, and enhancing the operational capacity of crisis response entities under martial law.

Key words: crisis management, martial law, emergencies, interagency cooperation, civil protection, National Police of Ukraine, State Emergency Service of Ukraine, coordination of forces and resources, information exchange, crisis response, national security, risk management.

Вступ. Сучасні надзвичайні ситуації характеризуються високим рівнем складності, масштабності наслідків та необхідністю оперативного залучення значної кількості сил і засобів різних державних органів. Особливої актуальності проблема координації набуває в умовах воєнного стану, коли надзвичайні ситуації можуть виникати внаслідок бойових дій, ракетних та дронівих атак, руйнування критичної інфраструктури, техногенних аварій і гуманітарних криз. За таких умов ефективність реагування безпосередньо залежить від рівня організації взаємодії між правоохоронними органами, рятувальними службами, військовими формуваннями, органами місцевого самоврядування та закладами охорони здоров'я.

Ліквідація наслідків надзвичайних ситуацій є комплексним процесом, який потребує чіткого розподілу повноважень, узгодженості управлінських рішень, своєчасного обміну інформацією та ефективного використання наявних ресурсів. В Україні ключову роль у виконанні таких завдань відіграють Національна поліція України, Державна служба України з надзвичайних ситуацій, Національна гвардія України, військові адміністрації, органи місцевого самоврядування та медичні служби. Водночас практика реагування на наслідки воєнних загроз демонструє наявність низки організаційних і технічних проблем, пов'язаних із забезпеченням міжвідомчої взаємодії, функціонуванням систем зв'язку, координацією дій у режимі реального часу та оперативним інформуванням населення.

Особливе значення в сучасних умовах має впровадження цифрових технологій управ-

ління кризовими ситуаціями, створення ситуаційних центрів, використання автоматизованих систем моніторингу та обміну даними. Водночас бойові дії суттєво ускладнюють процес управління силами та засобами через руйнування комунікаційної інфраструктури, обмеженість матеріально-технічних ресурсів, необхідність одночасного реагування на декілька надзвичайних подій та постійну зміну оперативної обстановки.

Важливим напрямом удосконалення національної системи кризового реагування є вивчення міжнародного досвіду організації міжвідомчої координації під час масштабних надзвичайних ситуацій і збройних конфліктів. Практика провідних держав світу свідчить про ефективність інтегрованих моделей управління, заснованих на єдиних центрах координації, стандартизованих процедурах взаємодії та сучасних інформаційно-комунікаційних технологіях.

Метою даного дослідження є комплексний аналіз організаційно-правових та управлінських засад координації сил і засобів під час ліквідації наслідків надзвичайних ситуацій, визначення основних проблем міжвідомчої взаємодії в умовах воєнного стану, а також вироблення пропозицій щодо підвищення ефективності управління та координації суб'єктів реагування з урахуванням міжнародного досвіду кризового менеджменту.

Матеріали та методи. Дослідження ґрунтується на комплексному використанні загальнонаукових і спеціально-юридичних методів наукового пізнання, що забезпечило всебічний аналіз організаційно-правових засад координації сил і засобів під час ліквідації наслід-

ків надзвичайних ситуацій в умовах воєнного стану.

Емпіричну основу дослідження становили положення нормативно-правових актів України, що регламентують діяльність суб'єктів сектору безпеки і оборони та Єдиної державної системи цивільного захисту, зокрема Кодекс цивільного захисту України, закони України «Про Національну поліцію», «Про Національну гвардію України», «Про правовий режим воєнного стану», «Про національну безпеку України», а також підзаконні нормативно-правові акти Кабінету Міністрів України та Міністерства внутрішніх справ України. Крім того, використано сучасні наукові публікації українських і зарубіжних учених (2022–2025 рр.), офіційні документи НАТО, OECD, Європейського Союзу та інші міжнародні матеріали, присвячені питанням кризового управління, цивільного захисту, міжвідомчої взаємодії та координації правоохоронних і рятувальних структур.

Методологічну основу дослідження становить діалектичний метод, який дав змогу розглянути кризове управління як динамічну систему, що розвивається під впливом сучасних безпекових викликів і трансформації державного управління. Застосування системного методу дозволило дослідити взаємозв'язки між Національною поліцією України, Державною службою України з надзвичайних ситуацій, Національною гвардією України, військовими адміністраціями, органами місцевого самоврядування та медичними службами як елементами єдиної системи реагування на надзвичайні ситуації.

За допомогою формально-юридичного методу проаналізовано норми чинного законодавства України, що визначають компетенцію, повноваження та порядок взаємодії суб'єктів кризового реагування. Порівняльно-правовий метод використано для дослідження міжнародних моделей кризового управління, зокрема механізмів координації, що застосовуються країнами-членами НАТО та Європейського Союзу, а також для визначення можливостей імплементації їх окремих елементів у національну систему цивільного захисту.

Структурно-функціональний метод застосовано під час аналізу розподілу функцій між суб'єктами міжвідомчої взаємодії, оцінювання особливостей функціонування оперативних штабів, ситуаційних центрів, цифрових платформ управління та систем інформаційного обміну. Використання аналізу та синтезу дозволило узагальнити наукові підходи до визначення поняття кризового управління, виокремити основні проблеми координації в умовах бойових дій та сформулювати напрями їх подолання.

Для дослідження міжнародного досвіду застосовано порівняльний та компаративний аналіз, що дав змогу оцінити ефективність моделей Incident Command System, Integrated Emergency Management, механізмів діяльності Euro-Atlantic Disaster Response Coordination Centre та Crisis Management and Disaster Response Centre of Excellence. Це дозволило визначити найбільш перспективні практики, які можуть бути адаптовані до української системи кризового управління.

На завершальному етапі дослідження використано метод узагальнення, за допомогою якого систематизовано отримані результати, сформульовано наукові висновки та обґрунтовано практичні рекомендації щодо вдосконалення міжвідомчої взаємодії, інформаційного забезпечення та координації сил і засобів під час ліквідації наслідків надзвичайних ситуацій в умовах воєнного стану. Запропонований комплекс методів забезпечив логічність, об'єктивність та достовірність отриманих результатів, а також дозволив комплексно дослідити організаційно-правові та управлінські аспекти кризового реагування в сучасних безпекових умовах.

Результати. Ефективність ліквідації наслідків надзвичайних ситуацій безпосередньо залежить від рівня організації міжвідомчої взаємодії між усіма суб'єктами сектору безпеки, оборони та цивільного захисту. В умовах воєнного стану в Україні ця проблема набуває особливої актуальності, оскільки значна частина надзвичайних ситуацій спричиняється збройною агресією, ракетними ударами, руйнуванням об'єктів критичної інфраструктури

та виникненням масштабних гуманітарних криз. За таких обставин ефективне реагування можливе лише за умови узгодженої діяльності Національної поліції України, Державної служби України з надзвичайних ситуацій, Національної гвардії України, органів місцевого самоврядування, військових адміністрацій, медичних установ та інших суб'єктів Єдиної державної системи цивільного захисту [1, с. 254; 2, с. 89–90].

Нормативно-правову основу міжвідомчої взаємодії становлять положення Кодексу цивільного захисту України, Законів України «Про Національну поліцію», «Про Національну гвардію України», «Про правовий режим воєнного стану», а також підзаконні нормативно-правові акти, що регламентують функціонування ЄДСЦЗ. Відповідно до чинного законодавства, усі суб'єкти реагування здійснюють свою діяльність у межах єдиної системи управління, спрямованої на координацію дій органів державної влади, місцевого самоврядування, спеціалізованих служб та аварійно-рятувальних формувань під час виникнення надзвичайних ситуацій різного характеру.

Провідна роль у безпосередній ліквідації наслідків надзвичайних ситуацій належить ДСНС, яка організовує проведення аварійно-рятувальних та інших невідкладних робіт, здійснює евакуацію населення, координує діяльність спеціалізованих служб і забезпечує функціонування системи цивільного захисту. Водночас ефективність таких заходів значною мірою залежить від взаємодії з Національною поліцією України, яка відповідає за підтримання громадського порядку, охорону місць подій, регулювання дорожнього руху та забезпечення безпеки населення під час проведення рятувальних операцій [3, с. 4; 4, с. 238].

Дослідження сучасної практики реагування свідчать, що найбільш результативними механізмами співпраці між ДСНС та Національною поліцією є створення спільних оперативних штабів, використання єдиних каналів зв'язку, оперативний обмін інформацією та проведення регулярних міжвідомчих навчань. Під час ліквідації наслідків ракетних ударів, пожеж, вибухів чи техногенних аварій

поліцейські підрозділи забезпечують ізоляцію небезпечних зон, контроль доступу до місць проведення робіт та сприяють евакуації населення, тоді як рятувальники здійснюють пошук постраждалих, деблокування людей із завалів та усунення вторинних факторів небезпеки [4, с. 240].

Важливим елементом системи міжвідомчої взаємодії в умовах воєнного стану є Національна гвардія України. Її підрозділи залучаються до охорони стратегічно важливих об'єктів, забезпечення правопорядку, супроводу гуманітарних вантажів, організації евакуаційних заходів та підтримки режимних обмежень у районах проведення спеціальних операцій. Наукові дослідження свідчать, що ефективна взаємодія Національної гвардії України з Національною поліцією України та іншими структурами сектору безпеки дозволяє суттєво підвищити рівень громадської безпеки та оперативності реагування на кризові ситуації [5, с. 128; 6, с. 25]. Особливого значення така координація набуває під час масових переміщень населення, проведення евакуаційних заходів та функціонування пунктів тимчасового розміщення громадян.

Суттєву роль у системі реагування відіграють органи місцевого самоврядування та військові адміністрації, які забезпечують організаційне та ресурсне супроводження заходів цивільного захисту. Саме на місцевому рівні формується первинна інформація про масштаби руйнувань, потреби населення, наявність матеріально-технічних ресурсів і можливості їх оперативного залучення. Військові адміністрації, створені відповідно до законодавства в умовах воєнного стану, координують діяльність органів влади, забезпечують взаємодію з військовими формуваннями та сприяють концентрації необхідних сил і засобів на найбільш критичних напрямках.

Практика функціонування системи цивільного захисту в Україні демонструє високу ефективність штабної форми управління. Створення регіональних та місцевих координаційних штабів забезпечує централізоване планування, розподіл ресурсів, визначення пріоритетів реагування та контроль за вико-

нанням управлінських рішень. Такий підхід дозволяє оперативно адаптувати алгоритми дій до змін оперативної обстановки та забезпечувати узгодженість роботи всіх задіяних служб [1, с. 255–256; 2, с. 90].

Не менш важливою складовою міжвідомчої взаємодії є співпраця з медичними службами та закладами охорони здоров'я. У випадку виникнення надзвичайних ситуацій саме медичні підрозділи забезпечують надання екстреної медичної допомоги, медичне сортування постраждалих, їх транспортування та подальшу евакуацію до спеціалізованих лікувальних закладів. Налагоджена координація між ДСНС, Національною поліцією України, медичними службами та органами місцевої влади сприяє скороченню часу реагування та підвищує шанси на збереження життя і здоров'я потерпілих.

Вагомим чинником підвищення ефективності міжвідомчої взаємодії є впровадження сучасних інформаційно-комунікаційних технологій. Використання цифрових платформ управління, геоінформаційних систем, ситуаційних центрів та автоматизованих систем підтримки прийняття рішень забезпечує оперативний обмін інформацією між усіма учасниками реагування. Завдяки цьому стає можливим швидко отримання даних про масштаби надзвичайної ситуації, потребу в додаткових ресурсах, кількість постраждалих та хід виконання рятувальних робіт, що суттєво підвищує ефективність управління кризовими процесами.

Міжнародний досвід також підтверджує визначальне значення міжвідомчої координації для успішного реагування на кризові події. У державах-членах НАТО та Європейського Союзу широко використовуються моделі Integrated Emergency Management та Incident Command System, які базуються на принципах єдиного керівництва, стандартизованих процедур взаємодії та централізованого інформаційного обміну. Практична реалізація таких підходів забезпечує чіткий розподіл функцій між усіма учасниками реагування та мінімізує ризики дублювання повноважень, що може бути корисним для подальшого вдосконалення української системи кризового управління [6, с. 27; 7, с. 80–81].

Налагоджена система міжвідомчої взаємодії створює організаційне підґрунтя для ефективного реагування на надзвичайні ситуації, проте результативність практичних заходів значною мірою залежить від чіткості алгоритмів управління та послідовності дій усіх залучених сил і засобів. У зв'язку з цим доцільним є подальший розгляд особливостей координації оперативних штабів, процедур прийняття управлінських рішень і механізмів управління силами під час ліквідації наслідків надзвичайних ситуацій в умовах воєнного стану.

Ефективність реагування на надзвичайні ситуації в умовах воєнного стану значною мірою залежить від своєчасного інформаційного обміну між усіма суб'єктами системи цивільного захисту та здатності органів управління оперативно координувати наявні сили і засоби. В умовах високої динаміки кризових подій інформація стає одним із ключових ресурсів, від якого залежить швидкість ухвалення управлінських рішень, розподіл ресурсів і результативність аварійно-рятувальних заходів. Тому сучасна система реагування повинна базуватися на інтегрованих цифрових механізмах збору, обробки та передачі інформації між усіма учасниками кризового управління [8, с. 407].

Одним із пріоритетних напрямів розвитку системи цивільного захисту є впровадження сучасних цифрових платформ управління, які забезпечують централізоване накопичення, аналіз та поширення інформації про надзвичайні події. Такі платформи дозволяють у режимі реального часу отримувати дані про масштаби руйнувань, кількість постраждалих, стан критичної інфраструктури, потреби у додаткових силах та засобах, а також контролювати виконання поставлених завдань. Дослідження у сфері цифровізації кризового управління свідчать, що використання інтегрованих інформаційних систем сприяє підвищенню швидкості реагування та покращенню координації між різними органами влади і спеціалізованими службами [8, с. 409; 9, с. 223].

Особливу роль у процесі управління силами відіграють ситуаційні центри, які функціонують як інформаційно-аналітичні вузли підтримки прийняття рішень. Їх основним за-

вданням є збір інформації з різних джерел, її узагальнення, прогнозування розвитку подій та підготовка пропозицій для керівників оперативних штабів. Завдяки використанню геоінформаційних технологій, електронних карт, систем моніторингу та засобів відеоспостереження ситуаційні центри забезпечують комплексне бачення оперативної обстановки та дозволяють швидко визначати пріоритетні напрямки реагування [8, с. 407–420].

Важливим елементом управління силами є налагодження безперервної комунікації між Національною поліцією України, ДСНС, Національною гвардією України, військовими адміністраціями, медичними службами та органами місцевого самоврядування. Для цього використовуються захищені канали зв'язку, автоматизовані системи оповіщення, електронний документообіг та спеціалізовані програмні комплекси, що забезпечують оперативний обмін даними між усіма суб'єктами реагування. Цифровізація комунікаційних процесів дозволяє мінімізувати часові втрати та зменшити ризик виникнення інформаційних розривів між окремими відомствами [9, с. 224–226].

Окремого значення набуває оперативне інформування населення про загрози та порядок дій у надзвичайних ситуаціях. У сучасних умовах для цього використовуються державні системи оповіщення, мобільні застосунки, офіційні вебресурси органів влади, соціальні мережі та засоби масової інформації. Своєчасне доведення достовірної інформації до населення сприяє зменшенню панічних настроїв, підвищенню рівня громадської безпеки та забезпечує більш ефективне проведення евакуаційних і рятувальних заходів. Водночас цифрові технології дозволяють не лише інформувати громадян, а й отримувати від них зворотний зв'язок щодо потреб у допомозі, стану інфраструктури та інших важливих аспектів кризової ситуації [8, с. 411; 9, с. 223–229].

Розвиток систем інформаційного обміну, цифрових платформ управління та ситуаційних центрів створює необхідні передумови для підвищення ефективності реагування на надзвичайні ситуації. Проте практична результативність цих механізмів значною мірою

визначається якістю підготовки персоналу та здатністю підрозділів діяти відповідно до встановлених алгоритмів. У зв'язку з цим наступним напрямом дослідження є аналіз підготовки особового складу, проведення спільних тренувань і формування професійних компетентностей, необхідних для діяльності в умовах кризових ситуацій.

Координація дій органів державної влади, підрозділів цивільного захисту, військових формувань та інших суб'єктів реагування в умовах бойових дій є одним із найскладніших елементів управління кризовими ситуаціями. На відміну від реагування на надзвичайні ситуації мирного часу, воєнні дії характеризуються високим рівнем невизначеності, значними руйнуваннями інфраструктури, обмеженістю ресурсів та швидкою зміною оперативної обстановки. У таких умовах ефективність взаємодії безпосередньо впливає на своєчасність прийняття управлінських рішень, безпеку населення та результативність проведення аварійно-рятувальних і гуманітарних заходів [10, с. 15].

Одним із ключових факторів, що ускладнюють координацію, є руйнування комунікаційної інфраструктури. Унаслідок ракетних ударів, артилерійських обстрілів та диверсійних дій можуть виходити з ладу телекомунікаційні мережі, центри обробки даних, об'єкти енергопостачання та канали передачі інформації. Це призводить до втрати зв'язку між органами управління різних рівнів, затримки передачі розпоряджень і ускладнення отримання актуальної інформації про розвиток кризової ситуації. Особливо критичними такі наслідки є для регіонів, де одночасно здійснюються евакуаційні заходи, ліквідація наслідків обстрілів та забезпечення життєдіяльності населення [11, с. 74].

Суттєвим викликом залишається дефіцит ресурсів, який проявляється у нестачі особового складу, спеціалізованої техніки, паливно-мастильних матеріалів, засобів зв'язку та матеріальних резервів. Під час тривалих бойових дій значна частина ресурсів спрямовується на виконання оборонних завдань, що обмежує можливості цивільного захисту щодо опера-

тивного реагування на надзвичайні події. Крім того, пошкодження транспортної інфраструктури ускладнює логістичне забезпечення та своєчасне переміщення сил і засобів до районів проведення рятувальних робіт. Міжнародний досвід реагування на комплексні кризи свідчить, що нестача ресурсів є одним із головних чинників зниження ефективності міжвідомчої взаємодії та гуманітарного реагування [12, с. 803–807].

Додаткові труднощі створює одночасне виникнення декількох кризових подій, коли органи управління змушені паралельно реагувати на наслідки бойових дій, техногенні аварії, пожежі, руйнування критичної інфраструктури та гуманітарні проблеми. У таких умовах виникає конкуренція за обмежені ресурси, що потребує оперативного визначення пріоритетів та постійного коригування планів реагування. Координаційні центри повинні забезпечувати синхронізацію дій великої кількості учасників, включаючи органи влади, аварійно-рятувальні служби, військові підрозділи, медичні установи та міжнародні гуманітарні організації.

Окремим фактором є висока динаміка зміни оперативної обстановки, характерна для сучасних воєнних конфліктів. Інформація про загрози, масштаби руйнувань, маршрути евакуації чи безпечні райони може втрачати актуальність протягом кількох годин або навіть хвилин. Це вимагає від суб'єктів реагування постійного моніторингу ситуації, швидкого оновлення даних та гнучкого коригування управлінських рішень. Відсутність своєчасного обміну інформацією або затримка в ухваленні рішень здатні суттєво знизити ефективність реагування та збільшити ризики для населення і персоналу оперативних служб.

Зазначені проблеми свідчать про необхідність формування стійких механізмів міжвідомчої взаємодії, розвитку резервних систем управління та впровадження сучасних підходів до планування кризового реагування. Саме тому доцільним є подальший розгляд практичних механізмів підвищення ефективності координації та напрямів удосконалення системи управління кризовими ситуаціями в умовах воєнного стану.

Досвід провідних держав і міжнародних організацій свідчить, що ефективне кризове управління ґрунтується на інтегрованій координації правоохоронних органів, аварійно-рятувальних служб, військових структур та органів державної влади. Особливого значення така взаємодія набуває під час масштабних надзвичайних ситуацій, терористичних загроз і збройних конфліктів.

Однією з найбільш розвинених моделей є система кризового менеджменту НАТО, яка передбачає використання як військових, так і цивільних інструментів реагування. Основними принципами є міжвідомча координація, оперативний обмін інформацією, спільне планування дій та багаторівневе управління кризами [13].

Важливим елементом натівської системи є Euro-Atlantic Disaster Response Coordination Centre – головний механізм цивільного реагування НАТО на надзвичайні ситуації. Центр забезпечує координацію міжнародної допомоги, обмін інформацією між державами та взаємодію рятувальних служб під час масштабних криз [14].

Значну роль у розвитку сучасних підходів до кризового управління відіграє Crisis Management and Disaster Response Centre of Excellence. Центр розробляє методики міжвідомчої взаємодії, проводить навчання та відпрацьовує сценарії реагування на комплексні кризові ситуації, включаючи збройні конфлікти та техногенні катастрофи [15; 16].

Практична підготовка фахівців здійснюється через спеціалізовані міжнародні програми, зокрема Crisis Management and Disaster Response Course, під час яких відпрацьовуються механізми координації між правоохоронними органами, рятувальними службами та військовими структурами в умовах швидкої зміни оперативної обстановки [17].

Аналіз зарубіжного досвіду демонструє, що ключовими умовами ефективного кризового управління є створення єдиного координаційного центру, використання сучасних інформаційно-комунікаційних систем, стандартизовані процедури взаємодії та регулярна спільна підготовка персоналу. Зазначені підходи можуть

бути використані для подальшого вдосконалення системи кризового управління та цивільного захисту України в умовах воєнних загроз і надзвичайних ситуацій.

Висновок. У результаті проведеного дослідження встановлено, що ефективне управління кризовими ситуаціями в умовах воєнного стану є одним із ключових чинників забезпечення національної безпеки, захисту населення та підтримання стійкості функціонування держави. Сучасні загрози, пов'язані зі збройною агресією, характеризуються комплексністю, високою динамікою розвитку та значним впливом на критичну інфраструктуру, що потребує скоординованих дій усіх суб'єктів сектору безпеки і цивільного захисту.

Дослідження показало, що важливу роль у системі кризового реагування відіграє взаємодія між органами державної влади, правоохоронними структурами, військовими формуваннями, аварійно-рятувальними службами та органами місцевого самоврядування. Результативність такої взаємодії значною мірою залежить від ефективного інформаційного обміну, наявності сучасних цифрових систем управління, чітко визначених повноважень та узгоджених процедур реагування.

Водночас було виявлено низку проблем, які ускладнюють координацію в умовах бо-

йових дій, зокрема руйнування комунікаційної інфраструктури, дефіцит ресурсів, необхідність одночасного реагування на декілька кризових подій та постійні зміни оперативної обстановки. Зазначені фактори потребують підвищення адаптивності системи управління та розвитку резервних механізмів координації.

Аналіз міжнародного досвіду засвідчив, що підвищення ефективності кризового управління досягається завдяки впровадженню інтегрованих моделей міжвідомчої взаємодії, створенню єдиних координаційних центрів, використанню сучасних інформаційно-комунікаційних технологій та систематичній підготовці персоналу. Адаптація таких підходів до національних умов сприятиме посиленню спроможностей України щодо реагування на надзвичайні ситуації та кризові явища в умовах воєнного стану.

Отже, удосконалення механізмів координації, цифровізація процесів управління, розвиток міжвідомчої взаємодії та впровадження кращих міжнародних практик є пріоритетними напрямками подальшого розвитку системи кризового управління України, що дозволить забезпечити більш ефективний захист населення та державних інтересів в умовах сучасних безпекових викликів.

Список використаних джерел:

1. Логвиненко Б.О., Дерев'янюк К.В. Взаємодія Національної поліції та Збройних сил України під час дії особливого правового режиму воєнного стану. Interaction between law enforcement agencies and public authorities to create a secure environment under martial law : колективна монографія. 2025. С. 254–272. <https://doi.org/10.30525/978-9934-26-589-1-13>
2. Honchuk A. A. Interaction of the Military Law Enforcement Service (Military Police) with the National Police and the SSU during stabilization operations in the “grey zone” and in de-occupied territories. *Актуальні питання розвитку сектору безпеки і оборони (зарубіжний досвід): зб. тез доп. учасників XXVII Міжнарод. наук.-практ. конф. для здоб. освіти інозем. мовами (м. Вінниця, Україна, 3 квіт. 2026 р.)*. МВС України, Харків. нац. ун-т внут. справ, Каф. мовн. підготовки. Вінниця: ХНУВС, 2026. С. 89–92. URL: <https://dspace.univd.edu.ua/items/b505166e-d8c6-48d4-9611-77231902a232>
3. Боровікова В.С., Лозинська І.В., Майстренко М.М., Павлик Л.В. Діяльність поліцейського щодо виявлення правопорушень у громадських місцях : методичні рекомендації. Львів : ЛьвДУВС, 2018. 76 с.
4. Голуб В. А. Взаємодія органів Національної поліції України та Державної служби України з надзвичайних ситуацій під час подій, пов'язаних із пожежами. *Проблеми сучасної поліцейстики : тези доп. наук.-практ. конф. (м. Харків, 20 квіт. 2022 р.)*. МВС України, Харків. нац. ун-т внут. справ, Ф-т № 6, Каф. правоох. діяльності та поліцейстики, Наук. парк «Наука та безпека». Харків, 2022. С. 238–241. URL: <https://dspace.univd.edu.ua/items/621fe375-3d7f-4394-b99d-538b835263aa>
5. Pylyp V. Interaction between the National guard of Ukraine and civil society institutions. *Honor and Law*. 2024. Vol. 1 (88). P. 128–133. <https://doi.org/10.33405/2078-7480/2024/1/88/302284>

6. Danko V. Theoretical principles of organizing cooperation between the National Guard of Ukraine and security sector institutions in ensuring public security. *The scientific journal of the National Academy of National Guard Honor and Law*. 2025. Iss. 3. 25–32. 10.33405/2078-7480/2025/3/94/349219
7. Чорнопіщук І. Обґрунтування основних напрямків наукових досліджень щодо дій прикордонного загону під час виконання завдань у кризових ситуаціях воєнного характеру. *Безпека держави*. 2023. Вип. 1(1). С. 80–85. <https://doi.org/10.33405/2786-8613/2023/1/1/288279>
8. Пожуєва Т., Щегловатих Д. Цифрові технології в антикризовому управлінні. *Економічний аналіз*. 2024. Вип. 34(2). с. 407–420. <http://dx.doi.org/10.35774/econa2024.02.407>
9. Рибалко-Рак Л., Гусаковська Т., Опришко В. Цифровізація та антикризове управління: стратегічні зміни для розвитку конкурентоспроможної екосистеми. *Проблеми економіки*. 2025. Вип. 1. С. 223–229. 10.32983/2222-0712-2025-1-223-229.
10. OECD. Enhancing Crisis Management and Resilience in the Context of Armed Conflicts. Paris: OECD Publishing, 2024. ISBN 978-92-64-98765-4 URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2013/08/oecd-risk-management_g17a2354/5k41rbd1l1zr7-en.pdf
11. Nazarenko O., Holovan O., Rudynskyi V. Assessment of Critical Infrastructure Vulnerability in Ukraine During Military Threats. *Безпека держави*. 2025. Вип. 1(5). С. 73–82. URL: <https://sts.nangu.edu.ua/article/download/336731/325342>
12. Maghsoudi, A., Falagara Sigala, I., Piotrowicz, W. D., & Allahi, F. Supply chain disruption and mitigation strategies: insights from humanitarian operations in a complex environment. *International Journal of Logistics Research and Applications*. 2026. Iss. 29(7). P. 803–836. <https://doi.org/10.1080/13675567.2025.2490570>
13. NATO. Crisis management. 30.04.2025. URL: <https://www.nato.int/en/what-we-do/introduction-to-nato/crisis-management>
14. NATO. Euro-Atlantic Disaster Response Coordination Centre. 21.05.2025. URL: <https://www.nato.int/en/about-us/organization/nato-structure/euro-atlantic-disaster-response-coordination-centre--eadrcc/about-eadrcc>
15. NATO Centres of Excellence – Crisis Management and Disaster Response. 31.07.2024. URL: <https://www.act.nato.int/article/cmdr-coe-2024/>
16. CMDR COE. Open-door policy. URL: https://cmdrcoe.org/menu.php?m_id=1
17. CMDR COE. Crisis management and disaster response course (NATO approved; NATO ETOC CODE: ETE-CM-21784). URL: https://cmdrcoe.org/menu.php?m_id=2&c_id=7

References:

1. Lohvynenko, B.O., & Derevianko, K.V. (2025). Vzaiemodiia Natsionalnoi politzii ta Zbroinykh syl Ukrainy pid chas dii osoblyvoho pravovoho rezhymu voiennoho stanu [Interaction between the National Police and the Armed Forces of Ukraine during the special legal regime of martial law]. *Interaction between law enforcement agencies and public authorities to create a secure environment under martial law: collective monograph*. S. 254–272. <https://doi.org/10.30525/978-9934-26-589-1-13> [in Ukrainian].
2. Honchuk, A. A. (2026). Interaction of the Military Law Enforcement Service (Military Police) with the National Police and the SSU during stabilization operations in the “grey zone” and in de-occupied territories. *Aktualni pytannia rozvytku sektoru bezpeky i oborony (zarubizhnyi dosvid): zb. tez dop. uchastykiv KhKh-VII Mizhnarod. nauk.-prakt. konf. dlia zdob. osvity inozem. movamy (m. Vinnytsia, Ukraina, 3 kvit. 2026 r.) (Current issues of development of the security and defense sector (foreign experience): collection of abstracts of the participants of the XXVII International Scientific and Practical Conference for Education in Foreign Languages (Vinnytsia, Ukraine, April 3, 2026).)*. MVS Ukrainy, Kharkiv. nats. un-t vnut. sprav, Kaf. movn. pidhotovky. Vinnytsia: KhNUVS. S. 89–92. Retrieved from <https://dspace.univd.edu.ua/items/b505166e-d8c6-48d4-9611-77231902a232> [in Ukrainian].
3. Borovikova, V.S., Lozynska, I.V., Maistrenko, M.M., & Pavlyk, L.V. (2018). Diialnist politseiskoho shchodo vyjavlennia pravoporushen u hromadskykh mistsiakh: metodychni rekomendatsii [Police officer activities in detecting offenses in public places: methodological recommendations]. Lviv: LvDUVS, 76 s. [in Ukrainian].
4. Holub, V. A. (2022). Vzaiemodiia orhaniv Natsionalnoi politzii Ukrainy ta Derzhavnoi sluzhby Ukrainy z nadzvychainykh sytuatsii pid chas podii, poviazanykh iz pozhezhamy [Interaction between the National Police of Ukraine and the State Emergency Service of Ukraine during fire-related events]. *Problemy suchasnoi politseistyky : tezy dop. nauk.-prakt. konf. (m. Kharkiv, 20 kvit. 2022 r.) (Problems of modern police science: theses of the additional scientific-practical conference (Kharkiv, April 20, 2022).)*. MVS Ukrainy, Kharkiv. nats.

un-t vnut. sprav, F-t № 6, Kaf. pravookh. diialnosti ta politsiistyky, Nauk. park «Nauka ta bezpeka». Kharkiv. S. 238–241. Retrieved from <https://dspace.univd.edu.ua/items/621fe375-3d7f-4394-b99d-538b835263aa> [in Ukrainian].

5. Pylyp, V. (2024). Interaction between the National guard of Ukraine and civil society institutions. *Honor and Law*. Vol. 1 (88). P. 128–133. <https://doi.org/10.33405/2078-7480/2024/1/88/302284> [in English].

6. Danko, V. (2025). Theoretical principles of organizing cooperation between the National Guard of Ukraine and security sector institutions in ensuring public security. *The scientific journal of the National Academy of National Guard Honor and Law*, 3, 25–32. <https://doi.org/10.33405/2078-7480/2025/3/94/349219> [in English].

7. Chornopishchuk, I. (2023). Obgruntuvannia osnovnykh napriamkiv naukovykh doslidzhen shchodo dii prykordonnoho zahonu pid chas vykonannia zavdan u kryzovykh sytuatsiiakh voiennoho kharakteru [Substantiation of the main directions of scientific research on the actions of the border detachment during the performance of tasks in crisis situations of a military nature]. *Bezpeka derzhavy (State security)*, 1(1), 80–85. <https://doi.org/10.33405/2786-8613/2023/1/1/288279> [in Ukrainian].

8. Pozhueva, T., & Shchekhlovatykh, D. (2024). Tsyfrovi tekhnolohii v antykryzovomu upravlinni [Digital technologies in crisis management]. *Ekonomichnyi analiz*, 34(2), 407–420. <https://doi.org/10.35774/econa2024.02.407> [in Ukrainian].

9. Rybalko-Rak, L., Husakovska, T., & Opryshko, V. (2025). Tsyfrovizatsiia ta antykryzove upravlinnia: stratehichni zminy dlia rozvytku konkurentospromozhnoi ekosystemy [Digitalization and crisis management: Strategic changes for the development of a competitive ecosystem]. *Problemy ekonomiky*, 1, 223–229. <https://doi.org/10.32983/2222-0712-2025-1-223-229> [in Ukrainian].

10. OECD. (2024). Enhancing Crisis Management and Resilience in the Context of Armed Conflicts. Paris: OECD Publishing. ISBN 978-92-64-98765-4 Retrieved from https://www.oecd.org/content/dam/oecd/en/publications/reports/2013/08/oecd-risk-management_g17a2354/5k41rbd1l1zr7-en.pdf [in English].

11. Nazarenko, O., Holovan, O., & Rudynskyi, V. (2025). Assessment of Critical Infrastructure Vulnerability in Ukraine During Military Threats. *Bezpeka derzhavy*, 1(5), 73–82. Retrieved from <https://sts.nangu.edu.ua/article/download/336731/325342> [in English].

12. Maghsoudi, A., Falagara, Sigala I., Piotrowicz, W. D., & Allahi, F. (2026). Supply chain disruption and mitigation strategies: insights from humanitarian operations in a complex environment. *International Journal of Logistics Research and Applications*, 29(7), 803–836. <https://doi.org/10.1080/13675567.2025.2490570> [in English].

13. NATO. (2025). Crisis management. 30.04.2025. Retrieved from <https://www.nato.int/en/what-we-do/introduction-to-nato/crisis-management> [in English].

14. NATO. (2025). Euro-Atlantic Disaster Response Coordination Centre. 21.05.2025. Retrieved from <https://www.nato.int/en/about-us/organization/nato-structure/euro-atlantic-disaster-response-coordination-centre--eadrcc-/about-eadrcc> [in English].

15. NATO Centres of Excellence – Crisis Management and Disaster Response. 31.07.2024. Retrieved from <https://www.act.nato.int/article/cmdr-coe-2024/> [in English].

16. CMDR COE. Open-door policy. Retrieved from https://cmdrcoe.org/menu.php?m_id=1 [in English].

17. CMDR COE. Crisis management and disaster response course (NATO approved; NATO ETOC CODE: ETE-CM-21784). Retrieved from https://cmdrcoe.org/menu.php?m_id=2&c_id=7 [in English].

Дата першого надходження статті до видання: 31.07.2026
Дата прийняття статті до друку після рецензування: 04.09.2026
Дата публікації (оприлюднення) статті: 00.00.2026

УДК 340.12:17:004(100)

DOI <https://doi.org/10.32782/2311-8040/2026-2-6>**Лукашук Юрій Андрійович,**

старший викладач кафедри автоматизованих систем управління,
Національний університет «Львівська політехніка»,
вулиця Степана Бандери, 12, Львів, 79013, Україна
ORCID: <https://orcid.org/0000-0002-8933-8635>
Scopus ID: 57214080904

Цмоць Уляна Олексіївна,

старший науковий співробітник,
Львівський державний університет внутрішніх справ,
вулиця Городоцька, 26, м. Львів, 79000, Україна
ORCID: <https://orcid.org/0000-0002-8423-8272>
Scopus ID: 59410804600

ДИНАМІКА ПЕРЕОСМИСЛЕННЯ ПРАВОВИХ І МОРАЛЬНИХ ЦІННОСТЕЙ У КОНТЕКСТІ ЦИФРОВИХ ТРАНСФОРМАЦІЙ

Анотація. У статті здійснено комплексний міждисциплінарний аналіз динаміки переосмислення правових і моральних цінностей у контексті цифрових трансформацій сучасного суспільства. Досліджено соціально-філософські та правові наслідки впровадження алгоритмічних систем, штучного інтелекту, великих даних, VR/AR-середовищ і цифрових платформ як нових чинників нормативного регулювання соціальної поведінки. Обґрунтовано тезу про трансформацію алгоритму в автономний регулятор, що функціонує паралельно до традиційних механізмів права і моралі та часто вступає з ними у ціннісний конфлікт.

На основі показників цифрової активності населення України станом на 2025 рік проаналізовано вплив цифрового середовища на модифікацію поведінкових норм, соціальних практик і ціннісних орієнтацій громадян. Виявлено системні суперечності між формально правомірними алгоритмічними практиками та моральними оцінками суспільства, зокрема у сферах модерації контенту, обробки персональних даних, автоматизованого ухвалення рішень і соціального скорингу.

