УДК 351.861:342.7:004.738.5
DOI: 10.36550/2522-9230-2025-18-343-347

Куркова Ксенія Миколаївна
доктор юридичних наук, професор,
завідувач відділу науково-правових
експертиз та законопроектних робіт
Науково-дослідного інституту публічного права
kurkova_ksenya@ukr.net
ORCID ID: 0000-0002-4259-5511

КОНЦЕПТУАЛЬНЕ РОЗУМІННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ У ПУБЛІЧНО-ІНФОРМАЦІЙНІЙ СФЕРІ

У статті досліджено концептуальне розуміння національної безпеки у публічно-інформаційній сфері. Акцентовано увагу, що сучасні глобалізаційні процеси, динамічний розвиток цифрових технологій та інтенсивне поширення інформаційно-комунікаційних систем обумовлюють формування нового виміру національної безпеки, що безпосередньо пов'язаний із публічно-інформаційною сферою. У такому контексті інформація постає як стратегічний ресурс держави, суспільства та окремої особи, від рівня достовірності, відкритості та захищеності якого залежить ефективність реалізації національних інтересів. Водночас зростання масштабів інформаційних загроз, поширення дезінформаційних кампаній, кібератак, а також технологій когнітивного та маніпулятивного впливу у публічному середовищі істотно підвищує ризики дестабілізації політичної системи, знижує рівень суспільної довіри до органів влади та ускладнює функціонування демократичних інститутів. У таких умовах забезпечення інформаційної безпеки стає не лише елементом національної безпеки, але й ключовим чинником стійкості соціально-політичної системи.

Розглянуто основні підходи до забезпечення національної безпеки у публічно-інформаційній сфері: традиційний, системний та комплексний (інтегративний). Визначено, що концептуальне розуміння національної безпеки у публічно-інформаційній має ґрунтуватися на комплексному підході, який є найбільш релевантним у сучасних умовах зростання гібридних загроз, оскільки він: 1) поєднує елементи традиційного (захист держави від реальних і потенційних загроз, насамперед воєнно-політичного характеру) та системного (узгодженість цілей, суб'єктів, об'єктів і механізмів забезпечення безпеки) підходів, але водночас виходить за їхні межі, дозволяючи розглядати безпеку не лише крізь призму воєнно-політичних аспектів, але й у більш широкому контексті – правовому, соціальному, економічному, інформаційно-технологічному вимірах; 2) розглядає національну безпеку у публічно-інформаційній сфері як динамічну поліструктурну систему, здатну протидіяти як технологічним (кібератаки, несанкціонований доступ, деструктивне втручання у критичні інформаційні інфраструктури), так і соціально-психологічним (маніпуляції суспільною свідомістю, поширення пропаганди, дезінформації) загрозам, що відповідає реаліям сучасного інформаційного суспільства; 3) забезпечує гнучкість та адаптивність відповідно до швидкої динаміки інформаційного середовища, інтегруючи правові механізми, інституційні рішення, інноваційні технології та соціальні практики, що створює умови для оперативної реакції на нові форми інформаційних атак, які традиційні підходи не завжди враховують; 4) передбачає системну кооперацію та взаємодію держави, інституцій громадянського суспільства, бізнесу та міжнародних партнерів, що створює синергію, без якої неможливо забезпечити стійкість інформаційного простору в умовах глобальної взаємозалежності; 5) спрямований на формування стійкої інформаційної екосистеми, яка забезпечує не лише захищеність від загроз, але й створює передумови для інноваційного науково-технологічного розвитку держави та суспільства, збереження культурної ідентичності, формування критичного мислення у суспільстві та підвищення рівня інформаційної грамотності громадян у довгостроковій перспективі.

Ключові слова: національна безпека, інформаційна безпека, публічно-інформаційна сфера, цифровізація, інформаційні загрози, дезінформація, кіберзахист, державна політика, публічне управління, цифрове урядування, інформаційний простір.