Особливу увагу приділено цифровізації кримінального процесу, використанню електронних доказів та алгоритмічного аналізу даних як чинникам трансформації уявлень про справедливість, відповідальність і презумпцію невинуватості. Розкрито правові й етичні проблеми VR/AR-середовищ, пов'язані з цифровим насильством, симуляцією шкоди та розмиванням меж юридичної відповідальності.

Запропоновано напрями гармонізації правових і моральних норм у цифрову епоху на засадах людиноцентризму, алгоритмічної прозорості, етичного дизайну, підзвітності цифрових систем і інтеграції етичних принципів у правове регулювання.

Доведено, що ефективне правове реагування на цифрові виклики потребує міждисциплінарної координації правових, етичних і технологічних підходів. Наголошено на необхідності адаптації національних правових систем до алгоритмічного регулювання з урахуванням міжнародних стандартів цифрової етики та прав людини.

Ключові слова: цифрова етика, штучний інтелект, цифрові цінності, алгоритмічна влада, VR/AR, цифрова приватність, правові норми, алгоритмічна справедливість.

Lukashchuk Yurii, Tsmots Uliana. DYNAMICS OF REINTERPRETING LEGAL AND MORAL VALUES IN THE CONTEXT OF DIGITAL TRANSFORMATIONS

Abstract. The article provides a comprehensive interdisciplinary analysis of the dynamics of rethinking legal and moral values in the context of digital transformations in modern society. It examines the socio-philosophical and legal consequences of the introduction of algorithmic systems, artificial intelligence, big data, VR/AR environments, and digital platforms as new factors in the normative regulation of social behavior. The thesis about the transformation of the algorithm into an autonomous regulator that functions in parallel with traditional mechanisms of law and morality and often enters into a value conflict with them is substantiated.

Based on indicators of the digital activity of the Ukrainian population as of 2025, the influence of the digital environment on the modification of behavioral norms, social practices, and value orientations of citizens is analyzed.

Systemic contradictions between formally legitimate algorithmic practices and moral assessments of society have been identified, particularly in the areas of content moderation, personal data processing, automated decision-making, and social scoring.

Particular attention is paid to the digitization of criminal proceedings, the use of electronic evidence, and algorithmic data analysis as factors transforming perceptions of justice, responsibility, and the presumption of innocence. The legal and ethical problems of VR/AR environments related to digital violence, simulation of harm, and blurring of the boundaries of legal responsibility are revealed.

Directions for harmonizing legal and moral norms in the digital age are proposed, based on human-centeredness, algorithmic transparency, ethical design, accountability of digital systems, and the integration of ethical principles into legal regulation.

It is proven that an effective legal response to digital challenges requires interdisciplinary coordination of legal, ethical, and technological approaches. The need to adapt national legal systems to algorithmic regulation, taking into account international standards of digital ethics and human rights, is emphasized.

Key words: digital ethics, artificial intelligence, digital values, algorithmic power, VR/AR, digital privacy, legal norms, algorithmic justice.

Вступ. Цифрова трансформація є системним процесом, що охоплює не лише технологічні, а й соціальні, правові, культурні та моральні виміри суспільного розвитку. Сучасна соціальна реальність формується в умовах стрімкого поширення інформаційних платформ, штучного інтелекту, алгоритмічних моделей ухвалення рішень, автономних цифрових агентів, сенсорних мереж і віртуальних середовищ. Унаслідок цього виникає потреба перегляду фундаментальних підходів до розуміння права і моралі як базових регуляторів суспільних відносин.

Штучний інтелект, машинне навчання, рекомендаційні системи та генеративні моделі створюють ситуацію, за якої традиційні механізми соціального контролю та нормативного регулювання втрачають монополію. Алгоритм дедалі частіше виступає новим регулятором поведінки, що функціонує на основі статистичних закономірностей і логіки оптимізації, часто поза межами моральної рефлексії та правової відповідальності [1; 2; 3].

У науковому дискурсі дедалі частіше обґрунтовується теза, що цифрове середовище перестає бути допоміжним інструментом і трансформується у базову реальність формування ідентичності, норм і цінностей. Інформаційні системи не лише опосередковують соціальні відносини, а й активно конструюють соціальний досвід, визначаючи доступ до інформації, рамки допустимого та моделі поведінки індивідів у цифровому просторі.

Для України ці процеси мають особливу актуальність. Високий рівень цифровізації, активне використання електронного урядування, соціальних мереж, месенджерів, цифрових фінансових сервісів і віртуальних платформ формують нові моделі соціальної поведінки. За даними міжнародного аналітичного звіту Digital 2025: Ukraine, понад 80 % населення України є активними користувачами інтернету, що свідчить про перехід цифрового середовища зі статусу додаткової сфери у статус основного простору реалізації соціальної, економічної та громадянської активності [4]. Такий рівень цифрової залученості означає, що саме у віртуальному просторі сьогодні формуються домінантні ціннісні орієнтації, моделі комунікації та уявлення про допустиме й недопустиме. Сучасні дослідження у сфері Управління штучним інтелектом наголошують, що ефективно управління штучним інтелектом потребує багаторівневої системи підзвітності, яка охоплює етапи проєктування, впровадження, моніторингу та аудиту алгоритмічних систем, а також участь державних органів, бізнесу й громадянського суспільства у процесах контролю та оцінювання ризиків [5; 6].

У цьому зв'язку актуалізується фундаментальна наукова проблема, що полягає у з'ясуванні того, яким чином процеси цифрової трансформації впливають на еволюцію правових і моральних цінностей суспільства, а також у визначенні спроможності традиційних нормативних систем забезпечувати належне та ефективне реагування на зазначені зміни. Ме-

тою статті є комплексний аналіз динаміки переосмислення правових і моральних норм у цифрову епоху та обґрунтування напрямів їх гармонізації.

Матеріали та методи. У дослідженні використано міждисциплінарний підхід, що поєднує інструменти філософії права, теорії моралі та правової науки для аналізу впливу цифрових технологій на трансформацію нормативних систем. Застосовано нормативно-ціннісний аналіз для виявлення суперечностей між правовими приписами, моральними оцінками та алгоритмічними практиками у цифровому середовищі. Порівняльно-правовий метод використано для зіставлення міжнародних етичних стандартів і національних підходів до регулювання штучного інтелекту, цифрової приватності та автоматизованих рішень. Елементи соціально-філософського та системного аналізу дали змогу розглянути алгоритмічні системи як автономний чинник соціального регулювання та джерело трансформації правових і моральних цінностей.

Результати. Право і мораль історично виступали основними регуляторами суспільної поведінки, визначаючи допустимі межі дій індивідів і соціальних груп [7]. Проте в умовах цифровізації формується новий тип регулятора – алгоритм, який діє на основі математичних моделей, статистичних кореляцій та автоматизованих рішень. Алгоритмічні системи, навіть за умови формальної законності, можуть породжувати упередженість, дискримінацію та несправедливість, що не завжди узгоджується з моральними уявленнями суспільства.

Цифрова трансформація правових і моральних регуляторів проявляється через кілька взаємопов'язаних процесів. Зокрема, відбувається ерозія традиційних моральних норм під впливом соціальних мереж і персоналізованих інформаційних стрічок, які формують так звані «моральні бульбашки» [1; 8; 9; 10]. Користувачі дедалі рідше стикаються з альтернативними поглядами, що сприяє поляризації та фрагментації ціннісних систем.

Водночас спостерігається автоматизація правового процесу. Інструменти на основі ШІ

застосовуються для аналізу цифрових слідів, прогнозування поведінки, оцінки ризиків і навіть ухвалення рішень у сфері правозастосування. Це змінює природу права, надаючи йому технократичного характеру та зменшуючи роль людського судження [2; 3; 11].

Особливо показовою є цифровізація кримінального процесу. У дослідженні Алрагад А.А. та ін. (2024) [11] доведено, що використання електронних доказів і алгоритмічного аналізу даних трансформує не лише процесуальні механізми, а й саму філософію кримінального правосуддя. Акцент зміщується з безпосередньої оцінки людських дій на аналіз цифрових репрезентацій поведінки, що створює ризики для принципів справедливості, змагальності та презумпції невинуватості. Алгоритмічна непрозорість у роботі з електронними доказами поглиблює розрив між формальною законністю та моральним відчуттям справедливості.

Окремим вектором цифрових змін є алгоритмічне опосередкування соціальних рішень, за якого автоматизовані системи визначають пріоритети, здійснюють оцінювання та впливають на розподіл соціальних ресурсів. Алгоритми автоматично ранжують контент, моделюють соціальний скоринг, впливають на доступ до ресурсів, працевлаштування чи фінансування [8; 9; 12; 13]. Такі рішення часто є непрозорими та недоступними для аудиту, що підриває довіру до правових інститутів.

Таким чином, алгоритм поступово перетворюється на автономне джерело нормотворення, яке функціонує паралельно до права і моралі, створюючи нові виклики для соціального порядку.

Цифрова етика формується як відповідь на зростаючий вплив інформаційних технологій на людське життя. Її теоретичною основою є концепція інфосфери, відповідно до якої інформаційна взаємодія стає ключовою формою соціальної реальності. Цифрове середовище розглядається не як інструмент, а як простір буття людини [14].

Серед ключових принципів цифрової етики виділяють прозорість алгоритмів, пояснюваність рішень, справедливість і недискримінацію, повагу до приватності, підзвітність роз-

робників та етичний дизайн. Ці принципи визнані міжнародною науковою та експертною спільнотою, зокрема закріплені в Рекомендації ЮНЕСКО з етики штучного інтелекту (UNESCO, 2021) [12] як базові для етичного використання ІІІ та цифрових систем.

Водночас на практиці цифрова етика часто має декларативний характер. Етичні рекомендації не завжди супроводжуються юридично зобов'язуючими механізмами реалізації, а відсутність ефективного контролю та моніторингу знижує їхню практичну дієвість. Це зумовлює необхідність інтеграції етичних принципів у правові норми та технічний дизайн цифрових систем.

Високий рівень цифрової активності населення України зумовлює глибокі соціальні трансформації. Масове використання інтернету, соціальних мереж, електронних сервісів і мобільних застосунків формує нові моделі комунікації, участі та соціальної взаємодії. Цифрове середовище стає основним простором реалізації економічних, політичних і громадянських відносин.

Алгоритми створюють персоналізовані інформаційні екосистеми, що суттєво відрізняються між собою. Це призводить до формування альтернативних систем цінностей, різного рівня інформованості та протилежних моральних суджень у межах однієї спільноти.

Дослідження цифровізації кримінального процесу підтверджує, що алгоритми набувають статусу де-факто нормотворчих суб'єктів. За висновками Алрагад А.А. та ін. (2024) автоматизовані системи аналізу електронних доказів впливають на перебіг кримінального провадження та судові переконання, виконуючи регулятивну функцію, яка раніше належала виключно людині.

VR/AR-технології породжують нові феномени – віртуальні домагання, симуляції насильства, маніпуляцію поведінкою через сенсорне занурення. Хоча такі дії відбуваються у віртуальному просторі, вони можуть мати реальні психоемоційні наслідки, що ставить під сумнів традиційні правові рамки [15; 16; 17].

Розвиток VR/AR-технологій формує принципово нові простори соціальної взаємодії,

у яких межа між віртуальним і реальним досвідом істотно розмивається. Симулятивний характер таких середовищ не усуває реальних психоемоційних наслідків для користувачів, зокрема у випадках віртуальних домагань, примусу, переслідування або насильницьких дій, що здійснюються через аватари та інтерактивні сценарії. Це актуалізує питання юридичної кваліфікації цифрового насильства у VR/AR-просторі та визначення механізмів правової відповідальності.

У чинних правових системах більшість VR/AR-інцидентів перебуває поза чітким нормативним регулюванням або розглядається крізь призму загальних норм інформаційного, цивільного та кримінального права. Зокрема, цивільно-правова відповідальність може наставати у випадках завдання моральної шкоди, порушення права на гідність, честь і недоторканність приватного життя. Водночас складність доведення причинно-наслідкового зв'язку між віртуальною дією та реальними наслідками значно ускладнює практичне застосування таких норм.

У площині кримінального права проблема полягає у відсутності чіткої прив'язки віртуальних дій до складів злочинів, сформульованих для фізичного світу. Хоча окремі прояви цифрового насильства можуть підпадати під ознаки переслідування, погроз або примушування, VR/AR-контекст створює додаткові труднощі, пов'язані з ідентифікацією суб'єкта, юрисдикцією та доказуванням умислу. Використання аватарів і анонімних профілів посилює ризик безкарності та знеособлення відповідальності.

Окрему роль у врегулюванні цифрового насильства відіграють платформні механізми відповідальності, зокрема внутрішні правила користування, модерація контенту, блокування акаунтів і алгоритмічне виявлення порушень. Однак такі інструменти мають обмежений правовий статус і не завжди відповідають принципам належної правової процедури, що породжує ризик свавільного або вибіркового застосування санкцій. Відсутність ефективних механізмів оскарження платформних рішень посилює недовіру

користувачів і не забезпечує повноцінного захисту їхніх прав.

У цьому контексті актуалізується необхідність розроблення спеціалізованих правових підходів до VR/AR-взаємодій, які б враховували: психоемоційний вплив віртуального досвіду; тілесну та просторову імітацію як юридично значущі фактори та особливості доказування цифрових інцидентів (лог-дані, сенсорні записи, поведінкові патерни).

Подальший розвиток метавсесвітів та інтегрованих VR/AR-платформ актуалізує необхідність формування нових підходів до правового регулювання цифрової взаємодії. У сучасних дослідженнях наголошується, що віртуальні середовища створюють складні виклики для забезпечення прав людини, захисту приватності, визначення юрисдикції та притягнення до відповідальності за цифрові правопорушення. Особливого значення набувають питання правового статусу віртуальних об'єктів, захисту користувачів від цифрового насильства та розроблення ефективних механізмів контролю за діяльністю платформ. За таких умов удосконалення нормативно-правового регулювання повинно поєднувати правові, етичні та технологічні інструменти забезпечення безпеки й справедливості у віртуальному просторі [18].

Перспективним є запровадження принципу підвищеної відповідальності щодо розробників і операторів VR/AR-платформ, які повинні забезпечувати превентивний етичний дизайн, інструменти персональної безпеки, прозорі процедури реагування на скарги та збереження цифрових доказів. Такий підхід узгоджується з концепцією вбудованої етики і дозволяє поєднати технічні, етичні та правові механізми захисту.

Отже, VR/AR-середовища вимагають переосмислення традиційних правових категорій шкоди, відповідальності та суб'єктності. Без інтеграції спеціальних правових норм і процесуальних гарантій цифрове насильство у віртуальних просторах ризикує залишатися в зоні морального засудження без ефективного юридичного реагування, що підриває довіру до права як універсального регулятора соціальних відносин у цифрову епоху.

Алгоритмічна упередженість є однією з ключових проблем сучасного ШІ [2; 21; 22]. Системи найму, кредитного скорингу та модерації контенту часто відтворюють соціальні стереотипи, маскуючи дискримінацію під технічну нейтральність. Це зумовлено як упередженими або нерепрезентативними даними, на яких навчаються моделі, так і вибором метрик та цілей оптимізації, що ігнорують соціальний контекст. Наслідками є посилення нерівностей, обмеження доступу до можливостей для вразливих груп та зниження довіри до цифрових рішень. Важливо розмежовувати алгоритмічну упередженість як технічну властивість моделей і алгоритмічну дискримінацію як її соціальний та правовий наслідок для конкретних груп населення, що проявляється у системному відтворенні історичних та інституційних нерівностей. Подолання алгоритмічної упередженості потребує поєднання технічних підходів (аудитів, дебіасингу, прозорості моделей) з етичним наглядом, механізмами підзвітності та міждисциплінарною відповідальністю розробників, інституцій і регуляторів.

Дані стають центральним ресурсом цифрової економіки. Водночас недостатня прозорість їх використання створює загрози приватності та сприяє розвитку «капіталізму стеження», що підриває довіру до цифрових платформ [9; 12]. Асиметрія інформації між користувачами та цифровими корпораціями призводить до формального характеру згоди на обробку персональних даних, яка часто не супроводжується реальним усвідомленням масштабів і наслідків цифрового спостереження. Масове збирання, агрегування та профілювання даних дозволяє формувати детальні поведінкові та психологічні портрети осіб, що створює ризики маніпуляції автономією вибору та порушення принципу інформаційного самовизначення. У правовому вимірі це актуалізує проблему адекватності традиційних механізмів захисту приватності, які не враховують алгоритмічну обробку даних у реальному часі. Відтак забезпечення ефективного захисту персональних даних потребує поєднання правових гарантій із етичними стандартами відповідального використання інформації та технічними інстру-

ментами контролю за цифровими процесами [9; 12; 15].

Крім того, концентрація масивів персональних даних у руках обмеженого кола приватних суб'єктів формує нові асиметрії влади, за яких контроль над інформацією перетворюється на інструмент соціального впливу та економічного домінування. Відсутність ефективних механізмів незалежного нагляду за обробкою даних посилює ризик зловживань, зокрема вторинного використання інформації поза первинними цілями її збору. За таких умов приватність втрачає статус фундаментальної цінності та дедалі частіше редукується до формального юридичного атрибуту, не здатного забезпечити реальний захист автономії особи в цифровому середовищі.

Процеси цифровізації спричиняють виникнення системних конфліктів між правовими нормами, моральними оцінками та алгоритмічним регулюванням соціальної поведінки. У цифровому середовищі дедалі частіше ви-

никають ситуації, коли дії, що є формально правомірними відповідно до чинного законодавства або умов користування цифровими платформами, викликають моральне неприйняття, соціальну тривогу або відчуття несправедливості.

Особливо показовим є використання алгоритмічних систем у сфері модерації контенту, обробки персональних даних, автоматизованого ухвалення рішень, а також у кримінальному процесі. Алгоритмічні рішення часто є непрозорими для користувачів і позбавленими механізмів ефективного оскарження, що підриває довіру до правових інститутів і цифрових платформ [8; 1; 9].

Узагальнення основних юридично-моральних конфліктів цифрової взаємодії подано в таблиці 1.

Як видно з таблиці 1, значна частина цифрових практик перебуває у «сірій зоні» між правом і мораллю. Особливо критичним є використання алгоритмічного аналізу елек-

Таблиця 1

Юридичні та моральні конфлікти цифрової взаємодії

Ситуація / феномен	Юридичний статус / характер	Моральні оцінки / соціальні реакції	Коментар / ризики
Алгоритмічна модерація контенту на цифрових платформах	Формально законна (умови користування, приватне регулювання)	Недовіра до непрозорих критеріїв, відчуття цензури	Ризик маніпуляції громадською думкою, обмеження свободи вираження [1; 8]
Використання персональних даних для таргетування, реклами та соціального скорингу	Легальне за формальної згоди користувача	Дискомфорт, страх тотального стеження	Порушення приватності, формування «капіталізму стеження» [9; 15]
Генеративні моделі, боти, автономні цифрові агенти	Недостатньо врегульовані	Невизначеність моральної відповідальності	Розмивання меж суб'єктності та відповідальності [19; 20]
Автоматизоване ухвалення рішень у сфері працевлаштування, кредитування, соціальних виплат	Часто правомірне відповідно до внутрішніх процедур	Підозра в упередженості та несправедливості	Алгоритмічна дискримінація, відсутність механізмів апеляції [20; 21]
VR/AR-симуляції насильства або домагань	Частково врегульовані або поза правовим полем	Етичне неприйняття, заперечення «нереальності» шкоди	Психологічна травматизація, потреба формування VR-етики [16; 17; 18]
Алгоритмічний аналіз електронних доказів у кримінальному процесі	Формально правомірний	Недовіра до «машинної» справедливості	Ризик порушення презумпції невинуватості, знеособлення відповідальності [11]

тронних доказів у кримінальному процесі. За результатами дослідження Алрагад А.А. та ін. [11], цифровізація роботи з доказами здатна змінювати баланс між ефективністю правосуддя та гарантіями прав людини, створюючи ризики для дотримання принципів справедливого суду, змагальності сторін і презумпції невинуватості.

Таким чином, юридично допустимі алгоритмічні практики дедалі частіше вступають у конфлікт із суспільними уявленнями про моральну справедливість, що свідчить про необхідність переосмислення нормативних засад цифрової взаємодії та інтеграції етичних критеріїв у правове регулювання.

Кібербулінг, діпфейк, цифрові маніпуляції та радикалізація змінюють моральні орієнтири суспільства, нормалізуючи агресію та порушення приватності.

Міжнародний досвід демонструє різні підходи до регулювання цифрових технологій. Для України актуальним є гібридний підхід, що поєднує міжнародні стандарти, національне законодавство та громадську участь [5; 6; 12; 19].

Пріоритетними напрямками гармонізації правових і моральних цінностей у сучасному суспільстві є людиноцентричний підхід, що ставить гідність, права та свободи людини в основу правового регулювання; етичний дизайн технологій і правових механізмів, який передбачає врахування моральних наслідків ще на етапі їх розроблення; активна громадська участь у формуванні, обговоренні та контролі нормативних рішень; підвищення рівня цифрової та правової грамотності населення з метою усвідомленого користування технологіями та захисту власних прав; а також постійна адаптація законодавства до цифрових викликів, зокрема пов'язаних із штучним інтелектом, обробкою персональних даних та автоматизованими рішеннями, з урахуванням етичних принципів справедливості, прозорості та відповідальності.

Висновки. Цифрова трансформація докорінно змінює фундаментальні уявлення про право, мораль і відповідальність, що підтверджується аналізом алгоритмічних систем як нових регуляторів соціальної поведінки. Алгоритмічні рішення, навіть за умов їх формальної законності, здатні породжувати стійкі моральні конфлікти, соціальну недовіру та відчуття несправедливості через відсутність прозорості, пояснюваності й чіткої юридичної підзвітності. Досвід цифровізації кримінального процесу показує, що застосування алгоритмічного аналізу електронних доказів без належних етичних і правових запобіжників створює ризики підриву принципів презумпції невинуватості, змагальності сторін і справедливого суду.

Гармонійний розвиток цифрового суспільства можливий лише за умови системної інтеграції правових і моральних цінностей у процеси розроблення, впровадження та використання цифрових технологій. Пріоритетними напрямками такої гармонізації мають стати людиноцентричний підхід, алгоритмічна прозорість і підзвітність, етичний дизайн технологій, а також міждисциплінарна координація правових, філософських і технологічних підходів з урахуванням міжнародних стандартів цифрової етики та прав людини.

Окрему загрозу становить тенденція до нормалізації алгоритмічного управління соціальними процесами, за якої технічна ефективність поступово підміняє собою етичну оцінку та правову легітимність рішень. Відсутність прозорості й пояснюваності алгоритмічних систем поглиблює розрив між формальною законністю цифрових практик і суспільним відчуттям справедливості, що підриває довіру до правових інститутів у цифровому середовищі. У цьому контексті подальший розвиток правового регулювання цифрових технологій має ґрунтуватися на міждисциплінарному діалозі, який поєднує правову доктрину, моральну філософію та принципи технологічної відповідальності.

Список використаних джерел:

1. Bucher T. If...Then: Algorithmic Power and Politics. Oxford University Press, 2018. <https://doi.org/10.1093/oso/9780190493028.001.0001>
2. Mittelstadt B. D. Principles alone cannot guarantee ethical AI. *Nature Machine Intelligence*. 2019. Vol. 1(11). P. 501–507. DOI: 10.1038/s42256-019-0114-4.
3. Pasquale F. The Black Box Society. Harvard University Press, 2015. ISBN 9780674970847 <https://www.hup.harvard.edu/books/9780674970847>
4. DataReportal. Digital 2025: Ukraine. 2025. URL: <https://datareportal.com/reports/digital-2025-ukraine>
5. Batool A., Zowghi D., Bano M. AI governance: a systematic literature review. *AI and Ethics*. 2025. Vol. 5. P. 3265–3279. DOI: 10.1007/s43681-024-00653-w.
6. Papagiannidis E, Mikalef P, Conboy K. Responsible Artificial Intelligence Governance: A Review and Research Framework. *Journal of Strategic Information Systems*. 2025. Vol. 34, Issue 2. Article 101885. doi:10.1016/j.jsis.2024.101885
7. Цмоць У.О. Співвідношення правових і моральних цінностей: компаративістський аналіз. Науковий вісник ЛьвДУВС. *Серія юридична*. 2025. № 3. С. 3–10. DOI: <https://doi.org/10.32782/2311-8040/2025-3-1>
8. Gillespie T. Custodians of the Internet. Yale University Press, 2018. <https://doi.org/10.12987/9780300235029>
9. Zuboff S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York : PublicAffairs, 2019. 704 p.
10. Sunstein C. R. #Republic: Divided Democracy in the Age of Social Media. Princeton : Princeton University Press, 2017. DOI: 10.1515/9781400884711.
11. Alraggad M. M., Almahasneh A. A. A. A., Borovikova V., Zhyvko Z., Komissarchuk Y. The policy of rethinking the criminal process in the national security system: The impact of digitalisation on working with electronic evidence. *Social and Legal Studies*. 2024. Vol. 7, No. 2. P. 162–170. DOI: 10.32518/sals2.2024.162.
12. UNESCO. Recommendation on the Ethics of Artificial Intelligence. Paris: United Nations Educational, Scientific and Cultural Organization, 2021. URL: <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics>
13. O’Neil C. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. New York : Crown, 2016.
14. Floridi L. The Fourth Revolution. Oxford University Press, 2014. <https://global.oup.com/academic/product/the-fourth-revolution-9780199606726?cc=ua&lang=en&>
15. Solove D. J. Understanding Privacy. Harvard University Press, 2008. <https://www.hup.harvard.edu/books/9780674035072> ISBN 9780674035072
16. Westerlund M. The Emergence of Deepfake Technology: A Review. *Technology Innovation Management Review*. 2019. Vol. 9(11). P. 39–52. DOI: 10.22215/timreview/1282
17. Madary M., Metzinger T. K. Real Virtuality: A Code of Ethical Conduct. Recommendations for Good Scientific Practice and the Consumers of VR-Technology. *Frontiers in Robotics and AI*. 2016. Vol. 3. Article 3. DOI: <https://doi.org/10.3389/frobt.2016.00003>
18. Freeman G., Zamanifard S., Maloney D., Acena D. Disturbing the Peace: Experiencing and Mitigating Emerging Harassment in Social Virtual Reality. *Proceedings of the ACM on Human-Computer Interaction*. 2022. Vol. 6 (CSCW2). DOI: <https://doi.org/10.1145/3555148>
19. Wang Y., Zhao X., Zhang Y. Ethical and Legal Challenges in the Metaverse: A Systematic Review. *Humanities and Social Sciences Communications*. 2024. Vol. 11. Article 437. DOI: 10.1057/s41599-024-02894-7.
20. Bostrom N. Superintelligence. Oxford University Press, 2014. ISBN: 9780199678112 <https://global.oup.com/academic/product/superintelligence-9780199678112?cc=ua&lang=en&>
21. Barocas S., Selbst A. D. Big Data’s Disparate Impact. *California Law Review*. 2016. Vol. 104, No. 3. P. 671–732.
22. Angwin J., Larson J., Mattu S., Kirchner L. Machine Bias. ProPublica. 2016. URL: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>

References:

1. Bucher, T. (2018). If...Then: Algorithmic Power and Politics. Oxford University Press. <https://doi.org/10.1093/oso/9780190493028.001.0001> [in English]
2. Mittelstadt, B. (2019). Principles Alone Cannot Guarantee Ethical AI. *Nature Machine Intelligence*. <https://doi.org/10.1038/s42256-019-0114-4> [in English]
3. Pasquale, F. (2015). The Black Box Society. Harvard University Press, ISBN 9780674970847. <https://www.hup.harvard.edu/books/9780674970847> [in English]

4. DataReportal. (2025). Digital 2025: Ukraine. Retrieved from <https://datareportal.com/reports/digital-2025-ukraine> [in English]
5. Batool, A., Zowghi, D., & Bano, M. (2025). AI governance: a systematic literature review. *AI and Ethics*, Vol. 5. P. 3265–3279. DOI: 10.1007/s43681-024-00653-w [in English].
6. Papagiannidis, E., Mikalef, P., & Conboy, K. (2025). Responsible artificial intelligence governance: A review and research framework. *Journal of Strategic Information Systems*, 34(2), Article 101885. <https://doi.org/10.1016/j.jsis.2024.101885> [in English].
7. Tsmots, U. O. (2025). Spivvidnoshennia pravovykh i moralnykh tsinnosti: komparatyvistskyi analiz [The relationship between legal and moral values: a comparative analysis]. *Naukovyi visnyk LvivDUVS. Seriya yurydychna – Scientific Bulletin of Lviv State University of Internal Affairs. Legal Series*, 3, 3–10. <https://doi.org/10.32782/2311-8040/2025-3-1> [in Ukrainian].
8. Gillespie, T. (2018). Custodians of the Internet. Yale University Press, 2018. <https://doi.org/10.12987/9780300235029> [in English].
9. Zuboff, S. (2019). The Age of Surveillance Capitalism. PublicAffairs, [in English]
10. Sunstein, C. R. (2017). #Republic: Divided Democracy in the Age of Social Media. Princeton : Princeton University Press. DOI: 10.1515/9781400884711 [in English].
11. Alraggad, M. M., Almahasneh, A. A. A. A., Borovikova, V., Zhyvko, Z., & Komissarchuk, Y. (2024). The policy of rethinking the criminal process in the national security system: The impact of digitalisation on working with electronic evidence. *Social and Legal Studies*, Vol. 7, No. 2. P. 162–170. DOI: 10.32518/sals2.2024.162 [in English].
12. UNESCO (2021). Recommendation on the Ethics of Artificial Intelligence. Paris: United Nations Educational, Scientific and Cultural Organization. URL: <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics> [in English].
13. O’Neil, C. (2016). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. New York : Crown [in English].
14. Floridi, L. (2014). The Fourth Revolution. Oxford University Press, <https://global.oup.com/academic/product/the-fourth-revolution-9780199606726?cc=ua&lang=en&> [in English].
15. Solove, D. J. (2008). Understanding Privacy. Harvard University Press. <https://www.hup.harvard.edu/books/9780674035072> ISBN 9780674035072 [in English].
16. Westerlund, M. (2019). The Emergence of Deepfake Technology: A Review. *Technology Innovation Management Review*, Vol. 9(11). P. 39–52. DOI: 10.22215/timreview/1282 [in English].
17. Madary, M., & Metzinger, T. K. (2016). Real Virtuality: A Code of Ethical Conduct. Recommendations for Good Scientific Practice and the Consumers of VR-Technology. *Frontiers in Robotics and AI*, Vol. 3. Article 3. DOI: <https://doi.org/10.3389/frobt.2016.00003> [in English].
18. Freeman, G., Zamanifard, S., Maloney, D., & Acena, D. (2022). Disturbing the Peace: Experiencing and Mitigating Emerging Harassment in Social Virtual Reality. *Proceedings of the ACM on Human-Computer Interaction*, Vol. 6 (CSCW2). DOI: <https://doi.org/10.1145/3555148> [in English].
19. Wang, Y., Zhao, X., & Zhang, Y. (2024). Ethical and Legal Challenges in the Metaverse: A Systematic Review. *Humanities and Social Sciences Communications*, Vol. 11. Article 437. DOI: 10.1057/s41599-024-02894-7 [in English].
20. Bostrom, N. (2014). Superintelligence. Oxford University Press. ISBN: 9780199678112. <https://global.oup.com/academic/product/superintelligence-9780199678112?cc=ua&lang=en&> [in English].
21. Barocas, S., & Selbst, A. D. (2016). Big Data’s Disparate Impact. *California Law Review*, Vol. 104, No. 3. P. 671–732 [in English].
22. Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). Machine Bias. ProPublica. URL: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> [in English].

Дата першого надходження статті до видання: 29.07.2026
Дата прийняття статті до друку після рецензування: 07.09.2026
Дата публікації (оприлюднення) статті: 00.00.2026

УДК 355.45:351.86(477)

DOI <https://doi.org/10.32782/2311-8040/2026-2-7>

Мовчан Анатолій Васильович,

доктор юридичних наук, професор,

професор кафедри оперативно-розшукової діяльності,

Львівський державний університет внутрішніх справ,

вулиця Городоцька, 26, Львів, 79000, Україна

ORCID: <https://orcid.org/0000-0002-6997-6517>

Scopus-Author ID: <https://www.scopus.com/authid/detail.uri?authorId=58689980100>

Researcher ID: <https://www.webofscience.com/wos/author/rid/AAJ-7771-2021>

МІЖВІДОМЧА ВЗАЄМОДІЯ СИЛ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ: СУТНІСТЬ, ПРОБЛЕМИ ТА НАПРЯМИ ВДОСКОНАЛЕННЯ

Анотація. У статті досліджено сутність та значення міжвідомчої взаємодії у діяльності сил сектору безпеки і оборони. Проаналізовано основні проблеми координації між суб'єктами безпекового середовища, визначено принципи ефективної взаємодії та окреслено сучасні інструменти її вдосконалення. Зазначається, що система суб'єктів міжвідомчої взаємодії є складною багаторівневою структурою. Її ефективність визначається рівнем координації, чіткістю розподілу повноважень та здатністю до інтеграції зусиль усіх учасників. Підкреслюється, що аналіз практики свідчить про наявність низки проблем реалізації міжвідомчої взаємодії, серед яких: відсутність єдиних механізмів координації, обмежений обмін інформацією, технічна несумісність систем, фрагментарність нормативно-правового регулювання та недостатній рівень підготовки персоналу.

Серед основних напрямів удосконалення взаємодії виділяється створення спільних ситуаційних центрів, впровадження інтегрованих інформаційних систем, проведення міжвідомчих навчань, стандартизація процедур діяльності та використання сучасних інформаційних технологій. Особливу увагу приділено міжнародному досвіду та можливостям його імплементації в Україні. Підкреслюється, що у країнах НАТО широко застосовується принцип взаємосумісності (interoperability), який передбачає здатність різних сил діяти в єдиному операційному середовищі. Її реалізація забезпечується через стандартизацію процедур, уніфікацію технічних рішень і спільну підготовку персоналу. Запропоновано практичні рекомендації щодо підвищення ефективності міжвідомчої співпраці.

Ключові слова: міжвідомча взаємодія, сектор безпеки і оборони, правоохоронні органи, координація, національна безпека, управління, інтеграція.

Movchan Anatolii. INTER-AGENCY INTERACTION OF FORCES IN THE SECURITY AND DEFENSE SECTOR: ESSENCE, PROBLEMS, AND DIRECTIONS FOR IMPROVEMENT

Abstract. The article examines the essence and significance of interagency interaction in the activities of the security and defense sector forces. The main problems of coordination between subjects of the security environment are analyzed, the principles of effective interaction are determined, and modern tools for its improvement are outlined. It is noted that the system of subjects of interagency interaction is a complex multi-level structure. Its effectiveness is determined by the level of coordination, the clarity of the distribution of powers, and the ability to integrate the efforts of all participants. It is emphasized that the analysis of practice indicates the presence of a number of problems in the implementation of interagency interaction, including: the lack of unified coordination mechanisms, limited information exchange, technical incompatibility of systems, fragmentation of regulatory and legal regulation, and insufficient level of personnel training.

Among the main areas of improving interaction, the creation of joint situational centers, the implementation of integrated information systems, conducting interdepartmental exercises, standardization of activity procedures, and the use of modern information technologies are highlighted. Particular attention is paid to international experience and the possibilities of its implementation in Ukraine. It is emphasized that the principle of interoperability, which implies the ability of different forces to operate in a single operational environment, is widely applied in NATO countries. Its implementation is ensured through the standardization of procedures, the unification of technical solutions, and joint training of personnel. Practical recommendations are proposed to improve the effectiveness of interagency cooperation.

Key words: *interagency cooperation, security and defense sector, law enforcement agencies, coordination, national security, management, integration*

Вступ. Сучасне безпекове середовище характеризується високим рівнем складності, гібридності та багатовимірності загроз. В умовах повномасштабної збройної агресії проти України особливої актуальності набуває формування якісно нового рівня організації діяльності сектору безпеки і оборони. За таких обставин визначальним чинником забезпечення національної безпеки є не лише інституційна спроможність окремих суб'єктів, а й ефективність їхньої взаємодії та координації. Саме міжвідомча взаємодія створює передумови для своєчасного реагування на загрози, раціонального використання наявних ресурсів і досягнення стратегічних цілей у сфері безпеки та оборони держави [1; 2].

Міжвідомча взаємодія являє собою сукупність організаційних, управлінських, комунікаційних та інформаційних заходів, спрямованих на узгодження діяльності суб'єктів сектору безпеки і оборони з метою досягнення спільних цілей і забезпечення належного рівня національної безпеки. Основними складовими такої взаємодії є своєчасний обмін інформацією, координація управлінських рішень, спільне планування заходів, а також чітке визначення функцій, повноважень і відповідальності кожного учасника процесу.

Питання міжвідомчої взаємодії у сфері безпеки і оборони розглядали у своїх працях О. М. Бандурка, А. В. Боровик, А. Г. Вархов, Д. О. Горбач, В. А. Денісенко, Н. З. Дерев'яно, О. В. Зайчук, В. Б. Звір, Д. П. Калаянов, Ю. Р. Кардашевський, О. Ф. Кобзар, А. Т. Комзюк, О. В. Кузьменко, І. О. Ліпко, Ю. М. Миколенко, Г. М. Сащук, Н. П. Свиридчук, В. І. Шкіндчук та інші науковці.

Зокрема, у статті «Модель досягнення взаємосумісності комунікаційних та інформаційних систем: запровадження досвіду НАТО в інтересах сил оборони держави» (2023) Ліпко І. О., Звір В. Б. та Миколенко Ю. М. запропонували модель досягнення взаємосумісності комунікаційних та інформаційних систем (КІС) ЗСУ на основі стандартів НАТО [3].

У статті «Еволюція стратегічних комунікацій сектору безпеки та оборони України як інструменту протидії інформаційним загрозам» (2025) Сащук Г. М. досліджує становлення й еволюцію стратегічних комунікацій (StratCom) сектору безпеки та оборони України з 2014 р. до 2025 р. як інструменту протидії інформаційним загрозам [4].

Разом із тим, стрімка трансформація безпекового середовища, цифровізація управління та активне входження України до євроатлантичного безпекового простору вимагають системного аналізу сучасних інструментів взаємодії з урахуванням концепції взаємосумісності (interoperability).

Метою статті є визначення сутності міжвідомчої взаємодії, аналіз основних проблем її реалізації та розроблення рекомендацій щодо підвищення ефективності функціонування сектору безпеки і оборони.

Матеріали та методи. Для досягнення поставленої мети визначено такі завдання: з'ясувати сутність, структуру та значення міжвідомчої взаємодії як елемента забезпечення національної безпеки; проаналізувати основні проблеми та деструктивні чинники, що стримують ефективну координацію між суб'єктами сектору безпеки і оборони (нормативні, інформаційні, технічні, організаційно-кадрові); визначити принципи та сучасні інструменти вдосконалення міжвідомчої співпраці, зокрема у частині створення спільних ситуаційних центрів та інтегрованих інформаційних систем; дослідити міжнародний досвід (зокрема концепцію interoperability у країнах НАТО) та окреслити шляхи його адаптації та імплементації в українську практику; сформулювати прикладні рекомендації щодо нормативно-правового, технічного та організаційного забезпечення міжвідомчої координації.

Для розв'язання поставлених завдань використано комплекс наукових методів: системний та структурно-функціональний (для аналізу сектору безпеки як цілісної багаторівневої системи); формально-догматичний

(для виявлення прогалин у нормативно-правовому регулюванні); порівняльно-правовий (для вивчення стандартів НАТО та концепції взаємосумісності); метод моделювання та проблемно-цільовий підхід (для розробки інструментів міжвідомчої координації та практичних рекомендацій).

Наукова новизна одержаних результатів полягає у системному обґрунтуванні концептуальних засад вдосконалення міжвідомчої взаємодії через інтеграцію трьох ключових компонентів: нормативно-процедурного (стандартизація процедур), технологічного (міжвідомчі ситуаційні центри та єдиний інформаційний простір) та кадрово-оперативного (спільні навчання за стандартами НАТО). Набули подальшого розвитку підходи щодо адаптації принципу взаємосумісності (interoperability) до національної системи управління в умовах сучасних гібридних та збройних загроз.

Практичне значення результатів. Сформульовані висновки та рекомендації можуть бути використані у нормотворчій діяльності при доопрацюванні законодавства у сфері національної безпеки і оборони, у практичній діяльності керівного складу суб'єктів сектору безпеки під час організації взаємодії та функціонування ситуаційних центрів, а також у освітньому процесі вищих навчальних закладів зі спеціальною формою навчання.

Результати. Система міжвідомчої взаємодії в Україні охоплює широкий спектр органів державної влади, військових формувань, правоохоронних органів та інших інституцій, діяльність яких спрямована на забезпечення національної безпеки і оборони держави. Її функціонування характеризується багаторівневістю та міжсекторальним характером, що зумовлює потребу в ефективній координації, узгодженості управлінських рішень і чіткому розподілі повноважень між усіма учасниками взаємодії.

Відповідно до чинної нормативно-правової бази та наукових підходів суб'єктів міжвідомчої взаємодії доцільно класифікувати за функціональним принципом, виходячи зі специфіки покладених на них завдань і ролі в системі забезпечення національної безпеки.

Ключове місце у структурі міжвідомчої взаємодії посідає військовий компонент, до складу якого входять Збройні Сили України, інші військові формування, утворені відповідно до законодавства, а також Сили територіальної оборони. Основним призначенням цих суб'єктів є забезпечення оборони держави, стримування та відсіч збройної агресії, захист суверенітету й територіальної цілісності України. У межах міжвідомчої взаємодії вони відіграють провідну роль у плануванні та проведенні оборонних операцій, координації спільних дій із правоохоронними органами, розвідувальними структурами та іншими складовими сектору безпеки і оборони під час реагування на кризові ситуації та загрози [1; 2].

Правоохоронний компонент представлений Національною поліцією України, Національною гвардією України та іншими органами, на які покладено виконання правоохоронних функцій. Їхня діяльність спрямована на забезпечення громадської безпеки і правопорядку, захист прав і свобод громадян, а також протидію злочинності. У межах міжвідомчої взаємодії зазначені суб'єкти забезпечують підтримання стабільності в тилкових районах, беруть участь у проведенні контрдиверсійних заходів, охороні критичної інфраструктури та взаємодіють із військовими формуваннями в умовах правового режиму воєнного стану [5].

До спеціальних та розвідувальних органів належать Служба безпеки України, розвідувальні органи держави, а також підрозділи, що здійснюють контррозвідувальну діяльність. Основними завданнями цих суб'єктів є виявлення, попередження та нейтралізація загроз державній безпеці, зокрема терористичних проявів, диверсійної діяльності, інформаційних операцій, кібератак та інших форм гібридного впливу [6].

Важливою складовою системи є органи цивільного захисту, насамперед Державна служба України з надзвичайних ситуацій. Їхня діяльність спрямована на реагування на надзвичайні ситуації природного, техногенного та воєнного характеру, ліквідацію їх наслідків, захист населення і територій, а також координацію гуманітарних та евакуаційних заходів [5].

Особливе місце в системі міжвідомчої взаємодії посідають органи державної влади та органи місцевого самоврядування, які забезпечують реалізацію державної політики у сфері національної безпеки й оборони, координацію діяльності суб'єктів безпеки на державному та регіональному рівнях, а також організаційне, фінансове й ресурсне забезпечення відповідних заходів [2; 7].

До допоміжних і партнерських суб'єктів належать підприємства оборонно-промислового комплексу, суб'єкти приватного сектору, зокрема у сфері кібербезпеки та інформаційних технологій, громадські об'єднання, волонтерські організації та міжнародні партнери України. Їхній внесок полягає у забезпеченні сектору безпеки і оборони сучасними технологіями, матеріально-технічними ресурсами, експертно-аналітичною підтримкою, а також у реалізації спільних програм і проєктів, спрямованих на зміцнення обороноздатності та стійкості держави [8].

Таким чином, система суб'єктів міжвідомчої взаємодії являє собою складну багаторівневу структуру, до складу якої входять органи державної влади, військові формування, правоохоронні органи, спеціальні служби, органи цивільного захисту, а також інші державні та недержавні інституції. Ефективність її функціонування значною мірою залежить від рівня координації діяльності, чіткості розмежування повноважень і відповідальності, а також здатності до консолідації ресурсів та зусиль усіх учасників [1; 2].

Водночас аналіз сучасної практики функціонування сектору безпеки і оборони України свідчить про наявність низки проблем, які негативно впливають на ефективність міжвідомчої взаємодії. Серед них слід виокремити недосконалість механізмів координації, обмеженість інформаційного обміну між окремими суб'єктами, технічну несумісність інформаційно-комунікаційних систем, фрагментарність нормативно-правового регулювання, а також недостатній рівень професійної підготовки персоналу до виконання спільних завдань в умовах кризових ситуацій.

У зв'язку з цим формування ефективної системи міжвідомчої взаємодії має ґрунтуватися на сукупності базових принципів, серед яких визначальними є єдність управління, оперативність і безперервність обміну інформацією, чіткий розподіл повноважень та відповідальності, сумісність організаційних процедур і технологій, а також взаємна довіра між усіма учасниками процесу [3; 9].

Серед пріоритетних напрямів удосконалення міжвідомчої взаємодії доцільно виокремити розвиток спільних ситуаційних та координаційних центрів, впровадження інтегрованих інформаційно-аналітичних систем, проведення регулярних міжвідомчих навчань і тренувань, стандартизацію процедур планування та реагування, а також активне використання сучасних цифрових технологій і засобів захищеного обміну інформацією [3; 7].

Міжнародний досвід переконливо свідчить, що ефективна міжвідомча взаємодія є одним із визначальних чинників забезпечення національної безпеки та стійкості держави до сучасних викликів і загроз. У країнах – членах НАТО важливе значення надається принципу взаємосумісності (interoperability), який передбачає здатність різних сил, структур та органів діяти в єдиному операційному середовищі, використовуючи узгоджені процедури, стандарти та засоби комунікації [10].

Важливим інструментом розвитку міжвідомчої взаємодії в країнах НАТО є проведення багатонаціональних навчань, зокрема Steadfast Defender, Trident Juncture та Sea Breeze. Під час таких заходів відпрацьовуються механізми координації дій між військовими формуваннями, правоохоронними органами, розвідувальними структурами та органами цивільного захисту, що сприяє підвищенню рівня оперативної готовності до реагування на кризові ситуації та надзвичайні події різного характеру [11].

У державах Європейського Союзу сформовано розвинену систему інтегрованого управління кризами (Integrated Crisis Response), яка забезпечує комплексний підхід до реагування на надзвичайні ситуації та загрози безпеці. Одним із ключових елементів цієї системи є

механізм Integrated Political Crisis Response (IPCR), що забезпечує координацію дій між інституціями ЄС та державами-членами під час кризових ситуацій. Його функціонування сприяє оперативному обміну інформацією, узгодженню політичних рішень і мобілізації необхідних ресурсів для подолання кризових явищ [12].

Показовим прикладом ефективної міжвідомчої співпраці є діяльність агентства Frontex, яке координує взаємодію прикордонних служб держав-членів ЄС. У межах його функціонування впроваджено єдині інформаційні системи, спільні операції та стандартизовані процедури реагування на транскордонні загрози, що забезпечує високий рівень узгодженості дій усіх учасників процесу [13].

У Сполучених Штатах Америки ефективна міжвідомча взаємодія реалізується через систему National Incident Management System (NIMS) та діяльність Department of Homeland Security (DHS). Зазначена система забезпечує координацію між федеральними, штатними та місцевими органами влади, а також суб'єктами приватного сектору під час реагування на надзвичайні ситуації та кризові події [14].

Особливу увагу в американській практиці приділено діяльності так званих fusion centers – міжвідомчих аналітичних центрів, які забезпечують інтеграцію та аналіз інформації, отриманої від правоохоронних органів, розвідувальних служб, кібербезпекових структур та інших суб'єктів безпеки [15].

Узагальнення міжнародного досвіду дає підстави стверджувати, що ключовими передумовами ефективної міжвідомчої взаємодії є наявність єдиної системи координації, стандартизованих процедур діяльності, сучасних інформаційних технологій, високого рівня професійної підготовки персоналу та розвинутої культури міжвідомчого співробітництва. Використання зазначених підходів є важливим для подальшого вдосконалення системи безпеки і оборони України та підвищення її стійкості в умовах сучасних загроз.

Досвід Ізраїлю також заслуговує на увагу. У цій країні ефективна взаємодія забезпечується через тісну координацію між армією,

розвідувальними службами та поліцією. Значна увага приділяється оперативному обміну інформацією та швидкому прийняттю рішень у режимі реального часу [16].

З урахуванням результатів проведеного аналізу та сучасних викликів у сфері національної безпеки доцільно запропонувати комплекс практичних заходів, спрямованих на підвищення ефективності міжвідомчої взаємодії суб'єктів сектору безпеки і оборони України.

1. Формування єдиної міжвідомчої інформаційної системи. Одним із пріоритетних напрямів удосконалення міжвідомчої взаємодії є створення інтегрованої цифрової платформи, яка забезпечуватиме оперативний обмін інформацією між усіма суб'єктами сектору безпеки і оборони в режимі реального часу. Така система має передбачати використання уніфікованих форматів даних, захищених каналів зв'язку, механізмів диференційованого доступу до інформаційних ресурсів, а також інструментів аналітичної обробки та узагальнення даних.

Важливим кроком у цьому напрямі стало затвердження Кабінетом Міністрів України постановою від 13 листопада 2025 р. № 1471 Порядку взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки та кіберзагрози із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними та розвідувальними органами, а також суб'єктами оперативно-розшукової діяльності [17].

2. Удосконалення нормативно-правового забезпечення. Необхідною умовою підвищення ефективності міжвідомчої взаємодії є системне вдосконалення нормативно-правової бази, що регулює діяльність суб'єктів сектору безпеки і оборони. Це передбачає чітке розмежування їхніх повноважень, нормативне закріплення механізмів координації, визначення процедур обміну інформацією та усунення наявних правових колізій і дублювання функцій.

Важливим інструментом реалізації зазначених завдань є Дорожня карта взаємосумісності, схвалена Комітетом сектору безпеки і оборони Ради Україна–НАТО 17 червня 2024 року та представлена під час Вашингтонського са-

міту НАТО у липні 2024 року [6]. Документ визначає основні напрями досягнення взаємосумісності між українськими структурами безпеки та оборони і відповідними інституціями держав – членів НАТО.

3. *Забезпечення технічної та процедурної сумісності.* Ефективна міжвідомча взаємодія неможлива без належного рівня технічної та процедурної сумісності. У зв'язку з цим актуальним є впровадження єдиних стандартів зв'язку та обміну даними, модернізація існуючих інформаційно-комунікаційних систем, інтеграція відомчих ІТ-рішень у спільний інформаційний простір, а також стандартизація алгоритмів дій і процедур реагування в кризових ситуаціях [18].

4. *Розвиток системи підготовки та підвищення кваліфікації кадрів.* Людський фактор залишається одним із ключових чинників забезпечення ефективної міжвідомчої взаємодії. У зв'язку з цим особливої актуальності набуває створення системи безперервної професійної підготовки та підвищення кваліфікації персоналу суб'єктів сектору безпеки і оборони. Доцільним є впровадження міжвідомчих освітніх програм, проведення регулярних спільних тренувань і навчань, розвиток навичок командної роботи, а також формування лідерських компетентностей у сфері кризового менеджменту та стратегічного управління [19].

5. *Розвиток інституційних механізмів координації.* Важливим напрямом удосконалення міжвідомчої взаємодії є розвиток інституційних механізмів координації діяльності суб'єктів сектору безпеки і оборони. З цією метою доцільно створювати або вдосконалювати діяльність постійно діючих координаційних структур, зокрема міжвідомчих ситуаційних центрів, спільних оперативних штабів та аналітичних центрів типу *fusion centers* [20].

6. *Впровадження сучасних інформаційних технологій.* Цифрова трансформація сектору безпеки і оборони є одним із визначальних чинників підвищення ефективності міжвідомчої взаємодії. Перспективними напрямами розвитку є використання систем штучного інтелекту для аналізу та прогнозування загроз,

впровадження технологій Big Data для обробки великих масивів інформації, застосування геоінформаційних систем (GIS) для підтримки управлінських рішень, а також посилення кіберзахисту інформаційних ресурсів та критичної інформаційної інфраструктури [21].

7. *Формування культури міжвідомчої співпраці.* Не менш важливою умовою ефективної взаємодії є розвиток організаційної культури, заснованої на принципах партнерства, довіри та спільної відповідальності за досягнення стратегічних цілей. Це передбачає подолання відомчої ізольованості, стимулювання обміну досвідом і кращими практиками, розвиток горизонтальних комунікацій, а також утвердження принципів відкритості, взаємної підтримки та професійної солідарності [22].

8. *Розширення міжнародного співробітництва.* Важливим чинником удосконалення міжвідомчої взаємодії є активізація міжнародного співробітництва у сфері безпеки та оборони. Поглиблення співпраці з міжнародними партнерами створює можливості для запозичення передового досвіду, участі у спільних навчаннях і тренуваннях, отримання технічної, експертної та консультативної допомоги, а також забезпечення поступової інтеграції України до європейських та євроатлантичних безпекових структур [23].

Висновки. На основі проведеного дослідження сутності, проблем та перспектив розвитку міжвідомчої взаємодії сил сектору безпеки і оборони України сформульовано такі висновки та прикладні рекомендації:

– з'ясовано, що міжвідомча взаємодія у сфері національної безпеки є складною багаторівневою функціонально-організаційною системою, ефективність якої визначається рівнем координації, чіткістю розподілу повноважень та здатністю суб'єктів безпекового середовища до інтеграції зусиль у єдиному операційному середовищі;

– аналіз практики довів, що основними бар'єрами на шляху до ефективної координації є: *нормативна фрагментарність* – відсутність єдиного уніфікованого нормативно-правового акта, який би чітко регламентував порядок та алгоритми міжвідомчої співпраці

в умовах критичних ситуацій; *інформаційні та технічні бар'єри* – відомча замкненість, відсутність захищених каналів автоматизованого обміну даними у режимі реального часу та технічна несумісність спеціальних засобів зв'язку; *кадрові та процедурні відмінності* – брак спільних тренувань за єдиними стандартами та різноманітність внутрішньовідомчих регламентів прийняття рішень;

обґрунтовано, що базовим орієнтиром для вдосконалення вітчизняної системи координації має слугувати євроатлантичний принцип взаємосумісності (interoperability), який передбачає досягнення триєдиної сумісності: *оперативної* (спільні процедури й алгоритми дій), *технічної* (єдині стандарти зв'язку та передачі даних) та *доктринально-організаційної* (спільне розуміння завдань та єдина культура управління).

З метою розв'язання виявлених проблем та підвищення стійкості сектору безпеки і оборони пропонується комплекс заходів за трьома основними напрямками:

1) *нормативно-правове та процедурне забезпечення*: ініціювати розробку та затвердження на рівні Кабінету Міністрів України уніфікованого Порядку міжвідомчої взаємодії суб'єктів сектору безпеки і оборони під час реагування на критичні загрози; запровадити розробку та постійне оновлення Спільних стандартних операційних процедур (Joint SOPs) для типових кризових сценаріїв (кібератаки, диверсійно-розвідувальні загрози, надзвичайні ситуації техногенного чи військового характеру);

2) *технологічна та інформаційна інтеграція*: прискорити розбудову та інтеграцію Головного ситуаційного центру України із ситуаційними центрами органів військового управління, СБУ, Національної поліції, ДПСУ та ДСНС на основі хмарних технологій та захищеного протоколу передачі даних; запровадити міжвідомчі аналітичні осередки (fusion centers) для акумуляції, аналізу та поширення розвідувальної й оперативної інформації між суб'єктами реагування у режимі 24/7; забезпечити перехід на єдині стандарти шифрування, цифрового захищеного зв'язку та обміну даними, сумісні з протоколами НАТО (STANAG);

3) *кадрове та оперативне забезпечення*: включити до навчальних програм закладів вищої освіти зі специфічними умовами навчання обов'язкові спільні командно-штабні навчання та практичні тренінги з опрацювання міжвідомчих зв'язків; запровадити практику короткострокового стажування офіцерів зв'язку та аналітиків у ситуаційних центрах суміжних відомств для подолання відомчих бар'єрів та підвищення рівня взаємної довіри.

Конфлікт інтересів: Мовчан А. є членом редакційної колегії журналу. Для забезпечення незалежності редакційного процесу рукопис розглядався редактором, який не мав конфлікту інтересів з автором. Автор не брав участі у відборі рецензентів, процесі рецензування та прийнятті рішення щодо публікації статті. Рукопис пройшов стандартну процедуру подвійного сліпого рецензування.

Список використаних джерел:

1. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.
2. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України від 14.09.2020 № 392/2020. *Урядовий кур'єр*. 2020. 16 вер. (№ 179).
3. Ліпко І., Звір В., Миколенко Ю. Модель досягнення взаємосумісності комунікаційних та інформаційних систем: запровадження досвіду НАТО в інтересах сил оборони держави. *Збірник наукових праць Центру воєнно-стратегічних досліджень НВУОУ*. 2023. № 2. С. 108–120. DOI: <https://doi.org/10.33099/2304-2745/2023-2-78/108-120>.
4. Сашук Г. М. Еволюція стратегічних комунікацій сектору безпеки та оборони України як інструменту протидії інформаційним загрозам. *Політичне життя*. 2025. № 3. С. 103–108. DOI: <https://doi.org/10.31558/2519-2949.2025.3.13>.
5. Дорожня карта взаємосумісності з НАТО. *Офіційний сайт Міністерства внутрішніх справ України*. URL: <https://mvs.gov.ua/jevroatlanticna-integraciia/doroznia-karta-vzajemsumisnosti-z-nato>

6. Денісенко В. А. Взаємодія Служби безпеки України з іншими суб'єктами сектору безпеки і оборони: адміністративно-правові проблеми координації. *Правові новели*. 2025. № 27. С. 218–226. DOI: <https://doi.org/10.32782/ln.2025.27.26>.
7. Боровик А. В., Вархов А. Г., Дерев'янка Н. З. Адміністративно-правовий механізм взаємодії суб'єктів сектору безпеки й оборони щодо забезпечення національної безпеки: питання теорії та практики : монографія. Одеса : Юридика, 2024. 186 с.
8. Комзюк А. Т., Шкіндюк В. І. Поняття взаємодії та координації у сфері правоохоронної діяльності як об'єкту адміністративно-правового регулювання. *Вісник кримінологічної асоціації України*. 2025. № 1 (34). С. 863–872. DOI: <https://doi.org/10.32631/vca.2025.1.72>.
9. NATO-Ukraine Action Plan // North Atlantic Treaty Organization : official website. 2002. Nov. 22. URL: <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2002/11/22/nato-ukraine-action-plan?selectedLocale=uk>
10. NATO Interoperability Standards: Enabling Seamless Coalition Operations Through Cross-Enterprise Orchestration. URL: <https://r4.ai/nato-interoperability-standards-coalition-operations/>
11. NATO Begins Exercise STEADFAST DETERRENCE 2026: Securing the High North, Reinforcing Transatlantic Collaboration on Collective Defence. Joint Warfare Centre : official website. 2026. URL: <https://www.jwc.nato.int/article/steadfast-deterrence-2026-begins/>
12. EU integrated political crisis response (IPCR) arrangements. EUR-Lex : Access to European Union law. URL: <https://eur-lex.europa.eu/EN/legal-content/summary/eu-integrated-political-crisis-response-ipcr-arrangements.html>
13. Frontex: Irregular border crossings into the EU down 40% in the first four months of 2026. Frontex : official website. 2026. URL: <https://www.frontex.europa.eu/media-centre/news/news-release/frontex-irregular-border-crossings-into-the-eu-down-40-in-the-first-four-months-of-2026-MwZAin>
14. National Incident Management System and Incident Command System. Division of Homeland Security and Emergency Services : official website of New York State. URL: <https://www.dhses.ny.gov/national-incident-management-system-and-incident-command-system>
15. Свиридчук Н. П., Кардашевський Ю. Р. Ф'южн-центри як важливий компонент моделі Intelligence-led Policing (ILP). *Аналітично-порівняльне правознавство*. 2023. № 6. С. 504–509. DOI: <https://doi.org/10.24144/2788-6018.2023.06.87>.
16. Матвієнко Ю. Приклад для України: Як в Ізраїлі реформують розвідувальні та спеціальні служби. *Defence Express*. URL: https://defence-ua.com/weapon_and_tech/jak_v_izrajili_reformujut_rozviduvalni_ta_spetsialni_sluzhbi-5668.html
17. Уряд затвердив Порядок взаємодії суб'єктів національної системи реагування на кіберінциденти та правоохоронних органів. *Голос України*. 2025. 17 листоп. URL: <https://www.golos.com.ua/article/388473>
18. Закон про електронні комунікації: парламент закріпив нові стандарти якості мобільного зв'язку. Український центр аналітики та досліджень UCAI. URL: <https://ucaai.com.ua/solutions/3225-zakon-pro-elektronn-komunkac-parlament-zakrpiv-nov-standarti-yakost-moblnogo-zvyazku>
19. Спінко С. Людський фактор: як зробити персонал запорукою успіху компанії. *Delo.ua*. URL: <https://delo.ua/business/lyudskii-faktor-yak-zrobiti-personal-faktorom-uspixu-kompaniyi-436071/>
20. Про рішення Ради національної безпеки і оборони України від 4 червня 2021 року «Щодо удосконалення мережі ситуаційних центрів та цифрової трансформації сфери національної безпеки і оборони» : Указ Президента України від 18.06.2021 № 260/2021. Рада національної безпеки і оборони України : офіційний вебсайт. URL: <https://www.rnbo.gov.ua/ua/Ukazy/4916.html>
21. Структура цифрової трансформації у Силах оборони: як це працює та як долучитися. Офіційний сайт Міністерства оборони України. URL: <https://mod.gov.ua/explanation/it-vertikal-u-silah-oboroni-yak-cze-praczuje-ta-yak-doluchitsya>
22. Шимановська-Діанич Л. М. Розвиток організаційної культури як важливий фактор забезпечення основної конкурентної переваги компанії. *Актуальні проблеми інноваційної економіки та права*. 2023. № 1–2. С. 71–76. DOI: <https://doi.org/10.36887/2524-0455-2023-1-12>.
23. Співпраця з міжнародними організаціями: можливості та перспективи. Народний комітет України. URL: <https://nku.com.ua/spivpracya-z-mizhnarodnymy-organizacziyamy-mozhlyvosti-ta-perspektyvy/>

References:

1. Verkhovna Rada of Ukraine. (2018). *Pro natsionalnu bezpeku Ukrainy* [On the national security of Ukraine] (Law of Ukraine No. 2469-VIII). *Vidomosti Verkhovnoi Rady*, (31), Art. 241. [in Ukrainian].

2. President of Ukraine. (2020, September 14). *Stratehiia natsionalnoi bezpeky Ukrainy* [National security strategy of Ukraine] (Decree No. 392/2020). *Uryadovyy Kurier*, (179). [in Ukrainian].
3. Lipko, I., Zvir, V., & Mykolenko, Yu. (2023). Model dosiahnennia vzaiemosumisnosti komunikatsiinykh ta informatsiinykh system: zaprovadzhennia dosvidu NATO v interesakh syl oborony derzhavy [Model for achieving interoperability of communication and information systems: Implementation of NATO experience in the interests of the state defense forces]. *Zbirnyk naukovykh prats Tsentru voienno-stratehichnykh doslidzhen NUOU*, (2), 108–120. <https://doi.org/10.33099/2304-2745/2023-2-78/108-120> [in Ukrainian].
4. Sashchuk, H. M. (2025). Evoliutsiia stratehichnykh komunikatsii sektoru bezpeky ta oborony Ukrainy yak instrumentu protydyi informatsiynym zahrozam [Evolution of strategic communications of the security and defense sector of Ukraine as a tool for countering information threats]. *Politychne Zhyttia*, (3), 103–108. <https://doi.org/10.31558/2519-2949.2025.3.13> [in Ukrainian].
5. Ministry of Internal Affairs of Ukraine. (n.d.). *Dorozhnia karta vzaiemosumisnosti z NATO* [Roadmap for interoperability with NATO]. <https://mvs.gov.ua/jevroatlantica-integraciia/dorozhnia-karta-vzajemosumisnosti-z-nato> [in Ukrainian].
6. Denysenko, V. A. (2025). Vzaiemodii Sluzhby bezpeky Ukrainy z inshymy subiektamy sektoru bezpeky i oborony: administratyvno-pravovi mekhanizmy koordynatsii [Interaction of the Security Service of Ukraine with other actors of the security and defense sector: Administrative and legal problems of coordination]. *Pravovi Novely*, (27), 218–226. <https://doi.org/10.32782/ln.2025.27.26> [in Ukrainian].
7. Borovyk, A. V., Varkhov, A. H., & Derevianko, N. Z. (2024). *Administratyvno-pravovyi mekhanizm vzaiemodii subiektiv sektoru bezpeky i oborony shchodo zabezpechennia natsionalnoi bezpeky: pytannia teorii ta praktyky* [Administrative and legal mechanism of interaction between actors of the security and defense sector in ensuring national security: Theory and practice] (Monograph). Yurydyka. [in Ukrainian].
8. Komziuk, A. T., & Shkindiuk, V. I. (2025). Poniattia vzaiemodii ta koordynatsii u sferi pravookhoronnoi diialnosti yak obiekta administratyvno-pravovoho rehuliuвання [Concept of interaction and coordination in law enforcement as an object of administrative legal regulation]. *Visnyk Kryminolohichnoi Asotsiatsii Ukrainy*, (1), 863–872. <https://doi.org/10.32631/vca.2025.1.72> [in Ukrainian].
9. North Atlantic Treaty Organization. (2002, November 22). *NATO-Ukraine action plan*. <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2002/11/22/nato-ukraine-action-plan?selectedLocale=uk> [in English].
10. R4 AI. (n.d.). *NATO interoperability standards: Enabling seamless coalition operations through cross-enterprise orchestration*. <https://r4.ai/nato-interoperability-standards-coalition-operations/> [in English].
11. Joint Warfare Centre. (2026). *NATO begins exercise STEADFAST DETERRENCE 2026: Securing the High North, reinforcing transatlantic collaboration on collective defence*. North Atlantic Treaty Organization. <https://www.jwc.nato.int/article/steadfast-deterrence-2026-begins/> [in English].
12. EUR-Lex. (n.d.). *EU integrated political crisis response (IPCR) arrangements*. Access to European Union Law. <https://eur-lex.europa.eu/EN/legal-content/summary/eu-integrated-political-crisis-response-ipcr-arrangements.html> [in English].
13. Frontex. (2026). *Frontex: Irregular border crossings into the EU down 40% in the first four months of 2026*. European Border and Coast Guard Agency. <https://www.frontex.europa.eu/media-centre/news/news-release/frontex-irregular-border-crossings-into-the-eu-down-40-in-the-first-four-months-of-2026-MwZAin> [in English].
14. New York State Division of Homeland Security and Emergency Services. (n.d.). *National incident management system and incident command system*. <https://www.dhses.ny.gov/national-incident-management-system-and-incident-command-system> [in English].
15. Svyrydiuk, N. P., & Kardashevskiy, Yu. R. (2023). Fiuzhn-tsentry yak vazhlyvyi komponent modeli Intelligence-Led Policing (ILP) [Fusion centers as an important component of the Intelligence-led Policing (ILP) model]. *Analitychno-Porivnialne Pravo Navstvo*, (6), 504–509. <https://doi.org/10.24144/2788-6018.2023.06.87> [in Ukrainian].
16. Matviyenko, Yu. (n.d.). *Pryklad dlia Ukrainy: Yak v Izraili reformuiut rozviduvalni ta spetsialni sluzhby* [An example for Ukraine: How intelligence and special services are reformed in Israel]. Defence Express. https://defence-ua.com/weapon_and_tech/jak_v_izrajili_reformujut_rozviduvalni_ta_spetsialni_sluzhbi-5668.html [in Ukrainian].
17. Uryad zatverdyv Poryadok vzayemodii subiektiv natsionalnoyi systemy reahuvannya na kiberintsydynty ta pravookhoronnykh organiv [The Government approved the Procedure for interaction between subjects of the national cyber incident response system and law enforcement agencies]. (2025, November 17). *Holos Ukrainy*. <https://www.golos.com.ua/article/388473> [in Ukrainian].

18. Ukrainian Center for Analytics and Research (UCAI). (n.d.). *Zakon pro elektronni komunikatsii: parlament zakrypyv novi standarty yakosti mobilnoho zviazku* [Law on electronic communications: Parliament consolidated new standards for mobile service quality]. <https://ucaai.com.ua/solutions/3225-zakon-pro-elektronn-komunkac-parlament-zakrpiv-nov-standarti-yakost-moblno-go-zvyazku> [in Ukrainian].
19. Spinko, S. (n.d.). *Liudskyi faktor: yak zrobyty personal Zaporukoiu uspihu kompanii* [The human factor: How to make staff the key to company success]. Delo.ua. <https://delo.ua/business/lyudskii-faktor-yak-zrobiti-personal-faktorom-uspiku-kompaniyi-436071/> [in Ukrainian].
20. President of Ukraine. (2021, June 18). *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 4 chervnia 2021 roku «Shchodo udoskonalennia merezhi situatsiinykh tsentriv ta tsyfrovoy transformatsii sfery natsionalnoi bezpeky i oborony»* [On the decision of the National Security and Defense Council of Ukraine dated June 4, 2021 «On improving the network of situation centers and digital transformation of the national security and defense sphere»] (Decree No. 260/2021). National Security and Defense Council of Ukraine. <https://www.rnbo.gov.ua/ua/Ukazy/4916.html> [in Ukrainian].
21. Ministry of Defence of Ukraine. (n.d.). *Struktura tsyfrovoy transformatsii u Sylakh oborony: yak tse pratsiue ta yak doluchytysia* [Structure of digital transformation in the Defense Forces: How it works and how to join]. <https://mod.gov.ua/explanation/it-vertikal-u-silah-oboroni-yak-cze-praczyuye-ta-yak-doluchitysia> [in Ukrainian].
22. Shymanovska-Dianych, L. M. (2023). Rozvytok mekhanizmu organizatsinoi kultury yak vazhlyvyi faktor zabezpechennia osnovnoi konkurentnoi perevahy kompanii [Development of organizational culture as an important factor in ensuring the main competitive advantage of the company]. *Aktualni Problemy Innovatsijnoi Ekonomiky Ta Prava*, (1–2), 71–76. <https://doi.org/10.36887/2524-0455-2023-1-12> [in Ukrainian].
23. People's Committee of Ukraine (NKU). (n.d.). *Spivpratsia z mizhnarodnymy mekhanizmy: mozhlyvosti ta perspektyvy* [Cooperation with international organizations: Opportunities and prospects]. <https://nku.com.ua/spivpracza-z-mizhnarodnymy-organizaciyamy-mozhlyvosti-ta-perspektyvy/> [in Ukrainian].

Creative Commons Attribution 4.0
International (CC BY 4.0)



Дата першого надходження статті до видання: 24.07.2026
Дата прийняття статті до друку після рецензування: 03.09.2026
Дата публікації (оприлюднення) статті: 00.00.2026

УДК 351.74:341.24:343.431

DOI <https://doi.org/10.32782/2311-8040/2026-2-8>

Панасюк Олександр Петрович,

кандидат історичних наук, доцент,
здобувач освітнього рівня «магістр»
спеціальності К9 Правоохоронна діяльність,
Запорізький національний університет,
вулиця Університетська, 66, Запоріжжя, 69011, Україна
ORCID: <https://orcid.org/0000-0002-9871-3441>
Scopus-Author ID: 60006155900
Researcher ID: MCJ-5862-2025

ОРГАНІЗАЦІЙНО-ТАКТИЧНІ ЗАСАДИ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ПЛАТФОРМ ІНТЕРПОЛУ ТА ЄВРОПОЛУ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ ЩОДО ПРОТИДІЇ ПОСЯГАННЯМ НА ВОЛЮ ОСОБИ

Анотація. У статті проаналізовано організаційно-тактичні засади використання інформаційних платформ Міжнародної організації кримінальної поліції (Інтерполу) та Агентства Європейського Союзу зі співробітництва правоохоронних органів (Європолу) у діяльності правоохоронних органів щодо протидії посяганням на волю особи – незаконному позбавленню волі, викраденню людини, захопленню заручників, торгівлі людьми та суміжним кримінальним правопорушенням. Розкрито інституційно-правовий статус зазначених міжнародних інституцій, охарактеризовано інформаційні ресурси: мережу I-24/7, систему міжнародних повідомлень (notices) та розсилок (diffusions) Інтерполу, а також Інформаційну систему Європолу (EIS), мережу безпечного обміну інформацією SIENA. Визначено нормативну основу участі України у зазначеній співпраці, зокрема діяльність Національного центрального бюро Інтерполу в Україні та підрозділу Національної поліції з питань взаємодії з Європолом. На основі узагальнення практики реалізації спільних оперативних та аналітичних проєктів (SPRING, OSCAR, спільна слідча група в межах операції «Гольф») обґрунтовано організаційно-тактичні форми використання зазначених платформ: обмін оперативною інформацією через офіцерів зв'язку, участь у спільних слідчих групах, аналітичну підтримку розслідувань, транскордонний розшук осіб, зниклих безвісти. Виявлено проблемні аспекти застосування отриманої через Інтерпол та Європол інформації у кримінальному провадженні, ризики політизації міжнародного розшуку та необхідність посилення гарантій захисту персональних даних. Наголошено на необхідності гармонізації національного законодавства про захист персональних даних з правом Європейського Союзу та інтеграції Єдиного реєстру осіб, зниклих безвісти за особливих обставин, з інформаційними ресурсами Інтерполу. Окреслено перспективи подальших досліджень, пов'язаних із процесуальним статусом інформації, отриманої в порядку міжнародного поліцейського співробітництва.

Ключові слова: Інтерпол, Європол, інформаційні платформи, посягання на волю особи, обмін інформацією.

Panasiuk Oleksandr. ORGANIZATIONAL AND TACTICAL FOUNDATIONS FOR THE USE OF INTERPOL AND EUROPOL INFORMATION PLATFORMS IN LAW ENFORCEMENT ACTI- VITY TO COUNTER ENCROACHMENTS ON PERSONAL LIBERTY

Abstract. The article analyzes the organizational and tactical foundations for using the information platforms of the International Criminal Police Organization (Interpol) and the European Union Agency for Law Enforcement Cooperation (Europol) in law enforcement activities to counter encroachments on personal liberty – unlawful deprivation of liberty, human kidnapping, hostage-taking, human trafficking, and related criminal offenses. The institutional and legal status of these international bodies is revealed, and their information resources are characterized: Interpol's I-24/7 network, the system of international notices and diffusions, as well as Europol's Information System (EIS) and the Secure Information Exchange Network Application (SIENA). The regulatory framework for Ukraine's participation in this cooperation is defined, particularly the activities of the National Central Bureau of Interpol in Ukraine and the National Police unit responsible for interaction with Europol. Based on a synthesis of practice in implementing joint operational and analytical projects (SPRING, OSCAR, joint investigation team within Operation "Golf"), the organizational and tactical forms of using these platforms are substantiated: exchange of operational information via liaison officers, participation in joint investigation teams, analytical

support for investigations, and cross-border search for missing persons. Problematic aspects of using information obtained through Interpol and Europol in criminal proceedings are identified, alongside the risks of politicization of international search and the need to strengthen personal data protection guarantees. The necessity of harmonizing national legislation on personal data protection with European Union law and integrating the Unified Register of Persons Missing under Special Circumstances with Interpol's information resources is emphasized. Prospects for further research related to the procedural status of information obtained through international police cooperation are outlined.

Key words: *Interpol, Europol, information platforms, encroachments on personal liberty, information exchange.*

Вступ. Права і свободи людини, зокрема її недоторканність та особиста свобода, є найвищою соціальною цінністю, захист яких є фундаментальним обов'язком демократичної держави. У сучасних умовах глобалізації, стрімкого розвитку інформаційно-комунікаційних технологій та інтенсифікації транскордонної міграції відбувається трансформація злочинності. Посягання на волю особи дедалі частіше набувають транснаціонального характеру, високого рівня адаптивності та супроводжуються використанням цифрових інструментів і складних мережових структур. Повномасштабна збройна агресія Російської Федерації проти України кардинально змінила криміногенне середовище та спричинила наймасштабнішу міграційну кризу в Європі. Це суттєво посилює ризики експлуатації вразливих категорій громадян, масового вимушеного переміщення та вчинення злочинів проти волі особи, зокрема: незаконного позбавлення волі або викрадення людини (ст. 146 КК України), насильницького зникнення (ст. 146-1 КК України), захоплення заручників (ст. 147 КК України) та торгівлі людьми (ст. 149 КК України).

Висока мобільність злочинних угруповань та юрисдикційні обмеження національних правоохоронних органів унеможливають швидке ефективне виявлення, припинення й розслідування таких правопорушень виключно внутрішньодержавними засобами. Зазначене зумовлює критичну необхідність активного залучення потенціалу міжнародного поліцейського співробітництва. Інституційно-технологічною основою для координації цих зусиль та оперативного обміну даними виступають інформаційні платформи Інтерполу та Європолу, дослідження організаційно-тактичних засад яких є пріоритетним напрямом для сучасної правоохоронної науки та практики.

Проблематика міжнародного співробітництва в межах Інтерполу та Європолу перебуває у полі уваги вітчизняної юридичної науки. Інституційно-правовий статус Європолу як Агентства Європейського Союзу зі співробітництва правоохоронних органів, генезу його нормативно-правового регулювання від Конвенції про заснування Європейського поліцейського офісу 1995 р. до Регламенту (ЄС) 2016/794 дослідив С. Переполькін [1]. Функціональні можливості Інтерполу як інструмента протидії злочинності, зокрема у сфері розшуку осіб, зниклих безвісти, розкрито М. Тома [2]. О. Горах та А. Громович здійснили порівняльний аналіз мандатів та інструментів Інтерполу й Європолу, зокрема дослідили проблеми процесуального використання отриманої інформації та ризики політизації [3]. Особливості практичної взаємодії Європолу з Україною, зокрема на конкретних прикладах оперативної співпраці, висвітлено Є. Моїсєвою, М. Латишевою та К. Шалупнею [4]. Загальну систему міжнародних інституцій, залучених до протидії злочинності, – Інтерполу, Європолу, Євроюсту, Асепанополу, Африполу, Америполу, – охарактеризовано О. Вороняниковим [5]. Питання міжнародного співробітництва правоохоронних органів у протидії злочинам проти волі, честі та гідності особи розглянули В. Філашкін та А. Антошук [6]. Водночас, як засвідчує аналіз наукових праць, питання співвідношення мандатів, інструментів та практичної ефективності Інтерполу й Європолу залишається дискусійним. Поряд із цим організаційно-тактичні аспекти застосування інформаційних платформ цих організацій у сфері протидії посяганням на волю особи все ще не отримали самостійного комплексного висвітлення, що й зумовлює актуальність цього дослідження.

Метою статті є визначення організаційно-тактичних засад використання інформаційних платформ Інтерполу та Європолу в діяльності правоохоронних органів України щодо протидії посяганням на волю особи.

Матеріали та методи. Нормативну основу дослідження становлять Статут Міжнародної організації кримінальної поліції – Інтерпол, Регламент (ЄС) 2016/794 Європейського Парламенту та Ради від 11 травня 2016 р. про Агентство Європейського Союзу зі співробітництва правоохоронних органів (Європол) [7], Угода між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво від 14 грудня 2016 р. [8], постанови Кабінету Міністрів України від 30.09.1992 № 555 «Про вступ України до Інтерполу» [9] та від 25.03.1993 № 220 «Про Національне центральне бюро Інтерполу» [10], Указ Президента України від 06.08.2004 № 872 «Про представника Національного центрального бюро Інтерполу України у Міжнародній організації кримінальної поліції – Інтерпол» [11], спільний наказ Міністерства внутрішніх справ України, Офісу Генерального прокурора, Національного антикорупційного бюро України, Служби безпеки України, Державного бюро розслідувань, Міністерства фінансів України, Міністерства юстиції України від 17.08.2020 № 613/380/93/228/414/510/2801/5 «Про затвердження Інструкції про порядок використання правоохоронними органами України інформаційної системи Міжнародної організації кримінальної поліції – Інтерпол» [12], Положення про Національну поліцію, затверджене постановою Кабінету Міністрів України від 28.10.2015 № 877 [13], наказ Міністерства внутрішніх справ України від 29.08.2022 № 535 «Про затвердження Порядку ведення Єдиного реєстру осіб, зниклих безвісти за особливих обставин» [14], Кримінальний кодекс України, зокрема ст. 146-149 [15], Протокол про попередження і припинення торгівлі людьми, особливо жінками і дітьми, і покарання за неї 2000 р. [16] та Конвенція Ради Європи про заходи щодо протидії торгівлі людьми 2005 р. [17].

Методологічну основу дослідження становить діалектичний метод пізнання правових явищ у їх розвитку та взаємозв'язку. Системно-структурний метод застосовано для аналізу інституційної побудови Інтерполу та Європолу як суб'єктів міжнародної поліцейської кооперації. Формально-юридичний (догматичний) метод використано для тлумачення положень Регламенту (ЄС) 2016/794, Статуту Інтерполу та національних нормативно-правових актів. Порівняльно-правовий метод дозволив зіставити глобальний мандат Інтерполу з регіональною спеціалізацією Європолу. Метод узагальнення правозастосовної практики застосовано для аналізу конкретних прикладів використання інформаційних платформ у розслідуванні злочинів проти волі особи. Функціональний метод використано для визначення тактичних форм застосування зазначених платформ у правоохоронній діяльності.

Під час підготовки статті автор використовував інструмент штучного інтелекту (мовну модель Gemini від Google) виключно з метою граматичної коректури, стилістичного редагування українського тексту, перекладу англійською мовою. Інструменти штучного інтелекту не застосовувалися для генерації наукових ідей, формулювання концептуальних висновків чи аналізу первинних джерел. Автор особисто перевіряв і відредагував увесь матеріал.

Результати. Аналіз кримінально-правової характеристики та практики протидії посяганням на волю особи свідчить, що в сучасних умовах ці злочини володіють високим ступенем транснаціоналізації та латентності. Їх специфіка як об'єкта міжнародної поліцейської кооперації зумовлена складною транскордонною структурою злочинної діяльності, коли підготовка, вербування, транзит та безпосередня експлуатація потерпілих охоплюють декілька державних юрисдикцій. В умовах повномасштабної агресії РФ проти України зазначені ризики трансформувалися внаслідок виникнення масових міграційних потоків, вимушеного переміщення цивільного населення та появи нових форм посягань, зокрема насильницьких зникнень і депортацій. Зазначені чинники визначають зміщення

акцентів у реалізації міжнародно-правових стандартів, закріплених у Протоколі про попередження і припинення торгівлі людьми, що доповнює Конвенцію ООН проти транснаціональної організованої злочинності [16], та Конвенції Ради Європи про заходи щодо протидії торгівлі людьми [17], з класичних процедур міжнародної правової допомоги на оперативно-інформаційну взаємодію правоохоронних органів у режимі реального часу.

Базовим елементом глобальної інфраструктури обміну поліцейською інформацією є телекомунікаційна мережа Інтерполу I-24/7, доступ до якої в Україні забезпечується через Департамент міжнародного поліцейського співробітництва Національної поліції України як робочий орган НЦБ Інтерполу. Ключовими інструментами міжнародного розшуку та обліку в системі організації є міжнародні сповіщення (notices) та циркулярні розсилки (diffusions). На відміну від сповіщень, розсилки спрямовуються Національним центральним бюро безпосередньо до органів-партнерів у конкретних країнах, минаючи попереднє опрацювання в Генеральному секретаріаті, однак так само вимагають суворого дотримання Статуту Інтерполу та Правил обробки даних [3; 4]. У системі протидії злочинам проти волі особи спеціалізованим інструментом є «жовте сповіщення» (Yellow Notice) – міжнародний запит про розшук зниклих безвісти осіб, а також ідентифікацію осіб, які не можуть повідомити відомості про себе внаслідок безпорадного стану чи віку. Автоматизована інтеграція даних Yellow Notice з інструментами прикордонного контролю дає змогу виявляти факти транскордонного переміщення потерпілих у режимі реального часу. Ефективність розшукового мандату Інтерполу в цій сфері забезпечується поєднанням кримінального обліку, інформаційного супроводу розшукових заходів національних органів та аналітичного підтримки розслідувань [2, с. 351].

Сформована в Україні нормативна база забезпечує централізовану модель взаємодії з Інтерполом та Європолом через Департамент міжнародного поліцейського співробітництва Нацполіції [12; 13]. Разом з тим, організацій-

но-тактичний аналіз цієї моделі вказує на її централізовано-бюрократичний характер: міжвідомча Інструкція [12] передбачає багаторівневу процедуру погодження запитів від інших правоохоронних суб'єктів (СБУ, ДБР, НАБУ), що в умовах протидії транснаціональним посяганням на волю особи призводить до втрати тактичного часу. У напрямі протидії торгівлі людьми Україна долучилася до проєкту I-Force, у межах якого відбувається навчання українських правоохоронців сучасним методикам розслідування цієї категорії злочинів [18].

Правовий статус Європолу як Агентства Європейського Союзу зі співробітництва правоохоронних органів визначено Регламентом (ЄС) 2016/794, який замінив Рішення Ради ЄС № 2009/371/ПВС і остаточно перетворив міжурядову організацію, засновану Конвенцією 1995 р., на агентство Європейського Союзу [1]. Компетенція Європолу охоплює понад сорок тяжких форм злочинності, серед яких безпосередньо названо викрадення людини, незаконне позбавлення волі і захоплення заручника, а також торгівлю людьми та незаконну торгівлю людськими органами і тканинами [1, с. 172]. Із метою збору, зберігання, обробки, аналізу та обміну інформацією, зокрема оперативними даними про злочинність, Європол використовує декілька взаємопов'язаних інструментів: Інформаційну систему Європолу (Europol Information System, EIS), яка дає змогу зберігати, шукати, візуалізувати та пов'язувати різні види інформації про транснаціональні злочини; мережу безпечного обміну інформацією SIENA (Secure Information Exchange Network Application), призначену для захищеної передачі даних між державами-членами; цілодобовий операційний центр, у якому здійснюється перехресна перевірка кримінальної інформації з різних джерел і країн; а також аналітичну підтримку, яку забезпечують понад сто кримінальних аналітиків Європолу. За узагальненими даними Є. Моїсєєвої, М. Латишевої та К. Шалупні Європол щороку супроводжує понад 12 000 справ, пов'язаних із тяжкими злочинами та тероризмом [4, с. 715].

Взаємодія України з Європолом здійснюється на основі Угоди між Україною та

Європейським поліцейським офісом про оперативне та стратегічне співробітництво від 14 грудня 2016 р., яка набрала чинності 17 серпня 2017 р. і замінила попередню Угоду про стратегічне співробітництво від 4 грудня 2009 р. [3, с. 273]. Координація здійснюється через офіцерів зв'язку, прикріплених до штаб-квартири Європолу в Гаазі, а національним контактним пунктом визначено підрозділ Національної поліції України з питань взаємодії з Європолом. До кола компетентних органів, відповідальних за виконання Угоди, віднесено, зокрема, Національну поліцію України, Службу безпеки України, Державну прикордонну службу України, Національне антикорупційне бюро України та інші органи [3, с. 274].

Узагальнення правозастосовної практики дає змогу виокремити декілька організаційно-тактичних форм використання розглянутих інформаційних платформ у протидії посяганням на волю особи. По-перше, це створення спільних слідчих груп за участю Європолу та Євроюсту: приклад – операція «Гольф», у межах якої партнерство прокуратури й поліції Румунії, Центру торгівлі людьми Великої Британії, Європолу та Євроюсту дало змогу викрити організовану злочинну мережу та засудити її учасників за торгівлю дітьми з метою кримінальної експлуатації [4, с. 716]. По-друге, це створення спеціалізованих оперативних платформ обміну інформацією в реальному часі: після повномасштабного вторгнення було створено віртуальний командний пункт SPRING для полегшення оперативного обміну даними щодо протидії торгівлі людьми між Україною, Румунією, Австрією, Угорщиною, Німеччиною, Словаччиною, Молдовою та Польщею, а також тимчасову робочу групу з питань торгівлі людьми для обговорення оперативних питань на ранній стадії у взаємодії з перевіреними неурядовими організаціями [4, с. 717]. По-третє, це аналітична підтримка розслідувань через профільні аналітичні проекти, зокрема операцію OSCAR, спрямовану на перехресну перевірку санкційних списків Європейського Союзу з наявними оперативними даними та виявлення зв'язків з організованою злочинністю. По-четверте, це вико-

ристання розшукових інструментів Інтерполу, передусім жовтої картки, для транскордонного розшуку осіб, зниклих безвісти, у поєднанні з функціонуванням національного Єдиного реєстру осіб, зниклих безвісти за особливих обставин, ведення якого регламентовано наказом Міністерства внутрішніх справ України від 29.08.2022 № 535 [14].

Попри розвинений інструментарій, практика застосування інформаційних платформ Інтерполу й Європолу супроводжується низкою проблемних питань, передусім у площині чіткого розмежування поліцейського та кримінального процесуального співробітництва. Інформація, отримана оперативними каналами (повідомлення / notices, розсилки / diffusions Інтерполу, дані систем EIS та SIENA Європолу), має статус орієнтувальної (оперативно-розшукової) і не є безпосереднім доказом у розумінні ст. 84 Кримінального процесуального кодексу України. Для надання їй процесуального значення та використання в доказуванні необхідна її легалізація через процедури міжнародної правової допомоги (Розділ IX КПК України) шляхом направлення відповідних запитів. Непослідовність у розумінні цього розмежування нерідко призводить до процесуальних помилок під час оцінки допустимості доказів у кримінальному провадженні. Поряд із цим актуальними залишаються ризики політизації міжнародного розшуку та питання забезпечення гарантій захисту прав людини [3, с. 137]. У науковій літературі висловлюється думка, що Європол доцільніше визначати як агентство з обробки інформації, а не як орган поліції у власному значенні цього слова, оскільки посадові особи Європолу під час виконання своїх завдань не мають права застосовувати примусові заходи [1, с. 273]. Зокрема, відомий європейський дослідник правоохоронної співпраці С. Файнаут наголошує на тому, що держави-члени ЄС свідомо обмежують Європол аналітичними функціями задля збереження власного суверенітету у сфері безпеки [19]. У свою чергу, К. Бласі Казагран класифікує це агентство як глобальний «інформаційний хаб» (information hub), діяльність якого передусім зосереджена на зборі та

перехресній перевірці масивів кримінальних даних [20]. Такий підхід повністю корелює із позицією самого керівництва Агентства; як зазначав колишній директор Європолу Р. Вейнрайт, за своєю сутнісною природою ця структура є саме інституцією з обробки інформації [21]. Це зумовлює необхідність чіткого розмежування інформаційно-аналітичної функції зазначених платформ і оперативно-розшукових повноважень національних правоохоронних органів, які залишаються виключними суб'єктами застосування примусу. Крім того, ефективність міжнародного обміну персональними даними прямо залежить від гармонізації національного законодавства про захист персональних даних із відповідним правом Європейського Союзу. На це орієнтовані, зокрема, зобов'язання України в межах переговорного процесу щодо вступу до ЄС, передусім за Розділом 24 «Юстиція, свобода та безпека». Наразі цей процес перебуває на етапі активної реформації. Попри те, що до чинного Закону України «Про захист персональних даних» 2010 року продовжують вноситися окремі процедурні зміни (зокрема, щодо повноважень органів фінансового контролю згідно із Законом № 4240-IX), сама національна система захисту інформації все ще визнається застарілою. Повноцінна інтеграція європейських стандартів очікується лише після ухвалення фундаментального законопроекту № 8153, покликаного імплементувати регламент GDPR та розв'язати питання створення незалежного наглядового органу [22]. Окремим напрямом інтенсифікації міжнародного співробітництва є інтеграція Єдиного реєстру осіб, зниклих безвісти за особливих обставин, із телекомунікаційними системами Інтерполу. Така цифрова взаємодія забезпечить автоматизоване генерування міжнародних запитів (зокрема, «жовтих сповіщень») щодо розшуку неповнолітніх та інших вразливих категорій осіб, які стали жертвами насильницького зникнення чи інших посягань на особисту свободу

Висновки. Організаційно-тактичні засади використання інформаційних платформ Інтерполу та Європолу в протидії посяганням на волю особи ґрунтуються на трирівневій нор-

мативній основі: установчих та спеціальних актах цих міжнародних організацій (Статут Інтерполу, Регламент (ЄС) 2016/794 з урахуванням змін, внесених Регламентом (ЄС) 2022/991, Директива (ЄС) 2024/1712 щодо протидії торгівлі людьми), міжнародних договорів України (зокрема, Угоді про оперативне та стратегічне співробітництво з Європолом) та національному законодавстві, яке визначає повноваження Департаменту міжнародного поліцейського співробітництва Національної поліції України (як НЦБ Інтерполу та Національного контактного пункту Європолу).

Інституційною складовою цих засад є функціонування зазначеного контактного пункту та мережі офіцерів зв'язку, які забезпечують безпосередній доступ українських правоохоронних органів до інформаційних ресурсів обох організацій – захищеної телекомунікаційної мережі I-24/7 Інтерполу, з одного боку, та Інформаційної системи Європолу (EIS), захищеної мережі SIENA і Цілодобового операційного центру – з іншого.

Тактичний вимір застосування зазначених платформ у протидії злочинам проти волі особи охоплює такі ключові напрями: інформаційне забезпечення участі у спільних слідчих групах (JITs); функціонування спеціалізованих оперативних платформ обміну даними в реальному часі (зокрема, у межах мультидисциплінарної платформи EMPACT); аналітичну підтримку розслідувань у межах цільових оперативних проєктів (зокрема, аналітичного проєкту Європолу «Phoenix»); транскордонний розшук осіб, зниклих безвісти, із використанням системи міжнародних сповіщень Інтерполу (зокрема, «жовтих сповіщень»). Практика реалізації цих напрямів підтверджує їх результативність у сфері протидії торгівлі людьми та суміжним кримінальним правопорушенням.

Разом з тим ефективність розглянутого напрямку міжнародного поліцейського співробітництва обмежується невизначеністю кримінального процесуального статусу відомостей, отриманих каналами Інтерполу та Європолу (зокрема, у контексті оцінки їх допустимості як доказів), ризиками політизації міжнародно-

го розшуку з боку окремих держав, а також незавершеним етапом гармонізації національного законодавства про захист персональних даних із правом Європейського Союзу (стандартами GDPR та Директиви (ЄС) 2016/680 для правоохоронного сектору).

Перспективними напрямками подальших наукових розвідок є обґрунтування процесу-

ального порядку адаптації, легалізації та використання як доказів відомостей, одержаних у межах міжнародного поліцейського співробітництва, а також розроблення юридичних та технічних протоколів взаємодії Єдиного реєстру осіб, зниклих безвісти за особливих обставин, з інформаційними системами Інтерполу та Європолу.

Список використаних джерел:

1. Перепьолкін С. М. Правовий статус агентства Європейського Союзу зі співробітництва правоохоронних органів (Європол). *Аналітично-порівняльне правознавство*. 2021. № 3. С. 270–275. DOI: <https://doi.org/10.24144/2788-6018.2021.03.50>
2. Тома М. Г. Інтерпол як інструмент протидії злочинності. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. Вип. 87, т. 3. DOI: <https://doi.org/10.24144/2307-3322.2025.87.3.53>
3. Гораш О. С., Громович А. А. Інтерпол і Європол як ключові суб'єкти міжнародної поліцейської кооперації в системі протидії транснаціональній організованій злочинності. *Вісник Кримінологічної асоціації України*. 2025. Т. 36, № 3. С. 136–146. DOI: <https://doi.org/10.32631/vsa.2025.3.10>
4. Моїсєєва Є. О., Латишева М. О., Шалупня К. С. Діяльність Європолу та співпраця з Україною. *Юридичний науковий електронний журнал*. 2023. № 4. С. 714–718. DOI: <https://doi.org/10.32782/2524-0374/2023-4/173>
5. Воронянников О. О. Діяльність міжнародних установ та організацій у боротьбі зі злочинністю. *Аналітично-порівняльне правознавство*. 2025. № 1. С. 876–880. DOI: <https://doi.org/10.24144/2788-6018.2025.01.141>
6. Філашкін В. С., Антошук А. О. Міжнародне співробітництво правоохоронних органів у протидії злочинам проти волі, честі та гідності особи. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2026. Т. 5, вип. 93. С. 236–240. DOI: <https://doi.org/10.24144/2307-3322.2026.93.5.29>
7. Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA. *Official Journal of the European Union*. 2016. L 135. P. 53–114.
8. Угода між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво від 14 груд. 2016 р. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/984_001-16#Text
9. Про вступ України до Інтерполу : Постанова Кабінету Міністрів України від 30 верес. 1992 р. № 555. *Офіційний вебпортал парламенту України*. URL: <https://zakon.rada.gov.ua/laws/show/555-92-%D0%BF#Text>
10. Про Національне центральне бюро Інтерполу: Постанова Кабінету Міністрів України від 25 берез. 1993 р. № 220. *Офіційний вебпортал парламенту України*. URL: <https://zakon.rada.gov.ua/laws/show/220-93-%D0%BF#Text>
11. Про представника Національного центрального бюро Інтерполу України у Міжнародній організації кримінальної поліції – Інтерпол: Указ Президента України від 6 серп. 2004 р. № 872/2004. *Офіційний вебпортал парламенту України*. URL: <https://zakon.rada.gov.ua/laws/show/872/2004#Text>
12. Про затвердження Інструкції про порядок використання правоохоронними органами України інформаційної системи Міжнародної організації кримінальної поліції – Інтерпол: Наказ Міністерства внутрішніх справ України, Офісу Генерального прокурора, Національного антикорупційного бюро України, Служби безпеки України, Державного бюро розслідувань, Міністерства фінансів України, Міністерства юстиції України від 17 серп. 2020 р. № 613/380/93/228/414/510/2801/5. *Офіційний вебпортал парламенту України*. URL: <https://zakon.rada.gov.ua/laws/show/z0849-20#Text>
13. Про затвердження Положення про Національну поліцію: Постанова Кабінету Міністрів України від 28 жовт. 2015 р. № 877. *Офіційний вебпортал парламенту України*. URL: <https://zakon.rada.gov.ua/laws/show/877-2015-%D0%BF#Text>

14. Про затвердження Положення про Єдиний реєстру осіб, зниклих безвісти за особливих обставин : Наказ Міністерства внутрішніх справ України від 29 серп. 2022 р. № 535. *Офіційний вебпортал парламенту України*. URL: <https://zakon.rada.gov.ua/laws/show/z0998-22#Text>
15. Кримінальний кодекс України : Закон України від 5 квіт. 2001 р. № 2341-III. *Офіційний вебпортал парламенту України*. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>
16. Протокол про попередження і припинення торгівлі людьми, особливо жінками і дітьми, і покарання за неї, що доповнює Конвенцію Організації Об'єднаних Націй проти транснаціональної організованої злочинності від 15 листоп. 2000 р. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/995_791#Text
17. Конвенція Ради Європи про заходи щодо протидії торгівлі людьми від 16 трав. 2005 р. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/994_858#Text
18. Протидія торгівлі людьми : методичні матеріали. Львівський державний університет внутрішніх справ: офіційний вебсайт. URL: <https://www.lvduvs.edu.ua/uk/karta-dokumentiv/category/252-slidstvo-12-dniv.html>
19. Fijnaut C. J. C. F. Police co-operation and the area of freedom, security and justice. *Europe's area of freedom, security and justice* / ed. by N. Walker. Oxford: Oxford University Press, 2004. P. 242–282.
20. Blasi Casagran C. The new Europol legal framework: implications for EU exchanges of information in the field of law enforcement. *Challenges and Critiques of the EU Internal Security Strategy: Rights, Power and Security* / ed. by M. O'Neill, K. Swinton. Cambridge : Cambridge Scholars Publishing, 2017. P. 138–161.
21. Wainwright R. Europol is uniting EU against fraud. *Fraud Magazine*. 2018. March/April. URL: <https://www.acfe.com/fraud-magazine/all-issues/issue/article?s=2018-marchapril-interview-rob-wainwright>
22. Про захист персональних даних: проєкт Закону України від 25 жовт. 2022 р. № 8153. *Офіційний вебпортал парламенту України*. URL: <https://itd.rada.gov.ua/billinfo/Bills/Card/40707>

References:

1. Perepiolkin, S. M. (2021). Pravovyi status ahentstva Yevropeiskoho Soiuzu zi spivrobotnytstva pravookhoronnykh organiv (Yevropol) [Legal status of the European Union Agency for Law Enforcement Cooperation (Europol)]. *Analitichno-porivnyalne pravoznavstvo*, (3), 270–275. <https://doi.org/10.24144/2788-6018.2021.03.50> [in Ukrainian].
2. Toma, M. H. (2025). Interpol yak instrument protydii zlochynnosti [Interpol as a tool for combating crime]. *Uzhhorod National University Scientific Bulletin. Series: Law*, 87(3), 349–353. <https://doi.org/10.24144/2307-3322.2025.87.3.53> [in Ukrainian].
3. Horash, O. S., & Hromovych, A. A. (2025). Interpol i Yevropol yak kliuchovi subiekty mizhnarodnoi politseiskoi kooperatsii v systemi protydii transnatsionalnii orhanizovanii zlochynnosti [Interpol and Europol as key entities of international police cooperation in the system of countering transnational organized crime]. *Bulletin of the Criminological Association of Ukraine*, 36(3), 136–146. <https://doi.org/10.32631/vca.2025.3.10> [in Ukrainian].
4. Moiseieva, Ye. O., Latysheva, M. O., & Shalupnia, K. S. (2023). Diialnist Yevropolu ta spivpratsia z Ukrainoiu [Europol's activities and cooperation with Ukraine]. *Yuridicheskiy nauchnyy elektronnyy zhurnal*, (4), 714–718. <https://doi.org/10.32782/2524-0374/2023-4/173> [in Ukrainian].
5. Voroniatnykov, O. O. (2025). Diialnist mizhnarodnykh ustanov ta orhanizatsii u borotbi zi zlochynnistiu [Activities of international institutions and organizations in the fight against crime]. *Analitichno-porivnyalne pravoznavstvo*, (1), 876–880. <https://doi.org/10.24144/2788-6018.2025.01.141> [in Ukrainian].
6. Filashkin, V. S., & Antoshchuk, A. O. (2026). Mizhnarodne spivrobotnytstvo pravookhoronnykh orhaniv u protydii zlochynam proty voli, chesti ta hidnosti osoby [International cooperation of law enforcement agencies in countering crimes against personal liberty, honor, and dignity]. *Uzhhorod National University Scientific Bulletin. Series: Law*, 93(5), 236–240. <https://doi.org/10.24144/2307-3322.2026.93.5.29> [in Ukrainian].
7. European Parliament & Council of the European Union. (2016). *Regulation (EU) 2016/794 of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA*. Official Journal of the European Union, L 135, 53–114 [in English].
8. Verkhovna Rada of Ukraine. (2016, December 14). *Uhoda mizh Ukrainoiu ta Yevropeiskym politseiskym ofisom pro operativne ta stratehichne spivrobotnytstvo* [Agreement between Ukraine and the European Police Office on Operational and Strategic Cooperation]. Official Web Portal of the Parliament of Ukraine. https://zakon.rada.gov.ua/laws/show/984_001-16#Text [in Ukrainian].

9. Cabinet of Ministers of Ukraine. (1992, September 30). *Pro vstup Ukrainy do Interpolu* [On Ukraine's accession to Interpol] (Resolution No. 555). Official Web Portal of the Parliament of Ukraine. <https://zakon.rada.gov.ua/laws/show/555-92-%D0%BF#Text> [in Ukrainian].
10. Cabinet of Ministers of Ukraine. (1993, March 25). *Pro Natsionalne tsentralne biuro Interpolu* [On the National Central Bureau of Interpol] (Resolution No. 220). Official Web Portal of the Parliament of Ukraine. <https://zakon.rada.gov.ua/laws/show/220-93-%D0%BF#Text> [in Ukrainian].
11. President of Ukraine. (2004, August 6). *Pro predstavnyka Natsionalnoho tsentralnoho biuro Interpolu Ukrainy u Mizhnarodnii orhanizatsii kryminalnoi politzii – Interpol* [On the Representative of the National Central Bureau of Interpol of Ukraine to the International Criminal Police Organization – Interpol] (Decree No. 872/2004). Official Web Portal of the Parliament of Ukraine. <https://zakon.rada.gov.ua/laws/show/872/2004#Text> [in Ukrainian].
12. Ministry of Internal Affairs of Ukraine, Office of the Prosecutor General, National Anti-Corruption Bureau of Ukraine, Security Service of Ukraine, State Bureau of Investigation, Ministry of Finance of Ukraine, & Ministry of Justice of Ukraine. (2020, August 17). *Pro zatverdzhennia Instruksii pro poriadok vykorystannia pravookhoronnymy orhanamy Ukrainy informatsiinoi systemy Mizhnarodnoi orhanizatsii kryminalnoi politzii – Interpol* [On approval of the Instruction on the procedure for using the information system of the International Criminal Police Organization – Interpol by Ukrainian law enforcement agencies] (Joint Order No. 613/380/93/228/414/510/2801/5). Official Web Portal of the Parliament of Ukraine. <https://zakon.rada.gov.ua/laws/show/z0849-20#Text> [in Ukrainian].
13. Cabinet of Ministers of Ukraine. (2015, October 28). *Pro zatverdzhennia Polozhennia pro Natsionalnu politziiu* [On approval of the Regulation on the National Police] (Resolution No. 877). Official Web Portal of the Parliament of Ukraine. <https://zakon.rada.gov.ua/laws/show/877-2015-%D0%BF#Text> [in Ukrainian].
14. Ministry of Internal Affairs of Ukraine. (2022, August 29). *Pro zatverdzhennia Poriadku vedennia Yedynoho reiestru osib, znyklykh bezvisti za osoblyvykh obstavyn* [On approval of the Procedure for maintaining the Unified Register of Persons Missing under Special Circumstances] (Order No. 535). Official Web Portal of the Parliament of Ukraine. <https://zakon.rada.gov.ua/laws/show/z0998-22#Text> [in Ukrainian].
15. Verkhovna Rada of Ukraine. (2001, April 5). *Kryminalnyi kodeks Ukrainy* [Criminal Code of Ukraine] (Law No. 2341-III). Official Web Portal of the Parliament of Ukraine. <https://zakon.rada.gov.ua/laws/show/2341-14#Text> [in Ukrainian].
16. United Nations. (2000, November 15). *Protokol pro poperedzhennia i prypynennia torkivli liudmy, osoblyvo zhinkamy i ditmy, i pokarannia za nei, shcho dopovniuie Konventsiiu Orhanizatsii Obiednanykh Natsii proty transnatsionalnoi orhanizovanoi zlochynnosti* [Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime]. Official Web Portal of the Parliament of Ukraine. https://zakon.rada.gov.ua/laws/show/995_791#Text [in Ukrainian].
17. Council of Europe. (2005, May 16). *Konventsiiia Rady Yevropy pro zakhody shchodo protydii torkivli liudmy* [Council of Europe Convention on Action against Trafficking in Human Beings]. Official Web Portal of the Parliament of Ukraine. https://zakon.rada.gov.ua/laws/show/994_858#Text [in Ukrainian].
18. Lviv State University of Internal Affairs. (n.d.). *Protydiia torkivli liudmy: metodychne zabezpechennia* [Countering human trafficking: Methodological materials]. <https://www.lvduvs.edu.ua/uk/karta-dokumentiv/category/252-slidstvo-12-dniv.html> [in Ukrainian].
19. Fijnaut, C. J. C. F. (2004). Police co-operation and the area of freedom, security and justice. In N. Walker (Ed.), *Europe's area of freedom, security and justice* (pp. 242–282). Oxford University Press [in English].
20. Blasi Casagran, C. (2017). The new Europol legal framework: Implications for EU exchanges of information in the field of law enforcement. In M. O'Neill & K. Swinton (Eds.), *Challenges and critiques of the EU internal security strategy: Rights, power and security* (pp. 138–161). Cambridge Scholars Publishing [in English].
21. Wainwright, R. (2018). Europol is uniting EU against fraud. *Fraud Magazine*, March/April. <https://www.acfe.com/fraud-magazine/all-issues/issue/article?s=2018-marchapril-interview-rob-wainwright> [in English].
22. Verkhovna Rada of Ukraine. (2022, October 25). *Pro zakhyst personalnykh danykh* [On personal data protection] (Draft Law No. 8153). Official Web Portal of the Parliament of Ukraine. <https://itd.rada.gov.ua/billinfo/Bills/Card/40707> [in Ukrainian].



УДК 343.985:351.74

DOI <https://doi.org/10.32782/2311-8040/2026-2-9>**Татаренко Світлана В'ячеславівна,**

доктор філософії в галузі права,

доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки

Навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції

імені Е. О. Дідоренка,

Донецький державний університет внутрішніх справ,

вулиця Велика Перспективна, 1, Кропивницький, 25015, Україна

ORCID: <https://orcid.org/0000-0001-9425-0227>**Явтушенко Юлія Вікторівна,**

викладач кафедри оперативно-розшукової

діяльності та інформаційної безпеки

Навчально-наукового інституту підготовки фахівців для підрозділів кримінальної поліції

імені Е. О. Дідоренка,

Донецький державний університет внутрішніх справ,

вулиця Велика Перспективна, 1, Кропивницький, 25015, Україна

ORCID: <https://orcid.org/0009-0004-3719-8871>

СПЕЦІАЛЬНІ ТЕХНІЧНІ ЗАСОБИ У РОЗШУКОВІЙ ДІЯЛЬНОСТІ КРИМІНАЛЬНОЇ ПОЛІЦІЇ: ПРАВОВІ ЗАСАДИ, ФУНКЦІОНАЛЬНІ МОЖЛИВОСТІ ТА НАПРЯМИ ВДОСКОНАЛЕННЯ

Анотація. У статті досліджено правові та організаційні засади застосування спеціальних технічних засобів працівниками кримінальної поліції під час розшуку осіб. Уточнено співвідношення категорій «спеціальна техніка», «оперативна техніка», «оперативно-технічні засоби» та «спеціальні технічні засоби», проаналізовано наукові підходи до визначення цього поняття та обґрунтовано доцільність використання терміна «застосування» щодо реалізації законних владних повноважень. Сформульовано узагальнене визначення спеціальних технічних засобів розшукової діяльності кримінальної поліції та запропоновано їх функціональну класифікацію, що охоплює шість взаємопов'язаних груп: засоби спостереження і фіксації; інформаційно-пошукові та аналітичні системи; засоби комунікаційного й геопросторового аналізу; засоби біометричної ідентифікації; засоби цифрового пошуку у відкритих джерелах; технічне забезпечення оперативно-розшукових заходів і негласних слідчих дій. Показано, що правовий режим кожної групи визначається не її назвою, а характером втручання у права людини, і проаналізовано відповідні положення Закону України «Про Національну поліцію». Розкрито функціональні можливості інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України», зокрема бази даних «Розшук» та інформаційної підсистеми «Електронна розшукова справа», обґрунтовано вимоги до якості первинного запису та своєчасного оновлення розшукових обліків. Сформульовано пропозиції щодо уніфікації понятійного апарату оперативно-розшукової діяльності на законодавчому та відомчому рівнях і узгодження положень Закону України «Про оперативно-розшукову діяльність», Кримінального процесуального кодексу України, Закону України «Про Національну поліцію» та відомчих актів, що регулюють функціонування інформаційних систем розшуку.

Ключові слова: кримінальна поліція, розшук осіб, спеціальні технічні засоби, оперативна техніка, оперативно-технічні засоби, правовий режим, база даних «Розшук», електронна розшукова справа, функціональна класифікація, оперативно-розшукова діяльність.

Tatarenko Svitlana, Yavtushenko Yuliia. SPECIAL TECHNICAL MEANS IN THE PERSON-SEARCH ACTIVITIES OF THE CRIMINAL POLICE: LEGAL FOUNDATIONS, FUNCTIONAL CAPABILITIES AND AREAS FOR IMPROVEMENT

Abstract. The article examines the legal and organizational foundations for the use of special technical means by criminal police officers in searching for persons. It clarifies the relationship between the concepts of special equipment, operational equipment, operational-technical means and special technical means, analyzes scientific approaches to defining this concept, and substantiates the use of the term «application» when lawful public

powers are exercised. A generalized definition of special technical means of the criminal police search activity is formulated, and a functional classification is proposed, covering six interconnected groups: observation and recording devices; information-search and analytical systems; telecommunications and geospatial analysis tools; biometric identification; open-source digital search; and technical support for operational-search measures and covert investigative actions. It is shown that the legal regime of each group is determined not by its name but by the nature of the interference with human rights, and the relevant provisions of the Law of Ukraine «On the National Police» are analyzed. The functional capabilities of the information and communication system «Information Portal of the National Police of Ukraine», including the «Search» database and the «Electronic Search Case» information subsystem, are disclosed, and requirements for the quality of primary data entry and timely updating of search records are substantiated. Proposals are formulated for unifying the conceptual apparatus of operational-search activity at the legislative and departmental levels and for harmonizing the provisions of the Law of Ukraine «On Operational-Search Activity», the Criminal Procedure Code of Ukraine, the Law of Ukraine «On the National Police» and departmental acts regulating the functioning of search information systems.

Key words: criminal police, search for persons, special technical means, operational equipment, operational-technical means, legal regime, the «Search» database, electronic search case, functional classification, operational-search activity.

Вступ. Розшук осіб належить до базових напрямів діяльності кримінальної поліції та охоплює встановлення місцезнаходження осіб, які переховуються від органів досудового розслідування, слідчого судді чи суду, ухиляються від відбування кримінального покарання, зникли безвісти, а також установлення особи невпізнаних трупів та осіб, які через стан здоров'я, вік або інші обставини не можуть повідомити відомості про себе. Результативність такої діяльності безпосередньо залежить від швидкості одержання, перевірки, зіставлення й реалізації інформації. У сучасному суспільстві значна частина відомостей про переміщення, соціальні зв'язки, цифрову активність і зовнішність людини фіксується технічними системами, тому традиційні розшукові прийоми дедалі більше доповнюються програмно-технічними комплексами, автоматизованими інформаційними ресурсами, системами відеоспостереження, біометричною ідентифікацією, геопросторовим аналізом та інструментами пошуку у відкритих джерелах.

Закон України «Про оперативно-розшукову діяльність» визначає оперативно-розшукову діяльність як систему гласних і негласних пошукових та контррозвідувальних заходів, що здійснюються із застосуванням оперативних і оперативно-технічних засобів [1]. Водночас законодавство не містить цілісного визначення спеціальних технічних засобів, які можуть застосовуватися кримінальною поліцією саме під час розшуку осіб. У різних нормативних

актах і наукових працях використовуються поняття «технічні засоби», «оперативно-технічні засоби», «спеціальна техніка», «оперативна техніка», «технічні засоби негласного отримання інформації» та «спеціальні технічні засоби негласного отримання інформації». Термінологічна неоднорідність ускладнює розмежування правових режимів, визначення підстав застосування певного засобу, документування результатів та оцінювання їх допустимості у кримінальному провадженні.

Технічна модернізація розшуку має подвійний правовий ефект. З одного боку, вона підвищує ймовірність своєчасного встановлення розшукуваної особи, дозволяє опрацьовувати значні масиви даних, зменшує залежність від суб'єктивного сприйняття працівника та сприяє раціональному використанню сил. З іншого боку, автоматизоване зіставлення біометричних даних, доступ до комунікаційної інформації, приховане спостереження або накопичення цифрових профілів здатні істотно втручатися у приватність не лише розшукуваної особи, а й невизначеного кола громадян. Через це ефективність технічного засобу не може бути самостійним виправданням його застосування: необхідними є законна мета, належна правова підстава, пропорційність, контрольованість і можливість подальшої перевірки отриманого результату.

Актуальність проблеми посилюється умовами воєнного стану, масштабним переміщенням населення, збільшенням кількості безві-

сно зниклих, ускладненням ідентифікації осіб, використанням злочинцями засобів конспірації, підроблених документів, анонімних облікових записів та сучасних каналів зв'язку. Водночас воєнні виклики не скасовують конституційних гарантій, а вимагають особливо чіткого визначення меж втручання. Наукове осмислення спеціальних технічних засобів у розшуковій діяльності повинно поєднувати оперативно-розшуковий, кримінальний процесуальний, криміналістичний, інформаційно-правовий та правозахисний підходи.

Аналіз останніх наукових джерел засвідчує таке. Теоретичні основи оперативно-розшукової діяльності та її технічного забезпечення розробляли О.М. Бандурка, Е.О. Дідоренко, О.Ф. Долженков, М.А. Погорецький, І.В. Сервецький, С.Б. Фомін, І.Ф. Хараберюш та інші науковці. І.Ф. Хараберюш у своїх працях розглядав різні аспекти застосування спеціальної техніки в поліцейській діяльності [2, с. 112–114; 3, с. 52–53; 4, с. 32–40], зокрема, оперативну техніку, як окремий розділ оперативно-розшукової діяльності [5, с. 340–343].

Історичні й організаційні аспекти технічного забезпечення карного розшуку дослідив Д.В. Безруков [6, с. 163–164]. Ю.П. Поляк запропонував розгорнуте визначення технічних засобів досудового розслідування і обґрунтував залежність допустимості даних, отриманих за допомогою технічних засобів, від дотримання процесуальної форми, збереження носіїв інформації та можливості перевірки її достовірності [7, с. 67–69]. А.М. Тимчишин розглядає застосування науково-технічних засобів у контексті спеціальних знань і криміналістичної розвідки, наголошуючи на перспективах аналітичних систем, технологій великих даних, Інтернету речей та відеоаналітики для швидкого встановлення підозрюваних [8, с. 131–141]. О.О. Юхно та О.О. Загуменний дослідили можливості автоматизованих інформаційно-пошукових систем МВС і Національної поліції, пошукових сервісів, соціальних мереж, ІР-адресації та фіксації цифрових слідів під час оперативно-розшукових заходів і негласних слідчих дій [9, с. 53–85]. А.М. Гребенюк, С.О. Прокопов і Л.В. Рибальченко сис-

тематизували методи розпізнавання осіб за фото- та відеозображеннями, проаналізували спеціалізовані пошукові системи й окреслили практичні можливості їх застосування підрозділами Національної поліції [10, с. 18–44]. Новітня праця І.О. Моргуна і Т.В. Морей присвячена розмежуванню термінів «використання» та «застосування» стосовно спеціальних технічних засобів; автори обґрунтовують, що «застосування» доцільно пов'язувати з реалізацією законних владних повноважень і безпосереднім функціональним призначенням засобу [11, с. 155–162].

Попри значну кількість робіт, комплексна модель застосування спеціальних технічних засобів саме працівниками кримінальної поліції під час розшуку різних категорій осіб залишається недостатньо розробленою. У науковій літературі переважно окремо розглядаються оперативна техніка, процесуальне використання результатів НСРД, цифровий пошук або біометрична ідентифікація. Недостатня увага приділяється інтеграції цих інструментів у єдиний розшуковий цикл, критеріям перевірки автоматизованих збігів, алгоритмічній упередженості, розмежуванню орієнтуючої та доказової інформації, а також стандартам документування дій оператора технічної системи.

Мета статті полягає у формуванні цілісного наукового підходу до розуміння спеціальних технічних засобів, що застосовуються працівниками кримінальної поліції під час розшуку осіб, визначенні їх поняття та функціональної класифікації, з'ясуванні правових режимів окремих груп засобів і можливостей інформаційно-пошукових систем «Розшук» та «Електронна розшукова справа», а також обґрунтуванні напрямів уніфікації термінології та гармонізації нормативного забезпечення такої діяльності.

Матеріали та методи. Методологічну основу дослідження становить комплекс загальнонаукових і спеціально-юридичних методів пізнання. Діалектичний метод застосовано для з'ясування взаємозв'язку між технологічним розвитком засобів розшуку та станом їх правового регулювання. За допомогою фор-

мально-логічного та юридико-догматичного методів опрацьовано зміст положень Закону України «Про оперативно-розшукову діяльність», Кримінального процесуального кодексу України, Закону України «Про Національну поліцію» та відомчих нормативних актів МВС України, що регламентують функціонування інформаційних систем розшуку. Термінологічний аналіз і метод юридичної герменевтики використано для зіставлення наукових дефініцій категорій «спеціальна техніка», «оперативна техніка», «оперативно-технічні засоби» та «спеціальні технічні засоби». Системно-структурний метод застосовано для побудови функціональної класифікації спеціальних технічних засобів розшукової діяльності. Матеріалами дослідження слугували нормативно-правові акти України, монографічна та періодична наукова література з питань оперативно-розшукової діяльності за 2015–2026 роки, а також відомчі інструкції, що регулюють ведення бази даних «Розшук» та інформаційної підсистеми «Електронна розшукова справа».

Результати. Розшук осіб як напрям діяльності кримінальної поліції охоплює встановлення місцезнаходження підозрюваних, обвинувачених, засуджених, які переховуються від органів досудового розслідування, слідчого судді або суду, осіб, які безвісти зникли за загальних чи особливих обставин, а також осіб, місцеперебування яких невідоме з інших причин, що мають значення для кримінального провадження. Реалізація цього завдання неможлива без використання оперативних і оперативно-технічних засобів, застосування яких дозволяє набагато ефективніше виявляти й розкривати кримінальні правопорушення, запобігати їм, а також розшукувати осіб, які уникають слідства та суду [12, с. 63].

Перш ніж перейти до розгляду практики застосування технічних засобів, доцільно з'ясувати понятійний апарат дослідження. Поняття спеціальних технічних засобів у розшуковій діяльності доцільно розглядати не лише через конструктивні особливості пристрою, а насамперед через його функціональне призначення, правовий режим та спосіб застосування. Наприклад, звичайна камера,

мобільний термінал або програмний продукт можуть використовуватися у загальнопобутових цілях, однак у межах розшуку вони стають складовою спеціально організованої діяльності зі збирання, оброблення, зіставлення або фіксації відомостей. Водночас спеціально розроблений засіб негласного одержання інформації має особливий режим обігу і застосування незалежно від конкретної операції. Тому ототожнення спеціальної техніки виключно із прихованими пристроями є методологічно звуженим.

Аналіз наукових доробок вчених, присвячених вивченню використання спеціальних технічних засобів у розшуковій діяльності, дає право стверджувати про полісемантичність визначення поняття «спеціальні технічні засоби».

Так, К.Д. Шаблевська, І.І. Євдокимов, А.О. Кисельов спеціальні технічні засоби визначають як «сукупність технічних пристроїв, речовин, цифрових носіїв та програм, обмежених у обороті, розроблених для негласного, контрольованого виявлення, отримання, фіксації інформації, що застосовуються належними суб'єктами під час проведення оперативно-розшукових заходів із метою вирішення завдань оперативно-розшукової діяльності» [13, с. 183–184].

І.Ф. Хараберюш у своїх працях розглядав оперативну техніку одночасно як розділ теорії оперативно-розшукової діяльності, вид діяльності уповноважених суб'єктів і складову спеціальної техніки правоохоронних органів. Автор визначає її як сукупність наукових положень і рекомендацій щодо застосування технічних, програмно-технічних, програмних засобів, речовин, інформаційних систем та спеціальних методів під час оперативно-розшукових заходів і негласних слідчих дій [5, с. 340–342].

С.В. Пеньков наголошує на тому, що «терміни «спеціальна техніка», «оперативна техніка», «оперативно-технічні засоби», «спеціальні технічні засоби для зняття інформації з каналів зв'язку, інші засоби негласного отримання інформації» не можна ототожнювати, натомість вони співвідносяться між собою, як єдине і частка» [14, с. 86].

Ю.П. Поляк, досліджуючи питання застосування технічних засобів при проведенні слідчих (розшукових), негласних слідчих (розшукових) дій, запропонував їх розгорнуте визначення як приладів, апаратів, устаткування, пристроїв, інструментів, матеріалів, програмного забезпечення, а також методів і прийомів їх гласного або негласного застосування для виявлення, фіксування, вилучення та дослідження інформації, що має значення для кримінального провадження [7, с. 24–25].

Наведені наукові підходи свідчать про відсутність у правовій доктрині єдиного розуміння змісту поняття «спеціальні технічні засоби». У широкому значенні воно охоплює систему технічних, програмних, інформаційних та методичних засобів забезпечення оперативно-розшукової і кримінальної процесуальної діяльності. У вузькому значенні спеціальні технічні засоби пов'язуються переважно з пристроями та технологіями, спеціально створеними або пристосованими для негласного одержання й фіксування інформації та обмеженими у цивільному обігу. Відмінності у позиціях учених зумовлені тим, що досліджуване поняття розглядається ними в різних площинах: як елемент спеціальної або оперативної техніки, як матеріальний інструментарій діяльності уповноважених підрозділів, як сукупність технічних засобів і способів їх використання, а також як функціональна система одержання та опрацювання інформації.

Спільним для проаналізованих визначень є визнання спеціальних технічних засобів складовою цілеспрямованої діяльності уповноважених суб'єктів, яка здійснюється на нормативно визначених підставах і спрямовується на одержання інформації, необхідної для виконання завдань оперативно-розшукової діяльності або кримінального провадження. Водночас сучасний рівень технологічного розвитку не дозволяє обмежувати зміст цієї категорії виключно матеріальними приладами чи пристроями. Розшукова діяльність кримінальної поліції передбачає використання програмного забезпечення, автоматизованих інформаційно-пошукових систем, технологій відеоаналітики, біометричної ідентифікації, геопросторового

аналізу та інших засобів оброблення значних масивів даних. Тому поняття спеціальних технічних засобів має визначатися з урахуванням не лише їх конструктивних характеристик, а й функціонального призначення, правового режиму та завдань, для виконання яких вони використовуються.

Узагальнюючи наявні позиції вчених спеціальні технічні засоби розшукової діяльності кримінальної поліції можна визначити як технічні, програмні, програмно-технічні засоби, інформаційні системи, спеціальні речовини та науково обґрунтовані методи їх застосування, що використовуються уповноваженими працівниками на законних підставах для виявлення, одержання, фіксування, збереження, оброблення, аналізу і перевірки відомостей, необхідних для встановлення місцезнаходження або ідентифікації розшукуваної особи. Таке визначення охоплює як гласні засоби, доступні без спеціального судового дозволу, так і негласні технології, застосування яких допускається лише в установленому законом порядку.

Науково обґрунтованим є вживання терміна «застосування», коли йдеться про здійснення працівником кримінальної поліції владних повноважень за допомогою технічного засобу. «Використання» може мати ширше нейтральне значення та охоплювати експлуатацію обладнання, роботу з отриманими даними або застосування результатів в іншій діяльності. Однак абсолютне протиставлення цих слів є недоцільним, оскільки законодавець традиційно вживає їх непослідовно. Для науки і правотворчості важливо не стільки механічно замінити один термін іншим, скільки пов'язати кожний спосіб технічного втручання з конкретними підставами, суб'єктом, процедурою та формою контролю [11, с. 155–162].

Класифікація спеціальних технічних засобів, що використовуються кримінальною поліцією під час розшуку осіб, може здійснюватися за різними критеріями. І. Ф. Хараберюш пропонує поділяти технічні засоби оперативно-розшукового призначення за критерієм оперативно-технічного спрямування на технічні засоби гласного отримання інформації, технічні засоби негласного отримання інформації та

засоби забезпечення оперативно-розшукових заходів [5, с. 341]. За функціональним призначенням завдання застосування технічних засобів автор поділяє на загальні – науково-технічне забезпечення практики оперативних підрозділів у роботі з пошуку та фіксації даних про протиправну діяльність осіб, і спеціальні – розроблення нових та вдосконалення наявних оперативно-технічних засобів, зокрема спеціальних програм та інтелектуальних систем аналітичного супроводження оперативно-розшукової діяльності [5, с. 342]. Наприклад, С.М. Зеленський деталізує цю класифікацію, виокремлюючи технічні засоби зв'язку для проведення оперативно-розшукових заходів; технічні засоби пошуку (металошукачі, тепловізори), що допомагають виявляти осіб, які переховуються від влади; технічні засоби психофізіологічного моніторингу (поліграф, аналізатори голосового стресу); технічні засоби оперативного спостереження, зокрема прилади нічного бачення та ендоскопи; технічні засоби й системи візуального контролю (біноклі, телескопи); технічні засоби фіксації інформації на різних носіях; технічні засоби та системи аудіоконтролю (мікрофони, лазерні системи, стетоскопи) [12, с. 64].

Ми вважаємо, що функціональна класифікація спеціальних технічних засобів розшуку може охоплювати шість взаємопов'язаних груп. Першу становлять засоби спостереження, виявлення та фіксації: фото- і відеокамери, прилади нічного бачення, тепловізійні засоби, системи відеоспостереження, засоби аудіофіксації та інші пристрої, що забезпечують візуальне або акустичне сприйняття подій. Другу групу утворюють інформаційно-пошукові та аналітичні системи, включаючи поліцейські бази даних, електронні розшукові справи, інструменти аналізу зв'язків і автоматизованого зіставлення відомостей. Третя група включає комунікаційні й геопросторові засоби, за допомогою яких аналізуються маршрути, місця активності, просторово-часові закономірності та, за наявності законних підстав, дані електронних комунікацій. До четвертої групи належать засоби біометричної ідентифікації: системи розпізнаван-

ня обличчя, автоматизовані дактилоскопічні та інші біометричні комплекси. П'яту групу становлять засоби цифрового пошуку у відкритих джерелах, що використовують загальнодоступні вебресурси, соціальні мережі, пошукові оператори, зворотний пошук зображень та інші OSINT-інструменти. Шоста група охоплює технічне забезпечення оперативно-розшукових заходів і негласних слідчих дій: спеціально розроблені або модифіковані засоби прихованого отримання, передавання й фіксації інформації. Межі між групами є рухомими: одна інтегрована платформа може одночасно здійснювати відеофіксацію, біометричний пошук, геоприв'язку і формування аналітичного повідомлення.

Правовий режим кожної групи визначається не її назвою, а характером втручання. Гласне опрацювання відкритої інформації, перевірка особи за поліцейською базою даних або перегляд запису камери, доступ до якого отримано законно, відрізняються від негласного спостереження за особою, зняття інформації з електронних комунікаційних мереж чи встановлення технічного засобу в приватному просторі. Останні дії можуть істотно обмежувати конституційні права і тому потребують спеціальної підстави, дотримання вимог Закону України «Про оперативно-розшукову діяльність», КПК України та, у передбачених випадках, дозволу слідчого судді [1; 15].

Закон України «Про Національну поліцію» покладає на поліцію завдання щодо розшуку осіб у випадках, визначених законом, і надає право формувати та використовувати інформаційні ресурси. Стаття 40 цього Закону передбачає застосування фото- і відеотехніки, технічних приладів та засобів, що мають функції фото- і кінозйомки, відеозапису, а також використання інформації, отриманої з автоматичної фото- і відеотехніки [16]. Проте зазначена норма не створює універсального дозволу на будь-яке технічне спостереження. Працівник повинен ураховувати мету, місце, очікуваний обсяг втручання, статус об'єкта, наявність оперативно-розшукової справи або кримінального провадження та спеціальні процедурні правила.

Центральне місце в сучасній організації розшуку посідає інформаційно-комунікаційна система «Інформаційний портал Національної поліції України». Інструкція, затверджена наказом МВС України від 28 червня 2023 року № 534, визначає базу даних «Розшук» як автоматизований банк відомостей щодо осіб, які переходять від органів досудового розслідування, суду, ухиляються від відбування покарання, зникли безвісти, не можуть повідомити інформацію про себе, а також інших законодавчо визначених категорій [17]. Її значення полягає не лише у зберіганні орієнтувань, а й у забезпеченні швидкої перевірки особи, актуалізації розшукових обліків та взаємодії різних підрозділів.

Інформаційна підсистема «Електронна розшукова справа», урегульована наказом МВС України від 5 липня 2023 року № 553, забезпечує електронне формування, оброблення й систематизацію інформації в оперативно-розшукових і розшукових справах [18]. Її впровадження створює передумови для переходу від розрізнених паперових матеріалів до структурованого цифрового середовища, у якому можуть поєднуватися біографічні дані, фотозображення, зв'язки, результати перевірок, відомості про можливі місця перебування та виконані заходи. Разом із тим цифровізація розшукової справи підвищує вимоги до розмежування доступу, журналювання операцій користувачів, резервного копіювання, контролю якості внесених даних і своєчасного припинення оброблення після завершення розшуку.

Якість автоматизованого пошуку залежить від якості первинного запису. Помилка у транслітерації прізвища, даті народження, статусі розшуку або фотозображенні може призвести до невиявлення особи чи хибного збігу. Тому внесення інформації має супроводжуватися перевіркою джерела, стандартизованим заповненням ідентифікаційних полів, зазначенням дати актуальності та можливих варіантів персональних даних. Не менш важливим є механізм швидкого оновлення інформації після затримання, добровільної явки, встановлення місцезнаходження або скасування правових

підстав розшуку. Застарілий запис здатний спричинити необґрунтоване втручання у права людини.

Удосконалення нормативної бази має розпочинатися з уніфікації понятійного апарату. Доцільно законодавчо або на рівні рамкового відомчого акта визначити загальне поняття технічних засобів оперативно-розшукової діяльності, їх основні групи та критерії віднесення до спеціальних засобів негласного отримання інформації. Водночас деталізовані тактико-технічні характеристики засекречених засобів не повинні бути відкритими. Публічна норма має визначати межі повноваження та гарантії, а закрита – конкретні методики й організацію застосування.

Необхідним є також узгодження Закону України «Про оперативно-розшукову діяльність», КПК України, Закону України «Про Національну поліцію» та відомчих актів щодо інформаційних систем. Працівник повинен чітко розуміти, коли інформаційна перевірка здійснюється як повсякденне виконання поліцейських повноважень, коли – як оперативно-розшуковий захід у межах відповідної справи, а коли потрібне доручення слідчого або прокурора і дозвіл слідчого судді. Змішування режимів може призвести до втрати доказового значення інформації та порушення прав людини.

Висновки. Проведене дослідження засвідчило, що зміст поняття «спеціальні технічні засоби» у розшуковій діяльності кримінальної поліції не отримав у правовій доктрині та законодавстві єдиного тлумачення: наявні визначення відображають різні площини аналізу – конструктивні характеристики пристроїв, функціональне призначення, правовий режим обігу та завдання, для виконання яких засоби застосовуються. Узагальнення наукових підходів дало змогу сформулювати визначення спеціальних технічних засобів розшукової діяльності як технічних, програмних, програмно-технічних засобів, інформаційних систем, спеціальних речовин та науково обґрунтованих методів їх застосування, що використовуються уповноваженими працівниками на законних підставах для виявлення, одержання, фіксування, збереження, оброблення, аналізу

і перевірки відомостей, необхідних для встановлення місцезнаходження або ідентифікації розшукуваної особи. Обґрунтовано, що термін «застосування» доцільно пов'язувати саме з реалізацією владних повноважень працівника кримінальної поліції, тоді як «використання» має ширше нейтральне значення.

Запропонована функціональна класифікація спеціальних технічних засобів, що охоплює шість взаємопов'язаних груп, дає змогу подолати штучне протиставлення «спеціальної», «оперативної» та «оперативно-технічної» техніки і зосередити увагу на правовому режимі, який визначається не назвою засобу, а характером втручання у права людини. Аналіз функціональних можливостей бази даних «Розшук» та інформаційної підсистеми «Електронна розшукова справа» показав, що результативність цифровізації розшукової справи безпосередньо залежить від якості первинного внесення відомостей, стандартизації ідентифікаційних полів і своєчасного оновлення інформації після зміни правових підстав розшуку.

Основними напрямками вдосконалення нормативного забезпечення застосування спеціальних технічних засобів у розшуковій діяльності кримінальної поліції є уніфікація понятійного апарату на законодавчому або рамковому відомчому рівні, розмежування публічних норм, що визначають межі повноважень і гарантії прав людини, та закритих методичних актів, які регламентують тактико-технічні характеристики засобів негласного отримання інформації, а також узгодження Закону України «Про оперативно-розшукову діяльність», Кримінального процесуального кодексу України, Закону України «Про Національну поліцію» та відомчих актів щодо інформаційних систем розшуку. Технологічні, тактичні та безпекові аспекти застосування конкретних інструментів розшуку – систем відеоспостереження, технологій розпізнавання обличчя, засобів цифрового пошуку у відкритих джерелах, геопросторового аналізу та гарантії захисту персональних даних – становлять предмет подальшого дослідження авторів.

Список використаних джерел:

1. Про оперативно-розшукову діяльність: Закон України від 18 лютого 1992 року № 2135-ХІІ. URL: <https://zakon.rada.gov.ua/go/2135-12> (дата звернення: 18.07.2026).
2. Хараберюш І.Ф. Визначення поняття «спеціальна техніка», що використовується в адміністративній діяльності правоохоронних органів. *Сучасний розвиток державотворення та правотворення в Україні: проблеми теорії та практики*: збірник матеріалів ІХ Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених, м. Маріуполь, 19 травня 2020 року. Маріуполь : МДУ, 2020. С. 112–114.
3. Хараберюш І.Ф. Місце спеціальної техніки в юридичній науці. *Актуальні проблеми науки та освіти*: збірник матеріалів ХХІІ підсумкової науково-практичної конференції викладачів, м. Маріуполь, 07 лютого 2020 року. Маріуполь : МДУ, 2020. С. 52–53.
4. Хараберюш І.Ф. Спеціальна техніка правоохоронних органів: поняття та система. *Вісник Маріупольського державного університету. Серія: Право*. 2019. № 17. С. 32–40.
5. Хараберюш І.Ф. Оперативна техніка як категорія науки оперативно-розшукової діяльності. *Сучасні проблеми правового, економічного та соціального розвитку держави*: матеріали науково-практичної конференції. м. Харків, 01 грудня 2017 року. Харків, 2017. С. 340–343.
6. Безруков Д.В. Використання технічних засобів підрозділами карного розшуку у протидії злочинам: історичний аспект. *Проблеми правознавства та правоохоронної діяльності*. 2015. № 1 (52). С. 163–173.
7. Поляк Ю.П. Застосування технічних засобів при проведенні слідчих (розшукових), негласних слідчих (розшукових) дій та використання його результатів під час досудового розслідування: дис. ... д-ра філософії: 081 Право. Львів, 2022. 230 с.
8. Тимчишин А.М. Спеціальні знання у кримінальному процесі України: теорія та практика: дис. ... д-ра юрид. наук: 12.00.09. Кропивницький, 2023. 438 с.
9. Юхно О.О., Загумений О.О. Використання сучасних інформаційних технологій працівниками поліції при проведенні негласних слідчих (розшукових) дій: навчальний посібник. 2-ге вид., допов. і перероб. Харків : Колегіум, 2020. 116 с.

10. Гребенюк А.М., Прокопов С.О., Рибальченко Л.В. Використання технологій розпізнавання обличчя на відео- та фотозображеннях: метод. рекомендації. Дніпро : Дніпропетровський державний університет внутрішніх справ, 2023. 48 с.

11. Моргун І.О., Морей Т.В. Вживання термінів «використання» та «застосування» стосовно «спеціальних технічних засобів». *Аналітично-порівняльне правознавство*. 2026. № 2. Ч. 3. С. 155–162. DOI: <https://doi.org/10.24144/2788-6018.2026.02.3.21>

12. Зеленський С. М. Технічні засоби оперативно-розшукової діяльності в аспекті протидії кримінальним правопорушенням. *Українська поліцейстика: теорія, законодавство, практика*. 2025. № 4 (16). С. 62–66. DOI: <https://doi.org/10.32782/2709-9261-2025-4-16-11>

13. Шаблевська К.Д., Євдокимов І.І., Кисельов А.О. Особливості використання технічних засобів під час оперативно-розшукової протидії в кримінальному правопорушенні. *UNIVERSUM*. 2024. № 9. С. 182–188.

14. Пеньков С.В. Місце та зміст окремих термінів у сфері застосування техніки в оперативно-розшуковій діяльності. *Право і безпека*. 2015. № 3 (58). С. 83–87.

15. Кримінальний процесуальний кодекс України: Закон України від 13 квітня 2012 року № 4651-VI. URL: <https://zakon.rada.gov.ua/go/4651-17> (дата звернення: 18.07.2026).

16. Про Національну поліцію: Закон України від 02 липня 2015 року № 580-VIII. URL: <https://zakon.rada.gov.ua/go/580-19> (дата звернення: 18.07.2026).

17. Про затвердження Інструкції з формування та ведення бази даних «Розшук» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України»: наказ МВС України від 28 червня 2023 року № 534. URL: <https://zakon.rada.gov.ua/go/z1486-23> (дата звернення: 18.07.2026).

18. Про затвердження Положення про інформаційну підсистему «Електронна розшукова справа» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України»: наказ МВС України від 05 липня 2023 року № 553. URL: <https://zakon.rada.gov.ua/go/z1504-23> (дата звернення: 18.07.2026).

References:

1. Pro operativno-rozshukovu diialnist [On operational and investigative activities]: Zakon Ukrainy vid 18 liutoho 1992 roku No 2135-XII. URL: <https://zakon.rada.gov.ua/go/2135-12> (data zvernennia: 18.07.2026) [in Ukrainian].

2. Kharaberiush, I.F. (2020) Vyznachennia poniattia «spetsialna tekhnika», shcho vykorystovuietsia v administrativnii diialnosti pravookhoronnykh orhaniv [Definition of the concept of «special equipment» used in the administrative activities of law enforcement agencies]. *Suchasnyi rozvytok derzhavotvorennia ta pravotvorennia v Ukraini: problemy teorii ta praktyky: zbirnyk materialiv IKh Mizhnarodnoi naukovo-praktychnoi konferentsii studentiv, aspirantiv i molodykh vchenykh*, m. Mariupol, 19 travnia 2020 roku. Mariupol: MDU. S. 112–114 [in Ukrainian].

3. Kharaberiush, I.F. (2020) Mistse spetsialnoi tekhniky v yurydychnii nautsi [The place of special equipment in legal science]. *Aktualni problemy nauky ta osvity: zbirnyk materialiv KhXII pidsumkovoï naukovo-praktychnoi konferentsii vykladachiv*, m. Mariupol, 07 liutoho 2020 roku. Mariupol: MDU. S. 52–53 [in Ukrainian].

4. Kharaberiush, I.F. (2019) Spetsialna tekhnika pravookhoronnykh orhaniv: poniattia ta systema [Special equipment of law enforcement agencies: concept and system]. *Visnyk Mariupolskoho derzhavnogo universytetu. Serii: Pravo*. No 17. S. 32–40 [in Ukrainian].

5. Kharaberiush, I.F. (2017) Operativna tekhnika yak katehoriia nauky operativno-rozshukovoi diialnosti [Operational equipment as a category of the science of operational and investigative activities]. *Suchasni problemy pravovoho, ekonomichnogo ta sotsialnogo rozvytku derzhavy: materialy naukovo-praktychnoi konferentsii*. m. Kharkiv, 01 hrudnia 2017 roku. Kharkiv. S. 340–343 [in Ukrainian].

6. Bezrukov, D.V. (2015) Vykorystannia tekhnichnykh zasobiv pidrozdilamy karnoho rozshuku u protydii zlochynam: istorychnyi aspekt [The use of technical means by criminal investigation units in combating crimes: a historical aspect]. *Problemy pravoznavstva ta pravookhoronnoi diialnosti*. No 1 (52). S. 163–173 [in Ukrainian].

7. Poliak, Yu.P. (2022) Zastosuvannia tekhnichnykh zasobiv pry provedenni slidchykh (rozshukovykh), nehlasnykh slidchykh (rozshukovykh) dii ta vykorystannia yoho rezultativ pid chas dosudovoho rozsliduvannia [The use of technical means when conducting investigative (search), covert investigative (search) actions and the use of its results during pre-trial investigation]. *PhD's thesis*. Lviv. 230 s. [in Ukrainian].

8. Tymchyshyn, A.M. (2023) Spetsialni znannia u kryiminalnomu protsesi Ukrainy: teoriia ta praktyka [Special knowledge in the criminal process of Ukraine: theory and practice]. *Doctor's thesis*. Kropyvnytskyi. 438 s. [in Ukrainian].
9. Yukhno, O.O., & Zahumennyi, O.O. (2020) Vykorystannia suchasnykh informatsiinykh tekhnolohii pratsivnykamy politsii pry provedenni nehlasnykh slidchykh (rozshukovykh) dii [The use of modern information technologies by police officers when conducting covert investigative (search) actions]: navchalnyi posibnyk. 2-he vyd., dopov. i pererob. Kharkiv: Kolehium. 116 s. [in Ukrainian].
10. Hrebenuk, A.M., Prokopov, S.O., & Rybalchenko, L.V. (2023) Vykorystannia tekhnolohii rozpoznavannia oblychchia na video- ta fotozobrazhenniakh [The use of facial recognition technologies in video and photo images]: metod. rekomendatsii. Dnipro: Dnipropetrovskyi derzhavnyi universytet vnutrishnikh sprav. 48 s. [in Ukrainian].
11. Morhun, I.O., & Morei, T.V. (2026) Vzhyvannia terminiv «vykorystannia» ta «zastosuvannia» stosovno «spetsialnykh tekhnichnykh zasobiv» [Use of the terms «use» and «application» in relation to «special technical means»]. *Analychno-porivnialne pravoznavstvo*. No 2. Ch. 3. S. 155–162. DOI: <https://doi.org/10.24144/2788-6018.2026.02.3.21> [in Ukrainian].
12. Zelenskyi, S. M. (2025) Tekhnichni zasoby operatyvno-rozshukovoi diialnosti v aspekti protydii kryriminalnym pravoporushenniam [Technical means of operational and investigative activities in the aspect of counteraction to criminal offenses]. *Ukrainska politseistyka: teoriia, zakonodavstvo, praktyka*. No 4 (16). S. 62–66. DOI: <https://doi.org/10.32782/2709-9261-2025-4-16-11> [in Ukrainian].
13. Shablevska, K.D., Yevdokymov, I.I., & Kyselov, A.O. (2024) Osoblyvosti vykorystannia tekhnichnykh zasobiv pid chas operatyvno-rozshukovoi protydii v kryriminalnomu pravoporushenni [Features of the use of technical means during operational and investigative counteraction in a criminal offense]. *UNIVERSUM*. No 9. S. 182–188 [in Ukrainian].
14. Penkov, S.V. (2015) Mistse ta zmist okremykh terminiv u sferi zastosuvannia tekhniki v operatyvno-rozshukovii diialnosti [Place and content of individual terms in the field of application of equipment in operational and investigative activities]. *Pravo i bezpeka*. No 3 (58). S. 83–87 [in Ukrainian].
15. Kryriminalnyi protsesualnyi kodeks Ukrainy [Criminal Procedure Code of Ukraine]: Zakon Ukrainy vid 13 kvitnia 2012 roku No 4651-VI. URL: <https://zakon.rada.gov.ua/go/4651-17> (data zvernennia: 18.07.2026) [in Ukrainian].
16. Pro Natsionalnu politsiiu [On the National Police]: Zakon Ukrainy vid 02 lyupnia 2015 roku No 580-VIII. URL: <https://zakon.rada.gov.ua/go/580-19> (data zvernennia: 18.07.2026) [in Ukrainian].
17. Pro zatverdzhennia Instruktzii z formuvannia ta vedennia bazy danykh «Rozshuk» informatsiino-komunikatsiinoi systemy «Informatsiyni portal Natsionalnoi politsii Ukrainy» [On approval of the Instructions for the formation and maintenance of the «Search» database of the information and communication system «Information Portal of the National Police of Ukraine»]: nakaz MVS Ukrainy vid 28 chervnia 2023 roku No 534. URL: <https://zakon.rada.gov.ua/go/z1486-23> (data zvernennia: 18.07.2026) [in Ukrainian].
18. Pro zatverdzhennia Polozhennia pro informatsiinu pidsystemu «Elektronna rozshukova sprava» informatsiino-komunikatsiinoi systemy «Informatsiyni portal Natsionalnoi politsii Ukrainy» [On approval of the Regulations on the information subsystem «Electronic Detective Case» of the information and communication system «Information Portal of the National Police of Ukraine»]: nakaz MVS Ukrainy vid 05 lyupnia 2023 roku No 553. URL: <https://zakon.rada.gov.ua/go/z1504-23> (data zvernennia: 18.07.2026) [in Ukrainian].



УДК 343

DOI <https://doi.org/10.32782/2311-8040/2026-2-10>**Тищенко Анна Дмитрівна,**

ад'юнкт кафедри кримінального права і кримінології,
Львівський державний університет внутрішніх справ,
вулиця Городоцька, 26, Львів, 79000, Україна
ORCID: <https://orcid.org/0009-0008-6001-147X>

ЮРИДИЧНИЙ АНАЛІЗ СКЛАДУ ЗЛОЧИНУ «ДОМАГАННЯ ДИТИНИ ДЛЯ СЕКСУАЛЬНИХ ЦІЛЕЙ»

Анотація. У науковій статті здійснено комплексний кримінально-правовий аналіз складу злочину «Домагання дитини для сексуальних цілей», передбаченого статтею 156-1 Кримінального кодексу України, з урахуванням імплементації положень Ланцаротської конвенції. Основну увагу зосереджено на визначенні об'єкта кримінального правопорушення, а також на характеристичні його об'єктивних, суб'єктивних ознак та суб'єкта.

Обґрунтовано, що традиційний підхід до визначення основного безпосереднього об'єкта як статевої недоторканості дитини є дискусійним, оскільки дії, передбачені ст. 156-1 КК України, не заподіюють безпосередньої шкоди цьому благу, а лише створюють загрозу її заподіяння. Запропоновано альтернативну позицію, згідно з якою основним безпосереднім об'єктом виступають суспільні відносини у сфері моральності, тоді як статевая недоторканість дитини є обов'язковим додатковим об'єктом.

Проаналізовано особливості об'єктивної сторони складу злочину, який має формальний характер і включає дві обов'язкові дії: пропозицію зустрічі та вчинення хоча б однієї дії, спрямованої на її реалізацію. Встановлено відмінності між положеннями національного законодавства та офіційним перекладом Ланцаротської конвенції, а також доведено, що українська норма точніше відтворює зміст міжнародного акта.

Розкрито ознаки суб'єкта злочину, яким є осудна фізична особа, що досягла 18-річного віку, та аргументовано відсутність підстав для визнання його спеціальним. Окрему увагу приділено проблемі впливу психічних розладів, зокрема педофільї, на кримінальну відповідальність. Досліджено суб'єктивну сторону злочину, яка характеризується прямим умислом і спеціальною метою сексуального характеру або втягнення у виготовлення порнографії.

На підставі аналізу судової практики виявлено проблеми кваліфікації та застосування ст. 156-1 КК України, зокрема відсутність єдності у підходах. Запропоновано конкретні правила кваліфікації залежно від стадії вчинення кримінального правопорушення та реалізації злочинної мети.

Ключові слова: кримінальне правопорушення, кримінальна відповідальність, статевая свобода, статевая недоторканість, домагання дитини, пропозиція зустрічі, дії сексуального характеру, розпусні дії, об'єкт, об'єктивна сторона, суб'єкт, суб'єктивна сторона.

Tyshchenko Anna. LEGAL ANALYSIS OF THE ELEMENTS OF THE CRIMINAL OFFENCE OF "GROOMING A CHILD FOR SEXUAL PURPOSES"

Abstract. The scientific article provides a comprehensive criminal-legal analysis of the elements of the crime of "harassment of a child for sexual purposes" provided for in Article 156-1 of the Criminal Code of Ukraine, taking into account the implementation of the provisions of the Lanzarote Convention. The main attention is focused on determining the object of the criminal offense, as well as on the characteristics of its objective, subjective signs and subject.

It is substantiated that the traditional approach to defining the main direct object as the sexual integrity of the child is debatable, since the actions provided for in Article 156-1 of the Criminal Code of Ukraine do not cause direct harm to this good, but only create a threat of causing it. An alternative position is proposed, according to which the main direct object is social relations in the sphere of morality, while the sexual integrity of the child is a mandatory additional object.

The features of the objective side of the crime, which is formal in nature and includes two mandatory actions: a proposal to meet and the commission of at least one action aimed at its implementation, are analyzed. The differences between the provisions of national legislation and the official translation of the Lanzarote Convention are identified, and it is also proven that the Ukrainian norm more accurately reproduces the content of the international act.

The characteristics of the subject of the crime, which is a sane individual who has reached the age of 18, are revealed, and the lack of grounds for recognizing it as special is argued. Special attention is paid to the problem of the influence of mental disorders, in particular pedophilia, on criminal liability. The subjective side of the crime, which is characterized by direct intent and a special purpose of a sexual nature or involvement in the production of pornography, is investigated.

Based on the analysis of judicial practice, problems of qualification and application of Article 156-1 of the Criminal Code of Ukraine were identified, in particular the lack of unity in approaches. Specific rules of qualification were proposed depending on the stage of committing a criminal offense and the implementation of the criminal purpose.

Key words: criminal offense, criminal liability, sexual freedom, sexual integrity, child molestation, proposal to meet, acts of a sexual nature, lewd acts, object, objective side, subject, subjective side.

Вступ. Війна в Україні, попри усі її жахіття, має і певні позитивні наслідки, одним з яких є ухвалення рішення про надання Україні статусу кандидата на членство в Європейському союзі. Процес набуття Україною членства в Європейському союзі вимагає проведення аналізу розбіжностей між українським та європейським правом та здійснення адаптації законодавства України, в тому числі – кримінального, до права ЄС. І це стосується не лише тих норм, які ще не були імplementовані у вітчизняне законодавство, але й тих, що були раніше впроваджені в українську правову систему, проте із певними розбіжностями чи недосконаlostями.

Зокрема, мова йде про імplementацію положень Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства (Ланцаротської конвенції) у вітчизняне кримінальне законодавство. Одна із новел, спричинена цією імplementацією – це новий склад кримінального правопорушення, який охоплює такі суспільно небезпечні діяння, як: пропозиція зустрічі, зроблена повнолітньою особою, у тому числі з використанням інформаційно-телекомунікаційних систем або технологій, особі, яка не досягла шістнадцятирічного віку, з метою вчинення стосовно неї будь-яких дій сексуального характеру або розпусних дій; а також пропозиція зустрічі, зроблена повнолітньою особою, у тому числі з використанням інформаційно-телекомунікаційних систем або технологій, неповнолітній особі з метою втягнення її у виготовлення дитячої порнографії.

Поява у кримінальному законі норми, якою заборонено ці діяння, породжує низку проблемних питань, таких як неоднотипність

розуміння, тлумачення окремих ознак цього складу злочину; правила кваліфікації та відмежування цього складу злочину від суміжних складів кримінальних правопорушень; і як наслідок – неоднотипність правозастосовної практики у кримінальних провадженнях щодо такого роду діянь.

Метою статті є здійснення комплексного кримінально-правового аналізу складу злочину «Домагання дитини для сексуальних цілей», передбаченого статтею 156-1 Кримінального кодексу України, з урахуванням імplementації положень Ланцаротської конвенції.

Матеріали та методи. Методологічну основу дослідження становить сукупність загальнонаукових та спеціально-юридичних методів пізнання, застосування яких дало змогу всебічно проаналізувати об'єкт, об'єктивну та суб'єктивну сторони, а також суб'єкта складу кримінального правопорушення «Домагання дитини для сексуальних цілей», передбаченого ст. 156-1 КК України.

У процесі дослідження використано діалектичний метод, який дозволив розглянути кримінально-правові явища у їх розвитку, взаємозв'язку та суперечностях, зокрема у контексті співвідношення охорони статевої недоторканості дитини та суспільних відносин моральності. Завдяки цьому методу виявлено дискусійні аспекти визначення основного безпосереднього об'єкта досліджуваного кримінального правопорушення.

Формально-юридичний метод застосовано для аналізу положень Кримінального кодексу України, насамперед статті 156-1, а також суміжних норм, що передбачають відповідальність за злочини проти статевої свободи, статевої недоторканості та моральності. Його

використання дозволило з'ясувати зміст юридичних конструкцій, визначити ознаки складу злочину, момент його закінчення та особливості законодавчої техніки.

Логіко-юридичний метод використано для дослідження внутрішньої узгодженості кримінально-правових норм, зокрема щодо співвідношення об'єкта домагання дитини для сексуальних цілей із родовим об'єктом відповідного розділу Особливої частини КК України. З його допомогою сформульовано аргументи щодо можливого порушення принципу систематизації кримінально-правових норм.

Порівняльно-правовий метод застосовано для зіставлення положень національного кримінального законодавства із нормами міжнародного права, зокрема Ланцаротської конвенції, а також для аналізу різних мовних версій її тексту. Це дозволило виявити розбіжності між офіційним українським перекладом і автентичними текстами Конвенції, а також оцінити відповідність ст. 156-1 КК України міжнародним стандартам.

Системно-структурний метод використано для визначення місця досліджуваного складу злочину в системі кримінального законодавства України, а також для аналізу його взаємозв'язку з іншими кримінально-правовими заборонами. Це дало змогу обґрунтувати висновок щодо можливого неправильного розміщення відповідної норми в Особливій частині КК України.

Емпіричну базу дослідження становлять положення чинного кримінального законодавства України, міжнародно-правові акти, наукові праці вітчизняних і зарубіжних учених, а також узагальнення судової практики щодо застосування ст. 156-1 КК України та суміжних норм.

Застосування зазначених методів у їх сукупності забезпечило комплексний характер дослідження та дозволило сформулювати обґрунтовані висновки щодо особливостей кримінально-правової характеристики домагання дитини для сексуальних цілей.

Результати.

Об'єкт складу злочину «Домагання дитини для сексуальних цілей».

Імплементуючи Ланцаротську конвенцію [1] законодавець помістив норму, яка передбачає відповідальність за домагання дитини для сексуальних цілей, у статті за номером 156-1 наприкінці розділу IV Особливої частини КК України «Кримінальні правопорушення проти статевої свободи та статевої недоторканості особи» [2].

Судячи із розміщення цієї кримінально-правової норми можна зробити висновок, що основним безпосереднім об'єктом цього злочину є статевая недоторканість дітей [3, с. 64]. При цьому, науковці, які дотримуються цієї позиції, додатковим обов'язковим об'єктом визнають нормальний фізичний, психічний і духовний розвиток дітей [4, с. 78].

Проте, таке трактування об'єкта даного кримінального правопорушення видається не безспірним. Адже, у кожній із трьох частин статті 156-1 КК України закріплено відповідальність за «попередню» кримінально-правну діяльність; фактично там мова йде про готування до вчинення інших кримінально-протиправних діянь, зокрема, таких як:

- вчинення розпусних дій чи дій сексуального характеру щодо особи, яка не досягла 16-річного віку (частина 1 статті 156-1 КК України);
- втягнення у виготовлення порнографії неповнолітньої особи (частина 2 статті 156-1 КК України);
- вчинення розпусних дій чи дій сексуального характеру щодо малолітньої особи або втягнення такої особи у виготовлення порнографії (частина 3 статті 156-1 КК України).

Тобто, стаття 156-1 КК України фактично диференціює відповідальність за окремі форми готування до вчинення інших кримінальних правопорушень. До того часу, поки цієї норми не було в КК України, дії, що передбачені нею, кваліфікувались як готування до зґвалтування чи до статевого насильства; до вчинення дій сексуального характеру з особою, яка не досягла шістнадцятирічного віку; до розбещення неповнолітніх; або ж до виготовлення предметів порнографічного характеру; до звідництва для розпусти; до втягнення особи для зайняття проституцією тощо.

Безумовно, пропонуючи дитині таку «зустріч» винний може переслідувати мету порушення її статевої недоторканості. Проте, істотна шкода суспільним відносинам, що охороняють статеву недоторканість дитини, в ході вчинення такої пропозиції не заподіюється. Дії, передбачені ст. 156-1 КК України, лише створюють загрозу заподіяння шкоди статевій недоторканості дитини.

Також, вартим уваги є той факт, що виготовлення дитячої порнографії, проведення видовищного заходу сексуального характеру за участю неповнолітньої особи, звідництво для розпусти, втягнення особи для зайняття проституцією розміщені в розділі XII Особливої частини КК України, а отже, віднесені законодавцем до кримінальних правопорушень проти моральності. І домагання дитини для сексуальних цілей може виступати одним із способів готування до будь-якого з цих злочинів проти моральності.

Послідовне дотримання правила, згідно з яким основний безпосередній об'єкт кримінального правопорушення є частиною його родового об'єкта, приводить до таких висновків:

- основним безпосереднім об'єктом виготовлення дитячої порнографії, примушування неповнолітньої особи до участі у створенні дитячої порнографії є суспільні відносини моральності;

- основним безпосереднім об'єктом домагання дитини з метою втягнення її у виготовлення дитячої порнографії є суспільні відносини з охорони статевої недоторканості особи.

Проте, що ці два висновки явно не є взаємоузгодженими. Тому виникає гіпотеза, що котрась із кримінально-правових норм, що передбачають відповідальність за ці кримінальні правопорушення, розміщена в Особливій частині КК України без дотримання основного критерію її систематизації – родового об'єкта.

Очевидно, що охорона таких відносин, як статевая свобода, статевая недоторканість дуже тісно взаємопов'язана із охороною моральності. Важко уявити суспільно небезпечне діяння, що посягає на статеву недоторканість особи, але при цьому не заподіює шкоду моральності.

Хоча порушити відносини моральності можна і не посягаючи на статеву свободу чи недоторканість іншої особи.

Отже, для з'ясування питання про те, що є основним безпосереднім об'єктом кримінального правопорушення, передбаченого ст. 156-1 КК України, слід зрозуміти, які суспільні відносини порушуються у будь-якому випадку вчинення домагання дитини для сексуальних цілей. В ході пошуку цієї відповіді не варто обмежуватись лише тією групою суспільних відносин, яка зазначена в назві розділу IV Особливої частини КК України.

Як зазначалось вище, дії, передбачені ст. 156-1 КК України, не заподіюють шкоди статевій недоторканості дитини, а лише створюють загрозу заподіяння такої шкоди. Якщо після домагання така шкода буде реально заподіяна, то вона отримає окрему кримінально-правову оцінку і буде кваліфікуватись за іншими нормами, розміщеними в розділі IV Особливої частини КК України (до прикладу, як зґвалтування, сексуальне насильство, розбещення тощо).

Водночас, домагання дитини для сексуальних цілей завжди заподіює шкоду суспільним відносинам моральності. Вчинити це кримінальне правопорушення без посягання на цей об'єкт неможливо. Тому, на мій погляд, основним безпосереднім об'єктом складу такого кримінального правопорушення «Домагання дитини для сексуальних цілей» є суспільні відносини моральності. А отже, кримінально-правова норма, яка закріплює цей склад, була помилково розміщена в розділі IV Особливої частини КК України із порушенням такого критерію систематизації норм Особливої частини, як родовий об'єкт.

Певні зауваження є і щодо такого додаткового об'єкта цього кримінального правопорушення, як нормальний фізичний, психічний і духовний розвиток дітей. Загально визнано, що додатковим об'єктом кримінального правопорушення визнаються ті суспільні відносини, які лежать поза межами його родового об'єкта, але, водночас, «таким об'єктом можуть бути тільки відносини, поставлені законодавцем під охорону закону, інакше кажучи, відносини, ви-

значені як такий об'єкт самим законодавцем» [5, с. 127] (тобто, відносини, які належать до будь-якого іншого родового об'єкта з поміж тих, що охороняються кримінальним законом).

«Нормальний фізичний, психічний і духовний розвиток дітей» серед родових об'єктів, що охороняються чинним кримінальним законом, не перебуває. Сумніви виникають і щодо того, чи здатне домагання дитини для сексуальних цілей заподіяти шкоду нормальному фізичному розвитку цієї дитини. Тому, на наш погляд, єдиним додатковим об'єктом цього кримінального правопорушення є, стаття недоторканість дитини. Цей додатковий об'єкт є обов'язковим, бо у кожному випадку вчинення домагання дитини для сексуальних цілей створюється загроза заподіяння істотної шкоди статевій недоторканості цієї дитини.

Потерпілою від домагання може бути будь-яка дитина, незалежно від статі, зокрема: фізична особа, яка не досягла 16-річного віку (ч. 1 ст. 156-1 КК України), а також фізична особа, яка не досягла 18-річного віку (ч. 2 ст. 156-1 КК України).

Об'єктивна сторона складу злочину «Домагання дитини для сексуальних цілей».

Основний склад аналізованого злочину сконструйовано так – «пропозиція зустрічі, зроблена повнолітньою особою, у тому числі з використанням інформаційно-телекомунікаційних систем або технологій, особі, яка не досягла шістнадцятирічного віку, з метою вчинення стосовно неї будь-яких дій сексуального характеру або розпусних дій, у разі якщо після такої пропозиції було вчинено хоча б одну дію, спрямовану на те, щоб така зустріч відбулася» (частина 1 статті 156-1 КК України) [2].

Така законодавча конструкція дає підстави для висновку про те, що об'єктивна сторона цього складу злочину характеризується двома обов'язковими суспільно небезпечними діями: 1) пропозицією зустрічі; та 2) дією, спрямованою на те, щоб така зустріч відбулася. Окрім того, законодавець зазначає один із можливих способів вчинення пропозиції зустрічі – пропозиція може бути зроблена за допомогою інформаційно-телекомунікаційних систем або технологій.

Цей склад злочину є «формальним» складом, адже не містить такої ознаки об'єктивної сторони, як суспільно небезпечні наслідки. Отож, домагання дитини визнається закінченим з моменту вчинення другого із зазначених вище діянь:

- незалежно від того, чи така зустріч відбулась;

- і незалежно від того, чи було реалізовано мету вчинення щодо потерпілого будь-яких дій сексуального характеру або розпусних дій.

Така конструкція об'єктивної сторони складу кримінального правопорушення є нетиповою для українського кримінального закону. Вочевидь, вона обумовлена прагненням вітчизняного законодавця не стільки імплементувати статтю 23 Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства (Ланцаротської Конвенції), скільки максимально близько скопіювати її текст.

Так, згідно з офіційним перекладом, ця стаття Конвенції закріплює наступне: «Кожна Сторона вживає необхідних законодавчих або інших заходів для забезпечення криміналізації умисної пропозиції, зробленої дорослою людиною за допомогою інформаційно-комунікаційних технологій, зустрітися з дитиною, яка не досягла віку, передбаченого пунктом 2 статті 18 цієї Конвенції, для скоєння проти неї одного з правопорушень, передбачених підпунктом «а» пункту 1 статті 18 або підпунктом «а» пункту 1 статті 20 цієї Конвенції, якщо після цієї пропозиції відбулись істотні дії, що призвели до такої зустрічі» [6]. Аналогічна версія українського перекладу розміщена і на офіційному сайті Ради Європи [7].

Однак, з правового кута зору існує неабияка відмінність між «діями, які призвели до такої зустрічі» та «діями, спрямованими на те, щоб така зустріч відбулася». Ця істотна відмінність полягає у тому моменті, з якого відповідний злочин визнається закінченим: у першому випадку – це момент зустрічі; у другому – момент вчинення дій, спрямованих на таку зустріч.

Отож, слід констатувати, що між офіційним українським перекладом ст. 23 Ланцаротської

конвенції та статтею 156-1 КК України існує очевидна невідповідність. Адже, виходячи із змісту офіційного перекладу цієї конвенційної норми вбачається, що окрім «пропозиції зустрічі» та «дій» повинна відбутись ще й власне «така зустріч».

Водночас, аналіз французького (*lorsque cette proposition a été suivie d'actes matériels conduisant à ladite rencontre* [8]) та англійського (*where this proposal has been followed by material acts leading to such a meeting* [9]) варіантів текстів Ланцаротської конвенції дає підстави стверджувати, що зміст статті 156-1 КК України більш точно відображає положення статті 23 цієї конвенції, аніж її офіційний український переклад.

На стадії прийняття статі 156-1 КК України виявився ще один спірний аспект, а саме – застосування терміну «істотні дії» в тексті офіційного перекладу Конвенції. Законопроект, яким КК України доповнювався аналізованою статтею, у первинній та в доопрацьованій редакції також містив конструкцію «вчинення істотних дій» [10]. Згодом це формулювання зазнало цілком обґрунтованої критики, висловленої Головним науково-експертним управлінням Верховної Ради України [11]; в тексті законопроекту його було замінено конструкцією «вчинено хоча б одну дію».

Вочевидь, україномовний варіант словосполучення «істотні дії» став наслідком невдалого перекладу із англійської мови словосполучення «material acts» (чи з французького «d'actes matériels»). Ці терміни, на наш погляд, у тексті ст. 23 Конвенції вжито на противагу віртуальним пропозиціям, про криміналізацію яких йдеться у цій статті. Логіка цієї норми полягає у тому, що умисні пропозиції зустрічі, здійснені у віртуальному просторі, мають бути поєднані ще й з реальними діями, спрямованими на те, щоб ця зустріч відбулась. Тобто йдеться не про «істотні» дії, а про фактичні, реальні дії.

Ще одна невідповідність проявляється в тому, що в Конвенції мова йде про дії (в множині), а в КК України – хоча б про одну дію. Така відмінність не суперечить вимогам Конвенції і є цілком допустимою, адже україн-

ський законодавець криміналізував домагання дитини для сексуальних цілей навіть за умови, що буде вчинено хоча б одну дію, спрямовану на те, щоб зустріч із потерпілою дитиною відбулась. Таким чином, кримінально-правова норма, закріплена в ст. 156-1 КК України є ще більш суворою, аніж того вимагає ст. 23 Ланцаротської конвенції.

Отож, об'єктивна сторона складу злочину «Домагання дитини для сексуальних цілей» сконструйована у чинному кримінальному законі України, як формальний склад; характеризується двома обов'язковими суспільно небезпечними діями (пропозицією зустрічі та дією, спрямованою на те, щоб така зустріч відбулась); цей злочин вважається закінченим із моменту вчинення другого з них. Хоч законодавець прямо вказав один із можливих способів вчинення такої пропозиції зустрічі (використання інформаційно-телекомунікаційних систем або технологій), спосіб вчинення цього діяння не є обов'язковою ознакою об'єктивної сторони даного складу злочину. Домагання дитини для сексуальних цілей є кримінально-караним діянням, незалежно від того у який спосіб до дитини було донесено відповідну пропозицію зустрічі.

Суб'єкт складу злочину «Домагання дитини для сексуальних цілей».

Суб'єктом домагання дитини для сексуальних цілей є фізична осудна особа, яка на момент вчинення домагання досягла вісімнадцятирічного віку. Відповідно до п. 6 ч. 1 ст. 96-3 КК України, вчинення уповноваженою особою юридичної особи (від імені та в інтересах цієї юридичної особи) злочину, передбаченого ст. 156-1 КК України, є підставою для застосування заходів кримінально-правового характеру до цієї юридичної особи.

Домагання дитини для сексуальних цілей не є гендерно обумовленим злочином, тобто його суб'єктом може виступати як особа чоловічої, так і особа жіночої статі. У той же час, у кримінальному законодавстві Великої Британії визначено, що суб'єктом злочинів проти статевої свободи та статевої недоторканості можуть бути лише особи чоловічої статі, жінка не може бути суб'єктом таких злочинів [12, с. 85].

Зауважимо, що повноліття – не є додатковою ознакою суб'єкта аналізованого злочину. Тому, вести мову про «спеціального суб'єкта» у складі домагання дитини для сексуальних цілей немає підстав. В цьому контексті, цілком обґрунтованою видається позиція, висловлена В.Я. Конопельським та В.О. Меркуловою, які під спеціальним суб'єктом кримінального правопорушення розуміють таку особу, яка має поряд з ознаками фізичної особи – осудністю і віком кримінальної відповідальності – і інші, додаткові ознаки, що передбачені в кримінальному законі або прямо витікають з нього і характеризують соціальну роль та правове положення суб'єкта, стосуються фізичних властивостей суб'єкта, характеризують взаємовідношення суб'єкта з потерпілим і обмежують коло осіб, які можуть бути виконавцями певного кримінального правопорушення [13, с. 142].

Аналіз правозастосовної практики свідчить про те, що доволі поширеними є випадки вчинення домагання тими дорослими особами, які є добре знайомими дитині, що потерпає від домагання (членами сім'ї, родичами, викладачами, керівниками гуртків, тренерами, вихователями дитячих будинків тощо). В науці кримінального права висловлена пропозиція доповнення ч. 3 ст. 156-1 КК України такою кваліфікуючою ознакою, як «вчинення дій членами сім'ї чи близькими родичами, особою, на яку покладено обов'язки щодо виховання потерпілого або піклування про нього» [14, с. 61]. На наш погляд, таке виокремлення спеціального суб'єкта злочину та диференціація кримінальної відповідальності за цієї ознакою є цілком обґрунтованим, оскільки зазначені вище обставини підвищують суспільну небезпечність домагання дитини для сексуальних цілей.

Водночас, при формулюванні даної кваліфікуючої ознаки в тексті кримінального закону видається за доцільне описувати суб'єкта злочину в однині, а не в множині. Адже, буквально тлумачення конструкції «вчинені членами сім'ї або близькими родичами» вимагатиме співучасті хоча б двох осіб, наділених усіма необхідними ознаками суб'єкта цього складу злочину.

Заглиблюючись у проблематику осудності особи, яка вчиняє домагання дитини для сексуальних цілей, варто дослідити питання впливу такого розладу, як педофілія, на кримінальну відповідальність осіб, що мають такий розлад. У сучасній психіатрії педофілія кваліфікується як психічний розлад, при якому дорослий або старший підліток відчуває первинний або винятковий сексуальний потяг до дітей препубертатного віку. Відповідно до МКХ-10 (F65.4) та МКХ-11 (6D32), це стійкий сексуальний потяг до дітей, які ще не досягли статевої зрілості. Варто зазначити, що далеко не кожен злочинець, що вчинив посягання на статеву недоторканість малолітньої жертви має педофільний розлад; з іншого боку – не кожна людина з таким діагнозом скоює статеві злочини.

Вирішення питання про кримінальну відповідальність суб'єкта злочину, що страждає на педофілію, залежить від того, чи визнається ця особа осудною (або обмежено осудною чи неосудною). Якщо злочинець має педофільний розлад, але при цьому він усвідомлює свої дії та може ними керувати, то він вважається осудним і підлягає кримінальній відповідальності. Якщо ж педофілія супроводжується таким психічним розладом, що позбавляє особу можливості усвідомлювати значення своїх дій чи керувати ними, суд може визнати таку особу неосудною, та замість кримінальної відповідальності застосувати до неї примусові заходи медичного характеру. Такі заходи можуть бути застосовані (поряд із призначенням покарання) також у тих випадках, коли особу із педофільним розладом суд визнає обмежено осудною.

З огляду на збереження схильності до рецидиву у тих осіб, які відбули покарання за подібні злочини, доволі гостро постає питання ефективності їх виправлення і ресоціалізації не лише через відбуття покарання. Більшість європейських країн, як і Україна, використовують судово-психіатричну експертизу і застосовують примусове лікування неосудних осіб, у тому числі – тих, що страждають на такий психічний розлад, як педофілія. У деяких країнах Європи (найвідоміший приклад – Республіка

Польща) існують законодавчі механізми, що дозволяють примусове або умовно-примусове застосування гормональної терапії (так званої «хімічної кастрації») для окремих категорій сексуальних злочинців. У Великій Британії також обговорюються програми застосування гормональної терапії в виправних установах (як частина стратегії зниження рецидивів). Деякі європейські держави мають реєстри з обмеженим доступом (поліція, роботодавці у сфері роботи з дітьми), інші країни зберігають подібні дані в закритих правоохоронних базах; у Польщі існують також публічні елементи реєстру (це виняток у європейському контексті). Висуваються та обговорюються пропозиції щодо обміну цією інформацією на рівні ЄС (створення єдиного європейського реєстру для такої категорії злочинців).

В Україні також впроваджено Єдиний реєстр осіб, засуджених за злочини проти статевої свободи та статевої недоторканості малолітньої особи. За умови належного функціонування, реєстр може стати дієвим інструментом попередження рецидиву та забезпечення безпеки дітей – шляхом обмеження доступу осіб, внесених в реєстр, до роботи в закладах, що пов'язані з малолітніми.

Тому запровадження цього реєстру з одного боку, є важливим кроком у протидії повторним правопорушенням, а з іншого боку – на практиці фіксуються певні порушення вимог щодо внесення даних до реєстру, а також відсутній ефективний механізм перевірки кандидатів, що претендують на роботу з дітьми. Законодавчі прогалини створюють умови, за яких потенційно небезпечні особи можуть уникати реального обмеження доступу до дітей. Для ефективного функціонування реєстру, на наш погляд, потрібно запровадити постійну заборону на роботу з дітьми для осіб, внесених до реєстру, а також внести низку змін до чинного законодавства України [15, с. 100–107].

Суб'єктивна сторона складу злочину «Домагання дитини для сексуальних цілей».

Із змісту статті 156-1 КК України випливає, що суб'єктивна сторона тих складів злочинів, що закріплені нею, характеризується виною у формі прямого умислу та метою:

– вчинення стосовно дитини будь-яких дій сексуального характеру або розпусних дій (ч. 1 ст. 156-1 КК України) або

– втягнення її у виготовлення дитячої порнографії (ч. 1 ст. 156-1 КК України).

Висновок про прямий умисел, як єдино можливий вид вини у складі домагання дитини для сексуальних цілей, випливає з того, що мета є обов'язковою ознакою суб'єктивної сторони кожного складу злочину, відповідальність за який встановлена в ст. 156-1 КК України.

Інакше кажучи, для встановлення наявності такого елемента цього складу злочину, як суб'єктивна сторона, потрібно довести, що винна особа усвідомлювала факт вчинення нею дій саме щодо дитини і мала на меті отримати певний сексуально орієнтований результат (включно з виготовленням матеріалів порнографічного характеру).

Щодо усвідомлення винним віку потерпілої особи достатнім є не лише варіант, коли винний достовірно знає вік потерпілої особи, але й той випадок, коли винний міг припустити, що потерпіла особа не досягла 16-річного (ч. 1 ст. 156-1 КК України), 18-річного (ч. 2 ст. 156-1 КК України) чи 14-річного (ч. 3 ст. 156-1 КК України) віку.

Про відсутність прямого умислу на вчинення домагання дитини може свідчити лише сумнінна помилка винного щодо віку потерпілої особи. У цьому контексті релевантною видається наступна правова позиція Верховного суду: «згідно усталеної судової практики кваліфікувати дії особи за ч. 3 ст. 152 КК можливо лише у випадках, коли винний знав та допускав, що вчиняє насильницький статевий акт з неповнолітньою особою, а так само коли він міг і повинен був це передбачити». Мотивуючи своє рішення Касаційний кримінальний суд вказав на те, що суд апеляційної інстанції не перевіряв, чи було враховано місцевим судом зовнішній вигляд потерпілої, її поведінку, показання обвинуваченого, потерпілої, чи було ретельно перевірено їх відповідність усім конкретним обставинам кримінального провадження, оскільки «неповнолітній вік потерпілої не може бути підставою для квалі-

фікації зґвалтування за ч. 3 ст. 152 КК, якщо буде доведено, що обвинувачений сумлінно помилявся щодо фактичного віку потерпілої»; «сам по собі факт неповноліття потерпілої не може бути достатньою підставою для кваліфікації дій за ч. 3 ст. 152 КК». Апеляційний суд також «не дослідив вказані обставини та їх у сукупності про те, чи обвинувачений не міг та не повинен був усвідомлювати, що потерпіла є неповнолітньою» [16].

За цих обставин колегія суддів Верховного Суду вирішила, що апеляційний розгляд кримінального провадження було здійснено без належної перевірки наведених у апеляційній скарзі захисника доводів та надання обґрунтованих відповідей на них, в зв'язку з чим ухвала апеляційного суду була визнана такою, що не відповідає вимогам статей 370, 419 КПК.

Отже, висновок про те, чи міг та чи повинен був винний усвідомлювати вік особи, якій він робив пропозицію зустрічі з сексуальною метою, повинен ґрунтуватись на всебічному та повному аналізі усіх обставин вчинення діяння (а не лише на показах винного). Зокрема, про вік потерпілої особи можуть свідчити:

зовнішній вигляд і поведінка потерпілої особи, які не давали (або давали) підстави вважати її повнолітньою; відповідність показань обвинуваченого тим показанням, які дає потерпіла особа або треті особи; їх відповідність іншим доказам у справі; інші матеріали справи, що дають підстави для висновку про сумнісність (несумнісність) помилки винного щодо віку потерпілої особи.

Повертаючись до такої ознаки суб'єктивної сторони досліджуваного складу злочину, як мета, варто зауважити наступне. Вказівка на ті дві мети, що зазначені в частині 1 та в частині 2 статті 156-1 КК України, фактично закріплює такий стан речей, за якого домагання дитини – це готування до вчинення інших злочинів проти статевої недоторканості дитини або злочинів проти моральності.

На практиці цей стан речей призводить до того, що стаття 156-1 КК України самостійно (без сукупності з іншими кримінально-правовими нормами) не застосовується [17, с. 360–365]. Досить проблемним видасть-

ся також процес виявлення, а тим паче – доведення самого лише факту домагання дитини, якщо надалі винна особа не реалізувала мету вчинення стосовно цієї дитини будь-яких дій сексуального характеру або розпусних дій або ж мету втягнення її у виготовлення дитячої порнографії.

За умов, коли пропозиція зустрічі за своїм змістом прямо не вказувала на мету, а лише якимось чином натякала на неї, або ж непрямо давала підстави вважати, що той, хто пропонує зустріч, переслідує власне «сексуальну, розпусну чи порнографічну» мету, практично неможливо довести ЩО САМЕ мала на меті особа, висловлюючи таку пропозицію. Тому в судовій практиці обвинувальні вирoki за ст. 156-1 КК України виносяться лише в тих випадках, коли відбулась не лише пропозиція зустрічі, але й сама зустріч, і на додаток – ще якийсь злочин, в ході якого, власне, і була реалізована «сексуальна, розпусна чи порнографічна» мета злочинця.

Водночас, аналіз судової практики в справах про зґвалтування, сексуальне насильство, розбещення, вчинені щодо неповнолітніх осіб, засвідчив відсутність єдності в підходах до застосування / не застосування статті 156-1 КК України. Часто дії винних осіб, які спершу вчинили домагання дитини для сексуальних цілей (запропонували дитині відповідну зустріч), а згодом вчинили щодо цієї ж дитини зґвалтування, сексуальне насильство чи розбещення, кваліфікуються лише відповідно за ст. 152, 153 чи 156 КК України, БЕЗ сукупності з ст. 156-1 КК України [18].

Для єдності правозастосування статті 156-1 КК України, пропонуємо застосовувати такі правила кваліфікації:

1) коли дії винного були припинені на етапі домагання, а мета домагання – вчинення будь-яких дій сексуального характеру або розпусних дій, або втягнення її у виготовлення дитячої порнографії – не була реалізована, кваліфікувати дії винної особи слід лише за відповідною частиною статті 156-1 КК України;

2) коли, крім домагання дитини для сексуальних цілей, винний вчинив ще й інші

підготовчі дії (знайшов співучасників для виготовлення дитячої порнографії; підшукав приміщення для цього; створив інші умови для вчинення кримінальних правопорушень, передбачених ст. 152, 153, 155, 156, 301-1 КК України) і його дії були припинені на стадії готування до якогось із цих злочинів, кваліфікація має здійснюватись за сукупністю відповідної частини ст. 156-1 КК України та ч. 1 ст. 14 і тою статтею Особливої частини КК України, що передбачає злочин, до вчинення якого готувався винний;

3) коли дії винного припинено на стадії замаху на злочини, передбачені ст. 152, 153, 155, 156, 301-1 КК України, якщо їм передувало домагання дитини для сексуальних цілей, кваліфікувати дії винного слід за сукупністю ст. 156-1 КК України та відповідної частини статті 15 КК і тієї статті Особливої частини КК України, яка передбачає злочин, замах на вчинення якого мав місце;

4) якщо домагання дитини для сексуальних цілей передувало вчиненню закінчених кримінальних правопорушень, передбачених ст. 152, 153, 155, 156, 301-1 КК України, кваліфікувати дії винного також слід за сукупністю ст. 156-1 КК України та відповідної статті Особливої частини КК України (ст. 152, 153, 155, 156, чи 301-1 КК України).

Висновки. Основним безпосереднім об'єктом складу «Домагання дитини для сексуальних цілей» є суспільні відносини моральності; кримінально-правова норма, яка закріплює цей склад, була помилково розміщена в розділі IV Особливої частини КК України із порушенням такого критерію систематизації норм Особливої частини, як родовий об'єкт; додатковим об'єктом цього кримінального правопорушення є статева недоторканість дитини.

Об'єктивна сторона складу злочину «Домагання дитини для сексуальних цілей» сконструйована як формальний склад; характеризується двома обов'язковими суспільно не-

безпечними діями (пропозицією зустрічі та дією, спрямованою на те, щоб така зустріч відбулася); цей злочин вважається закінченим із моменту вчинення другого з них; спосіб вчинення цього діяння (використання інформаційно-телекомунікаційних систем або технологій), не є обов'язковою ознакою об'єктивної сторони даного складу злочину.

Суб'єктом злочину домагання дитини для сексуальних цілей є фізична, осудна особа, незалежно від статі, що досягла 18 років. Вирішення питання про кримінальну відповідальність суб'єкта злочину, що страждає на педофілію, залежить від того, чи визнається ця особа осудною (або обмежено осудною чи неосудною). Кримінальний закон не диференціює кримінальну відповідальність за такі домагання залежно від ознак суб'єкта. У той же час, вчинення такого роду діянь особами, які беруть участь у вихованні дітей, чи піклуванні про них, за ступенем суспільної небезпечності суттєво відрізняються від домагань, вчинених «загальними» суб'єктами. Тому видається обґрунтованою пропозиція про доповнення ст. 156-1 КК такою кваліфікуючою ознакою, як «вчинення членом сім'ї чи близьким родичем, або особою, на яку покладено обов'язки щодо виховання потерпілого або піклування про нього».

Суб'єктивна сторона «Домагання дитини для сексуальних цілей» характеризується виною у формі прямого умислу та спеціальною метою – вчинення стосовно дитини будь-яких дій сексуального характеру або розпусних дій (ч. 1 ст. 156-1 КК України) або ж втягнення її у виготовлення дитячої порнографії (ч. 1 ст. 156-1 КК України). Віднесення цих двох видів мети до конструктивних ознак суб'єктивної сторони створює проблеми в правозастосовній практиці та призводить до різнотлумачень. Для єдності правозастосування запропоновано правила кваліфікації дій особи, яка вчинила домагання дитини для сексуальних цілей.

Список використаних джерел:

1. Про внесення змін до деяких законодавчих актів України щодо імплементації Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства (Ланцаротської конвенції): закон України від 18 лютого 2021 року № 1256-IX. URL: <https://zakon.rada.gov.ua/laws/show/1256-20#n24>

2. Кримінальний кодекс України від 05.04.2001 року № 2341-III. URL: <https://zakon.rada.gov.ua/laws/show/2341-14/conv#n1263>
3. Сенько В. Аналіз складу кримінального правопорушення за статтею 156-1 Кримінального кодексу України. *Науково-практичний журнал «Екологічне право»*. 2022. Випуск 3-4. С. 63–66. <https://doi.org/10.31733/2078-3566-2022-4-427-432>
4. Куковинець Д.О. Захист дітей від сексуальної експлуатації та сексуального насильства в інтернеті в умовах пандемії Covid-19: до питання домагання дитини для сексуальних цілей. *Питання боротьби зі злочинністю*. 2021. Випуск 42. С. 74–83. <https://doi.org/10.31359/2079-6242-2021-42-74>
5. Кримінальне право України: Загальна частина: підручник. За ред. В.Я. Тація, В.І. Тютюгіна, В.І. Борисова. Харків, 2020. 584 с.
6. Конвенція Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства (Ланцаротська Конвенція). URL: https://zakon.rada.gov.ua/laws/show/994_927#n91
7. Texte de la Convention en plusieurs langues. Ukrainien. URL: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168046e1df>
8. Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels (Convention de Lanzarote). URL: <https://rm.coe.int/la-protection-des-enfants-contre-l-exploitation-et-les-abus-sexuels-co/1680794e98>
9. Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention). URL: <https://rm.coe.int/protection-of-children-against-sexual-exploitation-and-sexual-abuse/1680794e97>
10. Порівняльна таблиця до проекту Закону України (реєстраційний № 3055) про внесення змін до деяких законодавчих актів України щодо імплементації Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства (Ланцаротської Конвенції). Друге читання. URL: <https://itd.rada.gov.ua/billInfo/Bills/pubFile/443338>
11. Висновок Головного науково-експертного управління Апарату Верховної Ради України на проект Закону України «Про внесення змін до деяких законодавчих актів України щодо імплементації Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства». URL: <https://itd.rada.gov.ua/billInfo/Bills/pubFile/50172>
12. Кримінальне право України і Англії: порівняльний аналіз (окремі питання Загальної частини): конспект лекцій для студентів II курсу першого (бакалаврського) рівня вищої освіти галузі знань 29 «Міжнародні відносини» спеціальності 293 «Міжнародне право» / уклад.: М. І. Панов, С. О. Харитонов, Ю. П. Дзюба та ін. 2-ге електрон. вид., перероб. та допов. Харків : Нац. юрид. ун-т ім. Ярослава Мудрого, 2021. 144 с.
13. Кримінальне право України. Загальна частина : підручник / за заг. ред. В.Я. Конопельського, В.О. Меркулової. Одеса : ОДУВС, 2021. 452 с.
14. Литвин А.С., Бугрик А.В., Дубіна М.П. Питання про грумінг та кримінальну відповідальність за нього. *Трибуна молодого науковця. Правова позиція*. Харків, 2022. №3 (36). С. 58–62. <https://doi.org/10.32782/2521-6473.2022-3.12>
15. Тищенко А.Д. Єдиний реєстр осіб, засуджених за злочини проти статевої недоторканості малолітніх: між законодавчим задумом і реальністю правозастосування. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична*. 2025. № 2. С. 100–107. <https://doi.org/10.32782/2311-8040/2025-2-14>
16. Постанова Касаційного кримінального суду Верховного Суду від 5 липня 2023 року у справі № 172/1359/17. *Єдиний державний реєстр судових рішень*. URL: <https://reyestr.court.gov.ua/Review/112146270>
17. Тищенко А.Д. Судова практика в справах про домагання дитини для сексуальних цілей. *Європеїзація кримінального права України: матеріали міжнародної наукової конференції (19 грудня 2024 року)*. Харків : Право, 2025. С. 360–365.
18. Вирок Вознесенського міськрайонного суду Миколаївської області від 15.11.2024 р. Справа № 473/4012/24. URL: <https://opendatabot.ua/court/123029038-ae0dd27a81788e9fde83f4f7670ca42b>

References:

1. Pro vnesennia zmin do deiakykh zakonodavchykh aktiv Ukrainy shchodo implementatsii Konventsii Rady Yevropy pro zakhyst ditei vid seksualnoi ekspluatatsii ta seksualnogo nasylstva (Lantsarotskoi konventsii): Zakon Ukrainy [On Amendments to Certain Legislative Acts of Ukraine Regarding the Implementation of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and

Sexual Abuse (Lanzarote Convention): Law of Ukraine] vid 18 liutoho 2021 roku № 1256-IX. Retrieved from <https://zakon.rada.gov.ua/laws/show/1256-20#n24> [in Ukrainian].

2. Kryminalnyi kodeks Ukrainy [Criminal Code of Ukraine] vid 05.04.2001 roku № 2341-III. Retrieved from <https://zakon.rada.gov.ua/laws/show/2341-14/conv#n1263> [in Ukrainian].

3. Senko, V. (2022). Analiz skladu kryminalnogo pravoporushennia za statteiu 156-1 Kryminalnogo kodeksu Ukrainy [Analysis of the composition of a criminal offense under Article 156-1 of the Criminal Code of Ukraine]. *Naukovo-praktychnyi zhurnal «Ekologichne pravo» – Scientific and Practical Journal “Ecological Law”*, 3–4, 63–66. <https://doi.org/10.31733/2078-3566-2022-4-427-432> [in Ukrainian].

4. Kukovynets, D.O. (2021). Zakhyst ditei vid seksualnoi ekspluatatsii ta seksualnogo nasylstva v interneti v umovakh pandemii Covid-19: do pytannia domahannia dytyny dlia seksualnykh tsilei [Protecting children from sexual exploitation and sexual abuse online during the Covid-19 pandemic: addressing the issue of child sexual abuse]. *Pytannia borotby zi zlochynnistiu – Issues of combating crime*, 42, 74–83. <https://doi.org/10.31359/2079-6242-2021-42-74> [in Ukrainian].

5. Tatsii, V.Ya., Tiutiuhin, V.I., & Borysov, V.I. (2020). Kryminalne pravo Ukrainy: Zahalna chastyna: pidruchnyk [Criminal Law of Ukraine: General Part: Textbook]. Kharkiv. 584 s.

6. Konventsiiia Rady Yevropy pro zakhyst ditei vid seksualnoi ekspluatatsii ta seksualnogo nasylstva (Lantsarotska Konventsiiia) [Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention)]. Retrieved from https://zakon.rada.gov.ua/laws/show/994_927#n91 [in Ukrainian].

7. Texte de la Convention en plusieurs langues. Ukrainien [Text of the Convention in several languages. Ukrainian]. (n.d.). Retrieved from <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMCContent?documentId=090000168046e1df> [in French].

8. Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels (Convention de Lanzarote) [Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention)]. (n.d.). Retrieved from <https://rm.coe.int/la-protection-des-enfants-contre-l-exploitation-et-les-abus-sexuels-co/1680794e98> [in French].

9. Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention). (n.d.). Retrieved from <https://rm.coe.int/protection-of-children-against-sexual-exploitation-and-sexual-abuse/1680794e97> [in English].

10. Porivnialna tablytsia do proektu Zakonu Ukrainy (reiestratsiinyi № 3055) pro vnesennia zmin do deiakykh zakonodavchykh aktiv Ukrainy shchodo implementatsii Konventsii Rady Yevropy pro zakhyst ditei vid seksualnoi ekspluatatsii ta seksualnogo nasylstva (Lantsarotskoi Konventsii). Druhe chytannia [Comparative table to the draft Law of Ukraine (registration number 3055) on amendments to certain legislative acts of Ukraine regarding the implementation of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention). Second reading]. Retrieved from <https://itd.rada.gov.ua/billInfo/Bills/pubFile/443338> [in Ukrainian].

11. Vysnovok Holovnoho naukovo-ekspertnoho upravlinnia Aparatu Verkhovnoi Rady Ukrainy na proekt Zakonu Ukrainy «Pro vnesennia zmin do deiakykh zakonodavchykh aktiv Ukrainy shchodo implementatsii Konventsii Rady Yevropy pro zakhyst ditei vid seksualnoi ekspluatatsii ta seksualnogo nasylstva» [Opinion of the Main Scientific and Expert Department of the Apparatus of the Verkhovna Rada of Ukraine on the draft Law of Ukraine “On Amendments to Certain Legislative Acts of Ukraine Regarding the Implementation of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse”]. Retrieved from <https://itd.rada.gov.ua/billInfo/Bills/pubFile/50172> [in Ukrainian].

12. Panov, M. I., Kharytonov, S. O., & Dziuba, Yu. P. et al. (2021). Kryminalne pravo Ukrainy i Anhlii: porivnialnyi analiz (okremi pytannia Zahalnoi chastyny): konspekt leksii dlia studentiv II kursu pershoho (bakalavrskoho) rivnia vyshchoi osvity haluzi znan 29 «Mizhnarodni vidnosyny» spetsialnosti 293 «Mizhnarodne pravo» [Criminal law of Ukraine and England: comparative analysis (separate questions of the General part): lecture notes for students of the 2nd year of the first (bachelor's) level of higher education in the field of knowledge 29 “International Relations” of the specialty 293 “International Law”]. 2-he elektron. vyd., pererob. ta dopov. Kharkiv: Nats. yuryd. un-t im. Yaroslava Mudroho. 144 s. [in Ukrainian].

13. Konopelsko, V.Ya., & Merkulova, V.O. (2021). Kryminalne pravo Ukrainy. Zahalna chastyna : pidruchnyk [Criminal law of Ukraine. General part: textbook]. Odesa : ODUVS. 452 s. [in Ukrainian].

14. Lytvyn, A.S., Buhryk, A.V., & Dubina, M.P. (2022). Pytannia pro hruminh ta kryminalnu vidpovidalnist za noho [The issue of grooming and criminal liability for it]. *Trybuna molodoho naukotsia. Pravova pozytsiia – Tribune of a young scientist. Legal position*, 3 (36), 58–62. <https://doi.org/10.32782/2521-6473.2022-3.12> [in Ukrainian].

15. Tyshchenko, A.D. (2025). Yedynyi reiestr osib, zasudzhenykh za zlochyny proty statevoi nedotorkanosti malolitnykh: mizh zakonodavchym zadumom i realnistiu pravozastosuvannia [Unified register of persons convicted of crimes against the sexual integrity of minors: between legislative intent and the reality of law enforcement]. *Naukovyi visnyk Lvivskoho derzhavnoho universytetu vnutrishnikh sprav. Seriia yurydychna – Scientific Bulletin of the Lviv State University of Internal Affairs. Legal Series*, 2, 100–107. <https://doi.org/10.32782/2311-8040/2025-2-14> [in Ukrainian].

16. Postanova Kasatsiinoho kryminalnoho sudu Verkhovnoho Sudu vid 5 lypnia 2023 roku u spravi № 172/1359/17. Yedynyi derzhavnyi reiestr sudovykh rishen [Resolution of the Cassation Criminal Court of the Supreme Court of July 5, 2023 in case No. 172/1359/17. Unified State Register of Court Decisions.]. Retrieved from <https://reyestr.court.gov.ua/Review/112146270> [in Ukrainian].

17. Tyshchenko, A.D. (2025). Sudova praktyka v spravakh pro domahannia dytyny dlia seksualnykh tsilei [Judicial practice in cases of child molestation for sexual purposes]. *Yevropeizatsiia kryminalnoho prava Ukrainy: materialy mizhnarodnoi naukovoï konferentsii (19 hrudnia 2024 roku) – Europeanization of criminal law of Ukraine: materials of the international scientific conference (December 19, 2024))*. Kharkiv : Pravo. S. 360–365. [in Ukrainian].

18. Vyroky Voznesenskoho miskraionnoho sudu Mykolaivskoi oblasti vid 15.11.2024r. Sprava № 473/4012/24 [Verdict of the Voznesenskyi City District Court of Mykolaiv Region dated 11/15/2024. Case No. 473/4012/24]. Retrieved from <https://opendatabot.ua/court/123029038-ae0dd27a81788e9fde83f4f7670ca42b> [in Ukrainian].

Дата першого надходження статті до видання: 28.07.2026

Дата прийняття статті до друку після рецензування: 08.09.2026

Дата публікації (оприлюднення) статті: 00.00.2026

УДК 351.74:351.86:338.49(477)

DOI <https://doi.org/10.32782/2311-8040/2026-2-11>

Умрихіна Ірина Олександрівна,

доктор філософії в галузі права, доцент,
завідувач кафедри адміністративно-правових дисциплін
факультету підготовки фахівців для підрозділів превентивної
діяльності Національної поліції України,
Донецький державний університет внутрішніх справ,
вулиця Велика Перспективна, 1, Кропивницький, 25015, Україна
ORCID: <https://orcid.org/0009-0003-9041-5831>

Тишлек Микола Миколайович,

доктор філософії в галузі права,
доцент кафедри адміністративного права та процесу
Навчально-наукового інституту права та соціального менеджменту,
Донецький державний університет внутрішніх справ,
вулиця Велика Перспективна, 1, Кропивницький, 25015, Україна
ORCID: <https://orcid.org/0009-0001-7221-6519>

Чепеляк Віталій Степанович,

викладач кафедри адміністративно-правових дисциплін
факультету підготовки фахівців для підрозділів превентивної
діяльності Національної поліції України,
Донецький державний університет внутрішніх справ,
вулиця Велика Перспективна, 1, Кропивницький, 25015, Україна
ORCID: <https://orcid.org/0009-0009-4281-7936>

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ТА СТІЙКОСТІ ФУНКЦІОНУВАННЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЯК ПРІОРИТЕТНИЙ НАПРЯМ ПУБЛІЧНОЇ БЕЗПЕКИ

***Анотація.** У статті обґрунтовано, що захист і стійкість критичної інфраструктури мають розглядатися як один із пріоритетних напрямів забезпечення публічної безпеки. Підкреслено, що безперервна робота об'єктів критичної інфраструктури безпосередньо впливає на безпеку населення, стабільність публічного управління, реалізацію прав і свобод людини та здатність держави ефективно діяти в умовах кризи. Розкрито зміст понять безпеки та стійкості критичної інфраструктури, а також показано їх тісний взаємозв'язок. Окрему увагу приділено взаємозалежності секторів критичної інфраструктури та каскадному характеру сучасних загроз, коли порушення роботи одного об'єкта може спричинити збої в інших сферах. Це зумовлює необхідність застосування комплексного, багаторівневого та ризик-орієнтованого підходу до організації захисту. Проаналізовано роль Національної поліції України та інших суб'єктів національної системи захисту критичної інфраструктури. Наголошено, що діяльність поліції у цій сфері не повинна обмежуватися реагуванням на вже вчинені правопорушення, а має включати оцінювання загроз, превентивну роботу, участь у спільному плануванні та навчаннях, евакуації населення, обмеженні доступу до небезпечних зон, забезпеченні публічного порядку й супроводженні аварійно-відновлювальних заходів. Обґрунтовано необхідність удосконалення міжвідомчого інформаційного обміну, розроблення типових алгоритмів реагування, розвитку публічно-приватного партнерства, посилення спроможності територіальних громад і впровадження спільної професійної підготовки залучених суб'єктів. Зроблено висновок, що захист і стійкість критичної інфраструктури є не лише технічним або оборонним завданням, а комплексним напрямом публічної безпеки, від якого залежать захищеність населення, підтримання правопорядку, доступ до життєво важливих послуг і здатність державних інституцій виконувати свої функції в кризових умовах.*

***Ключові слова:** критична інфраструктура, публічна безпека, стійкість, безпека, життєво важливі послуги, управління ризиками, Національна поліція, міжвідомча взаємодія.*

Umrykhina Iryna, Tyshlek Mykola, Chepeliak Vitalii. ENSURING THE PROTECTION AND RESILIENCE OF CRITICAL INFRASTRUCTURE AS A PRIORITY AREA OF PUBLIC SAFETY

Abstract. The article argues that the protection and resilience of critical infrastructure should be considered one of the priority areas for ensuring public safety. It emphasizes that the uninterrupted operation of critical infrastructure facilities directly affects public safety, the stability of public administration, the realization of human rights and freedoms, and the state's ability to act effectively in times of crisis. The article explores the concepts of security and resilience of critical infrastructure and demonstrates their close interconnection. Particular attention is paid to the interdependence of critical infrastructure sectors and the cascading nature of modern threats, where a disruption at one facility can cause failures in other areas. This necessitates a comprehensive, multi-level, and risk-based approach to organizing protection. The role of the National Police of Ukraine and other entities within the national critical infrastructure protection system is analyzed. It is emphasized that police activities in this area should not be limited to responding to offenses that have already been committed, but should include threat assessment, preventive measures, participation in joint planning and exercises, evacuation of the population, restricting access to hazardous areas, maintaining public order, and supporting emergency response and recovery operations. The paper justifies the need to improve interagency information exchange, develop standard response protocols, foster public-private partnerships, strengthen the capacity of local communities, and implement joint professional training for the relevant stakeholders. It is concluded that the protection and resilience of critical infrastructure is not merely a technical or defense-related task, but a comprehensive aspect of public safety upon which the security of the population, the maintenance of law and order, access to vital services, and the ability of state institutions to perform their functions in crisis conditions depend.

Key words: critical infrastructure, public safety, resilience, security, essential services, risk management, National Police, interagency cooperation.

Вступ. Сучасний етап розвитку української держави характеризується істотним ускладненням безпекового середовища, поєднанням воєнних, терористичних, диверсійних, техногенних, природних, інформаційних та кібернетичних загроз. За таких умов нормальне функціонування держави, територіальних громад, економіки та суспільства значною мірою залежить від здатності забезпечувати безперервне надання життєво важливих послуг, підтримувати керованість публічних процесів і швидко відновлювати пошкоджені системи. Саме тому безпека та стійкість критичної інфраструктури набувають значення не лише окремого напрямку державної політики у сфері національної безпеки, а й одного з визначальних складників публічної безпеки.

Актуальність дослідження посилюється тим, що порушення функціонування енергетичних об'єктів, систем водопостачання і водовідведення, транспортної інфраструктури, електронних комунікацій, закладів охорони здоров'я, органів державного управління, правоохоронних і рятувальних служб може спричинити каскадні наслідки. Відмова одного об'єкта або сектору здатна негативно вплинути на роботу інших взаємопов'язаних систем, призвести до погіршення умов життєдіяль-

ності населення, виникнення надзвичайних ситуацій, дестабілізації громадського порядку, обмеження доступу громадян до основних публічних послуг та зниження рівня довіри до державних інституцій. Відповідно, захист критичної інфраструктури має розглядатися не як сукупність відокремлених охоронних заходів, а як комплексна, багаторівнева та безперервна діяльність, спрямована на запобігання загрозам, забезпечення готовності, реагування, адаптацію і відновлення.

Проблеми визначення сутності критичної інфраструктури, формування національної системи її захисту, оцінювання загроз і забезпечення стійкості досліджували Д.С. Бірюков, О.М. Суходоля, М.О. Кизим, В.Є. Хаустова, Н.В. Трушкіна, Л.А. Арсенович, А.Т. Ковальчук та інші вітчизняні науковці.

Д.С. Бірюков одним із перших обґрунтував необхідність переходу від фрагментарної охорони окремих стратегічних об'єктів до формування комплексної державної політики захисту критичної інфраструктури, яка повинна ґрунтуватися на міжвідомчій координації, оцінюванні ризиків, державно-приватній взаємодії та врахуванні взаємозалежності різних інфраструктурних секторів [1, с. 168–169].

М.О. Кизим, В.Є. Хаустова та Н.В. Трушкіна досліджують критичну інфраструктуру як багаторівневу соціально-економічну та технічну систему, від безперервності функціонування якої залежать життєздатність держави, сталість економічного розвитку й рівень національної безпеки. Науковці звертають увагу на складність внутрішніх і зовнішніх зв'язків критичної інфраструктури, а також на необхідність урахування функціонального, секторального, просторового та безпекового вимірів цього поняття [2, с. 66].

Л.А. Арсенович, аналізуючи захист критичної інфраструктури в системі національної безпеки України, наголошує на необхідності формування дієвого алгоритму управління всією сукупністю критично важливих систем, об'єктів і ресурсів. На думку автора, моделі, розраховані переважно на умови мирного часу, не можуть повною мірою забезпечувати захист критичної інфраструктури під час воєнного стану, що потребує посилення координації суб'єктів, удосконалення оцінювання загроз та розвитку державно-приватного партнерства [3].

А.Т. Ковальчук досліджує сучасний стан правового регулювання захисту об'єктів критичної інфраструктури та звертає увагу на потребу узгодження галузевих нормативно-правових актів, конкретизації компетенції суб'єктів національної системи захисту критичної інфраструктури й нормативного визначення ролі правоохоронних органів у цій сфері. Важливою є позиція щодо доцільності більш чіткого закріплення захисту критичної інфраструктури серед напрямів діяльності Національної поліції України [4, с. 172].

Серед зарубіжних дослідників вагомий внесок у формування теоретичних засад стійкості критичної інфраструктури зробили М. Бруно (M. Bruneau) та І. Лінков (I. Linkov). Запропоновані ними підходи дають змогу розглядати стійкість не лише як здатність об'єкта протистояти певній загрозі, а як комплексну властивість інфраструктурної системи, що охоплює збереження її основних функцій, адаптацію до змінених умов та відновлення після деструктивного впливу [5, с. 741; 6].

У вітчизняній науковій літературі достатньо ґрунтовно розроблено питання визначення поняття і структури критичної інфраструктури, класифікації загроз, формування нормативно-правового механізму її захисту, управління ризиками, кібербезпеки, міжвідомчої координації, інженерно-технічного захисту та участі територіальних громад. Водночас недостатньо дослідженим залишається місце забезпечення безпеки й стійкості критичної інфраструктури саме в системі публічної безпеки. Потребують подальшого наукового опрацювання зміст і форми участі Національної поліції України, органів місцевого самоврядування та інших суб'єктів публічної безпеки у запобіганні інцидентам, підтриманні правопорядку в умовах припинення життєво важливих послуг, захисті населення, обміні інформацією та кризовому реагуванні.

Метою статті є теоретико-правове обґрунтування забезпечення безпеки та стійкості функціонування критичної інфраструктури як пріоритетного напрямку публічної безпеки, визначення взаємозв'язку між безперервністю надання життєво важливих послуг і станом захищеності населення, а також розроблення пропозицій щодо вдосконалення організаційно-правового механізму взаємодії органів публічної влади, Національної поліції України, інших правоохоронних і рятувальних органів, територіальних громад та операторів критичної інфраструктури.

Матеріали та методи. Матеріалами дослідження стали положення законодавства України у сфері захисту критичної інфраструктури, публічної та національної безпеки, діяльності правоохоронних органів і цивільного захисту, а також наукові праці Д.С. Бірюкова, М.О. Кизима, В.Є. Хаустової, Н.В. Трушкіної, Л.А. Арсеновича, А.Т. Ковальчука, М. Бруно, І. Лінкова.

Методологічну основу дослідження становить сукупність загальнонаукових і спеціально-правових методів. Системний метод використано для розгляду критичної інфраструктури як багаторівневої та взаємопов'язаної системи. Формально-юридичний метод дав змогу проаналізувати нормативні положення

та повноваження суб'єктів її захисту. За допомогою структурно-функціонального методу визначено роль Національної поліції України та інших суб'єктів національної системи захисту критичної інфраструктури. Методи аналізу, синтезу та узагальнення застосовано для систематизації загроз і формулювання пропозицій щодо вдосконалення міжвідомчої взаємодії, управління ризиками та кризового реагування.

Результати. Публічна безпека є складною правовою і соціально-управлінською категорією, зміст якої не може обмежуватися лише охороною громадського порядку, запобіганням правопорушенням або реагуванням на них. У широкому розумінні вона характеризує стан захищеності людини, суспільства, територіальних громад і держави від загроз, за якого забезпечуються належні умови життєдіяльності населення, реалізація прав і свобод людини, стабільне функціонування органів публічної влади та можливість отримання основних суспільно необхідних послуг.

За такого підходу публічна безпека безпосередньо залежить від належного функціонування енергетичних систем, об'єктів водопостачання й водовідведення, транспорту, електронних комунікацій, закладів охорони здоров'я, фінансових установ, органів державного управління, правоохоронних і рятувальних служб. Вихід із ладу відповідних об'єктів створює не тільки економічні або технічні проблеми, а й загрози правам людини, громадському порядку, соціальній стабільності та керованості суспільних процесів. Тому забезпечення безпеки критичної інфраструктури слід розглядати як невід'ємний елемент сучасної системи публічної безпеки.

Закон України «Про критичну інфраструктуру» визначає правові й організаційні засади створення та функціонування національної системи захисту критичної інфраструктури та відносить відповідне законодавство до сфери національної безпеки. Безпека критичної інфраструктури визначається як стан її захищеності, за якого забезпечуються функціональність, безперервність роботи, відновлюваність, цілісність і стійкість. Сама критична інфра-

структура являє собою сукупність об'єктів, систем, їх частин і комплексів, важливих для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам [7].

Законодавче визначення свідчить, що безпека критичної інфраструктури охоплює не тільки недопущення фізичного пошкодження або несанкціонованого проникнення на об'єкт. Її обов'язковими ознаками є функціональність, безперервність, цілісність, відновлюваність і стійкість. Отже, стан безпеки повинен оцінюватися передусім за здатністю відповідного об'єкта чи системи виконувати призначені функції та забезпечувати надання життєво важливих послуг навіть за умов негативного впливу.

Стійкість критичної інфраструктури законодавець визначає як стан, за якого забезпечується її спроможність функціонувати у штатному режимі, адаптуватися до умов, що постійно змінюються, протистояти та швидко відновлюватися після впливу загроз будь-якого виду [7]. Відповідна категорія відображає динамічний аспект безпеки. Якщо захищеність характеризує переважно здатність не допустити або мінімізувати реалізацію загрози, то стійкість означає спроможність системи продовжувати виконання основних функцій, пристосовуватися до змінених умов та відновити належні параметри діяльності після інциденту.

У сучасному безпековому середовищі абсолютне запобігання всім загрозам практично неможливе. Особливо це стосується умов воєнного стану, коли об'єкти критичної інфраструктури можуть зазнавати систематичних і комбінованих впливів. Тому державна політика повинна орієнтуватися не лише на запобігання інцидентам, а й на підтримання мінімально необхідного рівня функціональності, резервування основних ресурсів, визначення альтернативних способів надання послуг та скорочення строків відновлення.

Зміст стійкості доцільно розглядати через сукупність взаємопов'язаних спроможностей: прогнозувати можливі загрози; запобігати їх реалізації; витримувати негативний вплив без

повної втрати функціональності; адаптувати організаційні й технологічні процеси до змінених умов; оперативно реагувати на інцидент; відновлювати основні функції та враховувати отриманий досвід у подальшому плануванні. Такий підхід відповідає сучасному розумінню резильєнтності як здатності складної системи не лише протистояти деструктивному впливу, а й змінюватися з урахуванням нових ризиків.

На думку авторського колективу, критична інфраструктура має розглядатися як складна багаторівнева система, що поєднує технічні, економічні, соціальні, просторові й управлінські компоненти [2, с. 69]. Відповідно, її стійкість не може бути забезпечена виключно інженерно-технічними засобами. Вона залежить від якості нормативно-правового регулювання, професійної підготовки персоналу, наявності резервів, захищеності інформаційних ресурсів, спроможності органів управління приймати рішення у кризових умовах та ефективності взаємодії між усіма залученими суб'єктами.

Законодавством до життєво важливих функцій і послуг віднесено, зокрема, урядування та надання найважливіших публічних послуг, енергозабезпечення, водопостачання і водовідведення, продовольче забезпечення, охорону здоров'я, інформаційні послуги, електронні комунікації, фінансові послуги, транспортне забезпечення, оборону, державну безпеку, правопорядок, здійснення правосуддя, тримання під вартою, цивільний захист населення і територій та діяльність рятувальних служб [7].

Наведений перелік свідчить про подвійний зв'язок критичної інфраструктури з публічною безпекою. З одного боку, належне функціонування енергетики, транспорту, зв'язку, охорони здоров'я та інших секторів створює матеріальні й організаційні умови безпечної життєдіяльності населення. З іншого боку, правопорядок і цивільний захист самі є життєво важливими функціями, а отже, об'єкти та системи, за допомогою яких вони реалізуються, також потребують спеціального захисту й забезпечення стійкості.

Припинення надання критичних послуг здатне спричинити широкий спектр негативних наслідків для публічної безпеки. Тривала

відсутність електроенергії, тепла, води або зв'язку може призвести до панічних настроїв, конфліктів через доступ до обмежених ресурсів, неконтрольованого переміщення населення, ускладнення дорожнього руху, поширення неправдивої інформації та збільшення кількості правопорушень. Одночасно зростає навантаження на поліцію, рятувальні служби, медичні заклади, органи місцевого самоврядування й соціального захисту.

Безперебійність роботи критичної інфраструктури необхідно розглядати як матеріальну основу реалізації прав і свобод людини. Доступ до медичної допомоги, питної води, теплопостачання, засобів зв'язку, транспортних та адміністративних послуг є необхідним для забезпечення права на життя, охорону здоров'я, безпечні умови проживання та участь у суспільному житті. Тому порушення функціонування критичних систем має не тільки господарський або технічний, а й правозахисний вимір.

Державна політика у сфері захисту критичної інфраструктури ґрунтується на визнанні необхідності забезпечення її безпеки і стійкості, визначенні повноважень суб'єктів національної системи захисту, впровадженні заходів контролю за ризиками, створенні систем раннього виявлення загроз, розвитку публічно-приватного партнерства, міжнародного співробітництва та забезпеченні швидкого відновлення життєво важливих функцій і послуг [7].

До основних завдань державної політики законодавством віднесено запобігання просявам несанкціонованого втручання, прогнозування і попередження кризових ситуацій, створення та розвиток національної системи захисту критичної інфраструктури, розроблення нормативно-правової й нормативно-технічної бази, впровадження заходів контролю за ризиками, встановлення обов'язкових вимог до захищеності об'єктів на всіх етапах їх життєвого циклу, аналіз викликів і загроз, підготовку персоналу та взаємодію з міжнародними системами [7]. Зазначені положення дозволяють стверджувати, що сучасна державна політика має бути превентивною, ризик-

орієнтованою та функціонально спрямованою. Її результатом повинна бути не формальна наявність охоронних систем, паспортів безпеки чи планів реагування, а реальна спроможність об'єкта продовжувати надання критичної послуги під час інциденту та відновлювати її у визначені строки.

Важливим інструментом диференціації заходів захисту є законодавче визначення чотирьох категорій критичності. До першої належать особливо важливі об'єкти загальнодержавного значення, порушення функціонування яких може спричинити кризову ситуацію державного рівня; до другої – життєво важливі об'єкти, порушення роботи яких призведе до кризової ситуації регіонального рівня; до третьої – важливі об'єкти місцевого значення; до четвертої – необхідні об'єкти, порушення функціонування яких може спричинити локальну кризову ситуацію [7]. Поділ на категорії створює основу для встановлення пропорційних вимог щодо охорони, резервування, контролю доступу, підготовки персоналу та відновлення. Водночас категорія критичності не повинна бути єдиним критерієм визначення необхідних заходів. Потрібно враховувати взаємозалежність об'єкта з іншими секторами, його територіальне розташування, оперативну обстановку, кількість населення, яке залежить від відповідної послуги, наявність альтернативних потужностей та орієнтовну тривалість відновлювальних робіт.

Особливістю критичної інфраструктури є тісна взаємозалежність її секторів. Функціонування медичних закладів залежить від енергопостачання, води, транспорту, зв'язку та цифрових систем. Енергетичні підприємства, своєю чергою, залежать від логістики, електронних комунікацій, систем управління технологічними процесами, кадрового забезпечення та охорони. Пошкодження одного елемента здатне спричинити ланцюгові відмови у декількох секторах.

В. Є. Хаустова та Н. В. Трушкіна наголошують на каскадному характері сучасних загроз критичній інфраструктурі, за якого локальне порушення може поширюватися на інші системи через технологічні, ресурсні, інформаційні

та управлінські взаємозв'язки [8, с. 97–98]. З огляду на це оцінювання ризиків повинно здійснюватися не тільки щодо окремого об'єкта, а й з урахуванням можливого впливу його відмови на інші об'єкти, сектори і територіальні громади.

Управління ризиками має включати систематичне виявлення загроз, визначення вразливостей, оцінювання ймовірності та можливих наслідків інцидентів, вибір заходів зниження ризику, моніторинг результативності цих заходів та регулярне оновлення відповідних оцінок. Формальний перелік загроз без визначення їх імовірності, потенційного масштабу наслідків та пріоритетності реагування не забезпечує належної підготовленості об'єкта.

До основних груп загроз доцільно віднести воєнні й терористичні посягання, диверсії, кібератаки, несанкціонований доступ, технічні несправності, аварії, пожежі, природні небезпечні явища, помилки персоналу, кадровий дефіцит, перебої постачання ресурсів та інформаційно-психологічні впливи. Водночас загрози не повинні оцінюватися ізольовано, оскільки технічна аварія може бути посилена кібератакою, дефіцитом персоналу або поширенням дезінформації.

Практичну конкретизацію вимог до окремих секторів здійснено наказом Міністерства внутрішніх справ України від 17 квітня 2026 року № 351, яким затверджено Вимоги до захисту об'єктів критичної інфраструктури III та IV категорій критичності секторів громадської безпеки та цивільного захисту населення і територій. Відповідний акт визначає організаційні та інженерно-технічні заходи щодо створення, налагодження і підтримання безперервного функціонування систем захисту таких об'єктів [9].

Встановлена наказом система захисту має забезпечувати стаке функціонування об'єктів та відновлення їх діяльності в умовах кризових і надзвичайних ситуацій, захист персоналу та інших осіб, виявлення причин і умов учинення протиправних дій, запобігання актам несанкціонованого втручання, підготовку і тренування працівників, оповіщення та евакуацію, зниження ризику заподіяння шкоди

людям і майну, а також мінімізацію та ліквідацію наслідків кризових ситуацій [9].

До складу системи захисту включено контрольований доступ осіб і транспортних засобів, запобігання несанкціонованому проникненню до зон обмеженого доступу, забезпечення цілісності технологічних систем, захист критичної технологічної інформації, недопущення пронесення заборонених предметів, виявлення змін обстановки на об'єкті та прилеглої території, своєчасне передавання інформації Національній поліції України, ДСНС, Службі безпеки України та іншим суб'єктам, організацію оповіщення й евакуації, розміщення альтернативних джерел енергопостачання та відновлення штатного режиму функціонування [9].

Важливо, що створення системи захисту повинно плануватися ще на стадії проектування об'єкта та забезпечуватися під час його будівництва, експлуатації, реконструкції і технічного переоснащення [9]. Такий підхід відповідає принципу закладення безпеки на всіх етапах життєвого циклу. Усунення вразливостей на стадії проектування зазвичай є більш ефективним, ніж подальше пристосування вже створеного об'єкта до нових вимог.

Водночас наявність фізичної охорони, відеоспостереження або пропускового режиму сама по собі не гарантує стійкості. Об'єкт може бути достатньо захищеним від проникнення сторонніх осіб, але залишатися вразливим через відсутність резервного живлення, альтернативних каналів зв'язку, запасів пального, дублювання критичних даних, підготовленого персоналу або погодженого порядку взаємодії з екстреними службами.

Отже, система захисту повинна мати інтегрований характер і поєднувати фізичну охорону, кіберзахист, пожежну та техногенну безпеку, цивільний захист, кадрову надійність, захист інформації, резервування ресурсів, безперервність управління, кризові комунікації та плани відновлення. Відокремлене функціонування зазначених складових створює ризик дублювання одних заходів та залишення поза увагою інших вразливостей.

Національна система захисту критичної інфраструктури функціонує на загальнодержавному, регіональному, галузевому, місцевому та об'єктовому рівнях [7]. Така багаторівневність обумовлює необхідність чіткого розмежування повноважень та одночасного забезпечення єдності методологічних засад. Рішення, прийняті на загальнодержавному рівні, повинні конкретизуватися в секторальних і регіональних документах та реалізовуватися в об'єктових планах, а інформація про фактичний стан безпеки повинна надходити у зворотному напрямі.

Суб'єктами національної системи захисту критичної інфраструктури є Кабінет Міністрів України, уповноважений, секторальні та функціональні органи, Служба безпеки України, правоохоронні й розвідувальні органи, Збройні Сили України, місцеві органи виконавчої влади, органи місцевого самоврядування, оператори критичної інфраструктури та інші підприємства, установи й організації, діяльність яких пов'язана із забезпеченням її безпеки і стійкості [7].

Включення правоохоронних органів до відповідної системи підтверджує, що захист критичної інфраструктури є одним із напрямів забезпечення публічної та національної безпеки. Участь Національної поліції України не повинна зводитися виключно до прибуття після отримання повідомлення про вже вчинене правопорушення. Поліція має бути залучена до завчасного оцінювання криміногенних і терористичних ризиків, розроблення планів взаємодії, проведення спільних навчань, визначення маршрутів прибуття сил, порядку оточення небезпечних зон та евакуації населення.

Роль Національної поліції в забезпеченні безпеки критичної інфраструктури може реалізовуватися через охорону публічного порядку на об'єктах і прилеглих територіях, превентивну діяльність, перевірку інформації про можливі загрози, реагування на правопорушення, регулювання дорожнього руху, обмеження доступу до небезпечних зон, участь в евакуації, охорону місця події, документування протиправної діяльності та забезпечення

правопорядку під час проведення аварійно-відновлювальних робіт.

Окремого значення набуває діяльність поліції в умовах тривалого припинення критичних послуг. Такі ситуації можуть супроводжуватися значним скупченням людей біля пунктів видачі води, гуманітарної допомоги, обігріву чи заряджання електронних пристроїв, конфліктами через обмежені ресурси, спробами проникнення на пошкоджені об'єкти або заволодіння майном. Відповідно, плани реагування повинні передбачати розрахунок необхідних сил поліції, організацію патрулювання, охорону стратегічних запасів, регулювання транспортних потоків та комунікацію з населенням.

Законодавець передбачає вимогу своєчасного інформування територіальних органів і підрозділів Національної поліції України про наявні або потенційні загрози об'єктам критичної інфраструктури [9]. Реалізація цієї вимоги потребує визначення конкретних каналів зв'язку, контактних осіб, обсягу інформації, строків повідомлення та порядку підтвердження її отримання. Загальне формулювання обов'язку інформувати без відповідної процедури може знижувати оперативність реагування.

Доцільним є розроблення типових міжвідомчих алгоритмів дій залежно від характеру інциденту. Такі алгоритми мають визначати порядок первинного повідомлення, оцінювання обстановки, розподілу зон відповідальності, організації єдиного управління, евакуації, надання допомоги постраждалим, охорони території, проведення слідчих та аварійно-відновлювальних дій. Водночас типові алгоритми повинні адаптуватися до особливостей конкретного об'єкта і території.

Забезпечення стійкості критичної інфраструктури неможливе без належної участі органів місцевого самоврядування. Саме на рівні територіальної громади наслідки припинення життєво важливих послуг безпосередньо перетворюються на загрози публічній безпеці. Місцева влада першою стикається з потребами населення у воді, теплі, транспорті, медичній допомозі, тимчасовому розміщенні та достовірній інформації.

Місцеві програми забезпечення безпеки і стійкості повинні передбачати визначення найбільш критичних для громади об'єктів і послуг, створення резервів пального, води та матеріальних ресурсів, забезпечення альтернативних джерел енергопостачання, дублювання каналів зв'язку, підготовку пунктів обігріву й тимчасового розміщення, визначення маршрутів евакуації та порядку пріоритетного відновлення послуг.

При цьому повноваження органів місцевого самоврядування нерідко не відповідають рівню їх фактичної відповідальності перед населенням. Окремі об'єкти розташовані на території громади, однак перебувають у державній або приватній власності, а органи місцевого самоврядування мають обмежені можливості впливати на рішення їх операторів. Зазначене зумовлює необхідність розвитку договірних і координаційних механізмів взаємодії, проведення спільних навчань та включення представників громад до планування заходів реагування і відновлення.

Значна частина об'єктів критичної інфраструктури перебуває у приватній або комунальній власності, тому ефективність державної політики залежить від публічно-приватного партнерства. Оператори відповідають за поточне функціонування об'єктів, організацію систем захисту, підготовку паспортів безпеки, навчання персоналу, повідомлення про інциденти та вжиття відновлювальних заходів. Держава, зі свого боку, має визначати обов'язкові стандарти, надавати методичну допомогу, координувати діяльність, контролювати виконання встановлених вимог і забезпечувати обмін інформацією про актуальні загрози.

Публічно-приватна взаємодія повинна ґрунтуватися на довірі, взаємній відповідальності та захищеному інформаційному обміні. Оператор має бути зацікавлений у ранньому повідомленні державних органів про інцидент, а не приховуванні проблеми через побоювання репутаційних чи контрольних наслідків. Водночас державні органи повинні своєчасно надавати операторам інформацію, необхідну для уточнення профілів ризику та посилення захисних заходів.

Доцільним є створення постійних регіональних і секторальних координаційних платформ, у межах яких представники органів державної влади, поліції, ДСНС, СБУ, територіальних громад та операторів могли б аналізувати ризики, обмінюватися інформацією, узгоджувати плани взаємодії та проводити навчання. Такі платформи не повинні підміняти компетенцію окремих органів, але можуть забезпечити сталі комунікаційні зв'язки між ними.

Важливим елементом стійкості критичної інфраструктури є налагоджена комунікація з населенням у кризових ситуаціях. Під час аварій, атак або тривалого припинення надання життєво важливих послуг люди особливо потребують швидкої, достовірної та зрозумілої інформації. Її відсутність або несвоєчасне поширення сприяє появі чуток, дезінформації, тривоги та панічних настроїв. Саме тому в планах реагування необхідно заздалегідь визначати офіційні джерела інформування, порядок і періодичність повідомлень, способи оперативного спростування неправдивих відомостей, а також передбачати резервні канали оповіщення на випадок перебоїв з електропостачанням чи мобільним зв'язком.

Інформація для населення має бути доступною, конкретно і корисною для практичних дій. У повідомленнях слід чітко зазначати характер загрози, територію, якої вона стосується, правила безпечної поведінки, місця отримання допомоги та, за можливості, орієнтовні строки відновлення послуг. Особливо важливо враховувати потреби людей, яким складніше швидко отримати або правильно сприйняти інформацію, зокрема осіб з інвалідністю, людей похилого віку, дітей, іноземців та інших уразливих груп.

Не менш важливим є кадрове забезпечення. Навіть технічно досконала система не буде стійкою без персоналу, здатного приймати рішення в умовах невизначеності, дефіциту часу й ресурсів. Працівники операторів, органів публічної влади, поліції та рятувальних служб повинні володіти спільним понятійним апаратом, знати розподіл повноважень, порядок обміну інформацією та послідовність дій у різних режимах функціонування.

Закон України «Про критичну інфраструктуру» відносить підготовку, перепідготовку, підвищення кваліфікації та тренування працівників національної системи захисту критичної інфраструктури до завдань державної політики [7]. Відтак до освітніх і професійних програм необхідно включати питання управління ризиками, безперервності діяльності, кризового управління, захисту інформації, міжвідомчої взаємодії та комунікації з населенням.

Висновки. На підставі проведеного дослідження доцільно запропонувати комплекс взаємопов'язаних напрямів удосконалення забезпечення безпеки і стійкості критичної інфраструктури.

Передусім необхідно забезпечити взаємоузгодженість загальнодержавних, секторальних, регіональних, місцевих та об'єктових планів. Документи різних рівнів повинні використовувати єдиний понятійний апарат, методологію оцінювання ризиків і критерії визначення пріоритетності відновлення. Об'єктові плани мають ураховувати регіональні спроможності, а регіональні – фактичні потреби й вразливості конкретних операторів.

Необхідно конкретизувати роль Національної поліції України у національній системі захисту критичної інфраструктури, визначивши форми її участі в оцінюванні загроз, розробленні планів взаємодії, проведенні навчань, реагуванні на інциденти, забезпеченні режимних обмежень, евакуації та підтриманні правопорядку під час відновлення. Відповідні повноваження мають бути узгоджені з компетенцією СБУ, ДСНС, органів військового управління та підрозділів охорони об'єктів.

Доцільно створити типові міжвідомчі алгоритми реагування на основні види інцидентів та передбачити їх обов'язкову адаптацію до специфіки об'єкта. У таких алгоритмах слід визначати порядок управління силами, інформаційного обміну, доступу до об'єкта, евакуації, охорони небезпечної зони, документування події й організації відновлювальних робіт.

Важливим напрямом є посилення спроможності територіальних громад. Місцеві програми стійкості повинні супроводжуватися конкретним ресурсним забезпеченням, визна-

ченням відповідальних осіб, індикаторів виконання та порядку взаємодії з операторами. До планування необхідно залучати представників населення, громадських організацій, бізнесу та установ, які надають соціально значущі послуги.

Подальшого розвитку потребує система професійної підготовки. Варто запровадити спільні навчальні модулі для операторів, органів влади, поліції та рятувальних служб, що сприятиме формуванню єдиного розуміння ризиків і процедур. Особлива увага має при-

ділятися практичним тренуванням за сценаріями комбінованого та каскадного впливу.

Отже, забезпечення безпеки і стійкості критичної інфраструктури має розглядатися не як вузькоспеціалізований напрям технічного або оборонного характеру, а як комплексний пріоритет публічної безпеки. Його зміст охоплює захист населення, забезпечення громадського порядку, безперервність публічного управління, доступ до життєво важливих послуг та спроможність органів влади і служб реагування виконувати свої функції у кризових умовах.

Список використаних джерел:

1. Бірюков Д.С. Захист критичної інфраструктури в Україні: від наукового осмислення до розробки засад політики. *Науково-інформаційний вісник Академії національної безпеки*. 2015. № 3-4. С. 155–170. URL: http://nbuv.gov.ua/UJRN/nivanb_2015_3-4_14 (дата звернення: 13.07.2026).
2. Кизим М.О., Хаустова В.Є., Трушкіна Н.В. Сутність поняття «критична інфраструктура» з позицій національної безпеки України. *Бізнес Інформ*. 2022. № 12. С. 58–78. DOI: 10.32983/2222-4459-2022-12-58-78
3. Арсенович Л.А. Парадигма захисту критичної інфраструктури в системі національної безпеки України. *Державне управління: удосконалення та розвиток*. 2024. № 8. DOI: 10.32702/2307-2156.2024.8.7.
4. Ковальчук А.Т. Система правового регулювання захисту об'єктів критичної інфраструктури в Україні: сучасний стан та напрями удосконалення. *Науковий вісник Ужгородського національного університету*. Серія: Право. 2025. Вип. 90. Ч. 5. С. 172–184. DOI: <https://doi.org/10.24144/2307-3322.2025.90.5.21>
5. Bruneau M., Chang S. E., Eguchi R. T., Lee G. C., O'Rourke T. D., Reinhorn A.M., Shinozuka M., Tierney K., Wallace W.A., von Winterfeldt D. A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. *Earthquake Spectra*. 2003. Vol. 19. № 4. P. 733–752. DOI: 10.1193/1.1623497.
6. Linkov I., Trump B. D., Trump J., Pescaroli G., Hynes W., Mavrodieva A., Panda A. Resilience Stress Testing for Critical Infrastructure. *International Journal of Disaster Risk Reduction*. 2022. Vol. 82. Article 103323. DOI: 10.1016/j.ijdrr.2022.103323.
7. Про критичну інфраструктуру : Закон України від 16 листопада 2021 року № 1882-IX. URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text> (дата звернення: 13.07.2026).
8. Хаустова В.Є., Трушкіна Н.В. Загрози розвитку критичної інфраструктури: сутність і класифікація. *Проблеми економіки*. 2025. № 3. С. 89-104. DOI: 10.32983/2222-0712-2025-3-89-104
9. Про затвердження Вимог до захисту об'єктів критичної інфраструктури III та IV категорій критичності секторів громадської безпеки та цивільного захисту населення і територій : наказ Міністерства внутрішніх справ України від 17 квітня 2026 року № 351. URL: <https://zakon.rada.gov.ua/laws/show/z0616-26#Text> (дата звернення: 13.07.2026).

References:

1. Biriukov, D.S. (2015). Zakhyst krytychnoi infrastruktury v Ukraini: vid naukovooho osmyslennia do rozrobky zasad polityky [Protection of Critical Infrastructure in Ukraine: From Scientific Analysis to the Development of Policy Guidelines]. *Naukovo-informatsiyni visnyk Akademii natsionalnoi bezpeky*, 3–4, 155–170. Retrieved from: http://nbuv.gov.ua/UJRN/nivanb_2015_3-4_14 [in Ukrainian]
2. Kyzym, M.O., Khaustova, V.Ie., & Trushkina, N.V. (2022). Sutnist poniattia «krytychna infrastruktura» z pozytsii natsionalnoi bezpeky Ukrainy [The Concept of “Critical Infrastructure” from the Perspective of Ukraine’s National Security]. *Biznes Inform*, 12, 58–78. DOI: 10.32983/2222-4459-2022-12-58-78 [in Ukrainian]
3. Arsenovych, L.A. (2024). Paradyhma zakhystu krytychnoi infrastruktury v systemi natsionalnoi bezpeky Ukrainy [The Paradigm of Critical Infrastructure Protection in Ukraine’s National Security System]. *Derzhavne upravlinnia: udoskonalennia ta rozvytok*, 8. DOI: 10.32702/2307-2156.2024.8.7 [in Ukrainian]

4. Kovalchuk, A.T. (2025). Systema pravovoho rehuliuvannia zakhystu ob'ektiv krytychnoi infrastruktury v Ukraini: suchasnyi stan ta napriamy udoskonalennia [The Legal Framework for the Protection of Critical Infrastructure in Ukraine: Current Status and Areas for Improvement]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Serii: Pravo*, 90. Ch. 5, 172–184. DOI: <https://doi.org/10.24144/2307-3322.2025.90.5.21> [in Ukrainian]
5. Bruneau, M., Chang, S. E., Eguchi, R. T., Lee, G.C., O'Rourke, T.D., Reinhorn, A.M., Shinozuka, M., Tierney, K., Wallace, W.A., & von Winterfeldt, D.A (2003). Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. *Earthquake Spectra*, Vol. 19. № 4. P. 733–752. DOI: 10.1193/1.1623497 [in English].
6. Linkov, I., Trump, B. D., Trump, J., Pescaroli, G., Hynes, W., Mavrodieva, A., & Panda, A. (2022). Resilience Stress Testing for Critical Infrastructure. *International Journal of Disaster Risk Reduction*, Vol. 82. Article 103323. DOI: 10.1016/j.ijdr.2022.103323 [in English].
7. Pro krytychnu infrastrukturu [About Critical Infrastructure]: Zakon Ukrainy vid 16 lystopada 2021 roku № 1882-IX. Retrieved from: <https://zakon.rada.gov.ua/laws/show/1882-20#Text> [in Ukrainian]
8. Khaustova, V.Ye., & Trushkina, N.V. (2025). Zahrozy rozvytku krytychnoi infrastruktury: sutnist i klasyfikatsiia [Threats to the Development of Critical Infrastructure: Nature and Classification]. *Problemy ekonomiky*, 3, 89–104. DOI: 10.32983/2222-0712-2025-3-89-104 [in Ukrainian]
9. Pro zatverdzhennia Vymoh do zakhystu ob'ektiv krytychnoi infrastruktury III ta IV katehorii krytychnosti sektoriv hromadskoi bezpeky ta tsyvilnoho zakhystu naselennia i terytorii [On the Approval of Requirements for the Protection of Critical Infrastructure Facilities of Categories III and IV in the Sectors of Public Safety and Civil Protection of the Population and Territories]: nakaz Ministerstva vnutrishnikh sprav Ukrainy vid 17 kvitnia 2026 roku № 351. Retrieved from: <https://zakon.rada.gov.ua/laws/show/z0616-26#Text> [in Ukrainian]

Дата першого надходження статті до видання: 17.07.2026

Дата прийняття статті до друку після рецензування: 21.08.2026

Дата публікації (оприлюднення) статті: 00.00.2026

DOI <https://doi.org/10.32782/2311-8040/2026-2-12>**Яновицька Анна Віталіївна**

кандидат юридичних наук, доцент,
доцентка кафедри цивільно-правових дисциплін,
Львівський державний університет внутрішніх справ,
вулиця Городоцька, 26, Львів, 79000, Україна
ORCID: <https://orcid.org/0000-0001-7071-4234>

РЕЦЕНЗІЯ

**на монографію доктора філософії в галузі права Володимира Лопатнюка
«Правова охорона баз даних в Україні та ЄС: порівняльно-правове
дослідження» (Львів–Дрогобич : вид-во Посвіт, 2026. 245 с.)**

За наслідками індустріалізації, сучасний світ стрімко перейшов у цифрову епоху. Набрали актуальності процеси автоматизації обробки та використання значних обсягів інформації, збереження та її захист. Важливою є робота із даними для подальшого їх використання людьми, програмами або технічними системами для вирішення своїх завдань.

Саме проблематиці охорони баз даних в Україні та ЄС присвячене рецензоване наукове дослідження Володимира Лопатнюка «Правова охорона баз даних в Україні та ЄС: порівняльно-правове дослідження». Монографія побудована на основі ґрунтовних теоретичних досліджень у галузі права інтелектуальної власності, інформаційного права та загальних цивілістичних підходів до правового регулювання охорони баз даних.

Актуальність монографії не викликає сумнівів, адже проблематика вдосконалення українського законодавства, його гармонізація із законодавством ЄС є частиною першого, «фундаментального» кластера при вступі держави у ЄС, а робота над законодавством у сфері безпосередньо інтелектуальної власності є частиною кластера два щодо внутрішнього ринку.

Предметом представленого наукового дослідження є комплекс суспільних відносин, що виникають у процесі створення, використання та правової охорони баз даних, а також відповідні положення законодавства України та Європейського Союзу і практика їх застосування.

Наукова новизна роботи полягає у комплексному порівняльно-правовому дослідженні особливостей охорони баз даних в Україні та ЄС, з'ясуванні специфіки авторсько-правової охорони та права особливого роду (*sui generis*), а також у розробленні автором теоретичних положень і практичних пропозицій щодо вдосконалення національного законодавства з урахуванням європейських правових підходів.

З метою захисту баз даних, у праві ЄС впроваджено конструкцію прав особливого роду (*sui generis*); прийнято окрему Директиву 96/9/ЄС Європейського Парламенту та Ради «Про правовий захист баз даних» від 11 березня 1996 року. У новому Законі України «Про авторське право і суміжні права» від 1 грудня 2022 року, закріплені аналогічні правові підходи.

Однак, як слушно зауважує Володимир Лопатнюк, на сьогодні чинне законодавство України не повною мірою урегулює відносини як щодо створення, так і використання баз даних як об'єктів авторського права.

Основна частина монографії складається із чотирьох логічно пов'язаних між собою розділів. Розділ 1 «Загальнотеоретичні засади правового регулювання баз даних як об'єктів інтелектуальної власності» містить аналіз історичного розвитку правової основи охорони баз даних, сучасний стан правового регулювання та європейський вплив на правове регулювання охорони баз даних в Україні. Як пише автор, «наріжним каменем правової охорони баз даних в рамках ЄС стала Директива Євро-

пейського Парламенту та Ради Європейського Союзу «Про правовий захист баз даних» від 11 березня 1996 р.» (с. 22) “...реформування системи охорони інтелектуальної власності у відповідності до стандартів ЄС визнано одним із завдань згідно із Концепцією оновлення ЦК України” (с. 32).

Традиційно, перший розділ присвячений дослідженню понятійного апарату. Важливими із теоретичної та практичної точок зору, видаються запропоновані класифікації баз даних: А) За критерієм правової природи їх вмісту: 1) бази даних, які містять самостійні твори – є результатом систематизації самостійних об’єктів авторського права; 2) бази даних, які містять набір даних, інформації, які не є самостійними об’єктами авторсько-правової охорони; 3) змішані бази даних: ті, які містять як твори, які охороняються авторським правом, так і інформацію (дані), які не є об’єктами авторсько-правової охорони. Б) За колом суб’єктів, які мають право на доступ до бази даних: 1) бази даних із вільним доступом усіх бажаних користувачів; 2) бази даних з обмеженим доступом (секретні бази даних, бази даних, які охороняються в рамках комерційної таємниці тощо) (с. 53).

У розділі 2 «Правова охорона баз даних як об’єктів авторського права» досліджені питання суб’єктного складу, набуття прав на базу даних, зміст особистих немайнових та майнових прав автора.

Вартий уваги підхід автора до розмежування прав інтелектуальної власності на базу даних між окремими суб’єктами. Так, Володимир Лопатнюк підкреслює, що в силу “творчого характеру праці” ... “особисті немайнові та майнові права інтелектуальної власності на базу даних первинно виникають власне у фізичної особи – творця” (с. 56). І “...на сьогодні все ще рано, а в майбутньому – і недоцільно говорити про можливість надання штучному інтелекту чи роботам правосуб’єктності”, а тому “об’єкт, згенерований системою штучного інтелекту, який має творчий характер, повинен визнаватись об’єктом права інтелектуальної власності того суб’єкта, який задавав вихідні дані для створення такого об’єкта”

(с. 69). При створенні службових об’єктів “... як з боку роботодавця, та і з боку працівника – автора бази даних, відносини повинні будуватись на такій засаді цивільного права як добросовісність, яка виключатиме зловживання своїми правами як з однієї, так і з іншої сторони” (с. 62).

У розділі 3 «Правова охорона неоригінальних баз даних» досліджено правову природу *sui generis*. Зокрема, Володимир Лопатнюк аналізує ст. 7 Директиви 96/9/ЄС та ч. 5 ст. 21 Закону України «Про авторське право і суміжні права», на основі чого доходить висновку про необхідність широкого тлумачення поняття відчуження *sui generis* на базу даних. Такий підхід лягає в основу пропозиції автора, що *sui generis* на базу даних може бути об’єктом відносин правонаступництва: передаватись в порядку спадкування чи при реорганізації юридичної особи (с. 134–135).

Розділ 4 «Особливості захисту прав на бази даних» є завершальним і, серед іншого, присвячений авторським підходам до встановлення механізмів захисту прав інтелектуальної власності на бази даних. Як слушно зауважує автор, Закон України «Про авторське право і суміжні права», визначаючи правовий режим баз даних, не містить законодавчих положень щодо особливостей захисту прав на них. Відтак, при порушенні прав на бази даних слід керуватись загальними положеннями щодо видів порушень прав на об’єкти авторського права і щодо способів та порядку захисту цих прав. Актуальною видається пропозиція Володимира Лопатнюка передбачити у ст. 53 Закону України «Про авторське право і суміжні права» (підстави для захисту авторського права і суміжних прав) можливість застосування цієї статті “не лише до об’єктів авторських та суміжних прав, але і до об’єктів, які охороняються правом особливого роду (*sui generis*)” (підрозд. 4.2).

Загалом, слід відзначити завершений характер рецензованого монографічного дослідження. Надзвичайно актуальним видається повсякчасне застосування порівняльно-правового методу, завдяки якому у монографії з’являються актуальні пропозиції із вдоско-

налення українського правового регулювання охорони баз даних із врахуванням досвіду правового регулювання ЄС. Наприклад: обґрунтовано необхідність внесення змін до ст. 21 Закону України «Про авторське право і суміжні права», передбачивши “можливість набуття, здійснення та захисту прав на неоригінальні бази даних кількома особами, які спільною працею із залученням фінансових та організаційних ресурсів розробили базу даних, яка є неоригінальною та охороняється правом особливого роду”; “обґрунтовано, що в Законі України «Про авторське право і суміжні права» слід передбачити положення щодо можливості набуття права особливого роду (*sui generis*) юридичними особами. Запропоновано відповідні доповнення до

ст. 21 Закону України «Про авторське право і суміжні права»” (с. 193–231) та ін.

Монографія Володимира Лопатнюка «Правова охорона баз даних в Україні та ЄС: порівняльно-правове дослідження» є науковою працею із актуальної і проблемної на сьогодні теми. Дослідження, висновки і пропозиції, які у ній наведені, будуть цікавими для юристів-дослідників, юристів-практиків та усіх, хто безпосередньо причетний до постійної роботи із базами даних. Слід звернути увагу й на наявність професійного перекладу ключових тез монографії англійською та польською мовами. Матеріали монографії можуть використовуватись у освітній діяльності та у подальших наукових дослідженнях із даної теми.

ЗМІСТ

Барабаш Ольга Олегівна	
КОНЦЕПТУАЛЬНІ ЗАСАДИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ПРОФЕСІЙНОЇ ТАЄМНИЦІ ПРИ ВИКОРИСТАННІ ШТУЧНОГО ІНТЕЛЕКТУ ПІД ЧАС КВАЛІФІКАЦІЙНИХ ІСПИТІВ ЧЛЕНІВ ЕКІПАЖІВ: СТАНДАРТИ НАТО ТА ПЕРСПЕКТИВИ ІМПЛЕМЕНТАЦІЇ В УКРАЇНІ.....	3
Боровікова Віталіна Станіславівна, Баб'як Андрій Васильович,	
ІНФОРМАЦІЙНО-АНАЛІТИЧНА ДІЯЛЬНІСТЬ У ПРАВООХОРОННИХ ОРГАНАХ УКРАЇНИ: ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ТА НОРМАТИВНЕ ЗАБЕЗПЕЧЕННЯ.....	15
Гурковська Катерина Андріївна,	
АДМІНІСТРАТИВНО-ПРАВОВА ХАРАКТЕРИСТИКА ВЗАЄМОДІЇ СУБ'ЄКТІВ У СФЕРІ ЗАПОБІГАННЯ ТА ПРОТИДІЇ ДОМАШНЬОМУ НАСИЛЬСТВУ.....	25
Кравченко Іван Олександрович	
ТРАНСФОРМАЦІЯ НАЦІОНАЛЬНИХ ПІДХОДІВ ДО КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ЗА НЕЦІЛЬОВЕ ВИКОРИСТАННЯ ГУМАНІТАРНОЇ ДОПОМОГИ: ІМПЛЕМЕНТАЦІЯ СТАНДАРТІВ ЄВРОПЕЙСЬКОГО СОЮЗУ.....	34
Лиса Марія Олегівна, Булачек Володимир Романович, Курляк Мар'ян Дмитрович, Синенький Володимир Михайлович, Гречанюк Андрій Олексійович	
КООРДИНАЦІЯ СИЛ ТА ЗАСОБІВ ПІД ЧАС ЛІКВІДАЦІЇ НАСЛІДКІВ НАДЗВИЧАЙНИХ СИТУАЦІЙ.....	42
Лукашук Юрій Андрійович, Цмоць Уляна Олексіївна	
ДИНАМІКА ПЕРЕОСМИСЛЕННЯ ПРАВОВИХ І МОРАЛЬНИХ ЦІННОСТЕЙ У КОНТЕКСТІ ЦИФРОВИХ ТРАНСФОРМАЦІЙ.....	53
Мовчан Анатолій Васильович	
МІЖВІДОМЧА ВЗАЄМОДІЯ СИЛ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ: СУТНІСТЬ, ПРОБЛЕМИ ТА НАПРЯМИ ВДОСКОНАЛЕННЯ.....	62
Панасюк Олександр Петрович	
ОРГАНІЗАЦІЙНО-ТАКТИЧНІ ЗАСАДИ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ПЛАТФОРМ ІНТЕРПОЛУ ТА ЄВРОПОЛУ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ ЩОДО ПРОТИДІЇ ПОСЯГАННЯМ НА ВОЛЮ ОСОБИ.....	72
Татаренко Світлана В'ячеславівна, Явтушенко Юлія Вікторівна	
СПЕЦІАЛЬНІ ТЕХНІЧНІ ЗАСОБИ У РОЗШУКОВІЙ ДІЯЛЬНОСТІ КРИМІНАЛЬНОЇ ПОЛІЦІЇ: ПРАВОВІ ЗАСАДИ, ФУНКЦІОНАЛЬНІ МОЖЛИВОСТІ ТА НАПРЯМИ ВДОСКОНАЛЕННЯ.....	81
Тищенко Анна Дмитрівна	
ЮРИДИЧНИЙ АНАЛІЗ СКЛАДУ ЗЛОЧИНУ «ДОМАГАННЯ ДИТИНИ ДЛЯ СЕКСУАЛЬНИХ ЦІЛЕЙ».....	91
Умрихіна Ірина Олександрівна, Тишлек Микола Миколайович, Чепеляк Віталій Степанович	
ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ТА СТІЙКОСТІ ФУНКЦІОНУВАННЯ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЯК ПРІОРИТЕТНИЙ НАПРЯМ ПУБЛІЧНОЇ БЕЗПЕКИ.....	104
Яновицька Анна Віталіївна	
РЕЦЕНЗІЯ НА МОНОГРАФІЮ ДОКТОРА ФІЛОСОФІЇ В ГАЛУЗІ ПРАВА ВОЛОДИМИРА ЛОПАТНЮКА «ПРАВОВА ОХОРОНА БАЗ ДАНИХ В УКРАЇНІ ТА ЄС: ПОРІВНЯЛЬНО-ПРАВОВЕ ДОСЛІДЖЕННЯ»	115

CONTENTS

Barabash Olha	
CONCEPTUAL FOUNDATIONS OF THE LEGAL PROTECTION OF PROFESSIONAL SECRECY IN THE USE OF ARTIFICIAL INTELLIGENCE DURING CREW MEMBERS’ QUALIFICATION EXAMINATIONS: NATO STANDARDS AND PROSPECTS FOR IMPLEMENTATION IN UKRAINE.....	3
Borovikova Vitalina, Babiak Andrii	
INFORMATION AND ANALYTICAL ACTIVITIES IN THE LAW ENFORCEMENT AGENCIES OF UKRAINE: THEORETICAL AND LEGAL FOUNDATIONS AND REGULATORY FRAMEWORK.....	15
Hurkovska Kateryna	
ADMINISTRATIVE AND LEGAL CHARACTERISTICS OF INTERACTION BETWEEN SUBJECTS IN THE FIELD OF PREVENTION AND COUNTERACTION TO DOMESTIC VIOLENCE.....	25
Kravchenko Ivan	
TRANSFORMATION OF NATIONAL APPROACHES TO CRIMINAL LIABILITY FOR THE MISUSE OF HUMANITARIAN AID: IMPLEMENTATION OF EUROPEAN UNION STANDARDS.....	34
Lysa Mariia, Bulachek Volodymyr, Kurliak Marian, Synenkyi Volodymyr, Grechanuk Andrii	
COORDINATION OF FORCES AND RESOURCES DURING THE ELIMINATION OF THE CONSEQUENCES OF EMERGENCIES.....	42
Lukashchuk Yurii, Tsmots Uliana	
DYNAMICS OF REINTERPRETING LEGAL AND MORAL VALUES IN THE CONTEXT OF DIGITAL TRANSFORMATIONS.....	53
Movchan Anatolii	
INTER-AGENCY INTERACTION OF FORCES IN THE SECURITY AND DEFENSE SECTOR: ESSENCE, PROBLEMS, AND DIRECTIONS FOR IMPROVEMENT.....	62
Panasiuk Oleksandr	
ORGANIZATIONAL AND TACTICAL FOUNDATIONS FOR THE USE OF INTERPOL AND EUROPOL INFORMATION PLATFORMS IN LAW ENFORCEMENT ACTIVITY TO COUNTER ENCROACHMENTS ON PERSONAL LIBERTY.....	72
Tatarenko Svitlana, Yavtushenko Yuliia	
SPECIAL TECHNICAL MEANS IN THE PERSON-SEARCH ACTIVITIES OF THE CRIMINAL POLICE: LEGAL FOUNDATIONS, FUNCTIONAL CAPABILITIES AND AREAS FOR IMPROVEMENT.....	81
Tyshchenko Anna	
LEGAL ANALYSIS OF THE ELEMENTS OF THE CRIMINAL OFFENCE OF “GROOMING A CHILD FOR SEXUAL PURPOSES”.....	91
Umrykhina Iryna, Tyshlek Mykola, Chepeliak Vitalii	
ENSURING THE PROTECTION AND RESILIENCE OF CRITICAL INFRASTRUCTURE AS A PRIORITY AREA OF PUBLIC SAFETY.....	104
Yanovytska Anna	
RETSENZIYA. NA MONOHRAFIYU DOKTORA FILOSOFIYI V HALUZI PRAVA VOLODYMYRA LOPATNYUKA «PRAVOVA OKHORONA BAZ DANYKH V UKRAYINI TA YES: PORIVNYANNO-PRAVOVE DOSLIDZHENNYA».....	115

НАУКОВИЙ ВІСНИК

ЛЬВІВСЬКОГО ДЕРЖАВНОГО УНІВЕРСИТЕТУ ВНУТРІШНІХ СПРАВ

Серія правоохоронна

Випуск 2

Коректор *І. М. Чудеснова*
Комп'ютерне верстання *О. І. Молодецька*

Дата розміщення онлайн: 23.04.2026.
Дата друку: 30.04.2026.
Формат 60×84/8. Гарнітура Times New Roman.
Папір офсет. Цифровий друк. Ум. друк. арк. 13,95. Зам. № 0926/750.
Наклад 100 прим.

Надруковано: Видавничий дім «Гельветика»
65101, Україна, м. Одеса, вул. Інглезі, 6/1
Телефони: +38 (095) 934 48 28, +38 (097) 723 06 08
E-mail: mailbox@helvetica.ua
Свідоцтво суб'єкта видавничої справи
ДК № 7623 від 22.06.2022 р.