Kurkova K. CONCEPTUAL UNDERSTANDING OF NATIONAL SECURITY IN THE PUBLIC INFORMATION SPHERE

The article explores the conceptual understanding of national security in the public information sphere. It is emphasized that modern globalization processes, the dynamic development of digital technologies and the intensive spread of information and communication systems determine the formation of a new dimension of national security, which is directly related to the public information sphere. In such a context, information appears as a strategic resource of the state, society and the individual, the level of reliability, openness and security of which determines the effectiveness of the implementation of national interests. At the same time, the growth of the scale of information threats, the spread of disinformation campaigns, cyberattacks, as well as technologies of cognitive and manipulative influence in the public environment significantly increases the risks of destabilization of the political system, reduces the level of public trust in government bodies and complicates the functioning of democratic institutions. In such conditions, ensuring information security becomes not only an element of national security, but also a key factor in the stability of the socio-political system.

The main approaches to ensuring national security in the public information sphere are considered: traditional, systemic and comprehensive (integrative). It is determined that the conceptual understanding of national security in the public information sphere should be based on a comprehensive approach, which is most relevant in the current conditions of the growth of hybrid threats, since it: 1) combines elements of the traditional (protection of the state from real and potential threats, primarily of a

military-political nature) and systemic (coherence of goals, subjects, objects and mechanisms for ensuring security) approaches, but at the same time goes beyond them, allowing security to be considered not only through the prism of military-political aspects, but also in a broader context - legal, social, economic, information and technological dimensions; 2) considers national security in the public information sphere as a dynamic polystructural system capable of counteracting both technological (cyberattacks, unauthorized access, destructive interference in critical information infrastructures) and socio-psychological (manipulation of public consciousness, dissemination of propaganda, disinformation) threats, which corresponds to the realities of the modern information society; 3) provides flexibility and adaptability in accordance with the rapid dynamics of the information environment, integrating legal mechanisms, institutional solutions, innovative technologies and social practices, which creates conditions for an operational response to new forms of information attacks that traditional approaches do not always take into account; 4) provides for systemic cooperation and interaction of the state, civil society institutions, business and international partners, which creates synergy, without which it is impossible to ensure the stability of the information space in conditions of global interdependence; 5) is aimed at forming a sustainable information ecosystem that provides not only protection from threats, but also creates the prerequisites for innovative scientific and technological development of the state and society, preservation of cultural identity, formation of critical thinking in society and increasing the level of information literacy of citizens in the long term.

Keywords: national security, information security, public information sphere, digitalization, information threats, disinformation, cyber defense, state policy, public administration, digital governance, information space.

Постановка проблеми. Сучасні глобалізаційні процеси, динамічний розвиток цифрових технологій та інтенсивне поширення інформаційно-комунікаційних систем обумовлюють формування нового виміру національної безпеки, що безпосередньо пов'язаний із публічно-інформаційною сферою. У такому контексті інформація постає як стратегічний ресурс держави, суспільства та окремої особи, від рівня достовірності, відкритості та захищеності якого залежить ефективність реалізації національних інтересів. Водночас зростання масштабів інформаційних загроз, поширення дезінформаційних кампаній, кібератак, а також технологій когнітивного та маніпулятивного впливу у публічному середовищі істотно підвищує ризики дестабілізації політичної системи, знижує рівень суспільної довіри до органів влади та ускладнює функціонування демократичних інститутів. У таких умовах забезпечення інформаційної безпеки стає не лише елементом національної безпеки, але й ключовим чинником стійкості соціально-політичної системи.

Попри наявність значної кількості наукових праць у досліджуваній сфері, понятійно-категоріальний апарат, який відображає сутність національної безпеки у публічно-інформаційному аспекті, залишається фрагментарним. У правовій доктрині відсутня єдина концепція, яка б комплексно розкривала природу цього явища, визначала його функціональне місце у системі національних інтересів та окреслювала специфіку правових і інституційних механізмів забезпечення в системі публічного управління. Наведене актуалізує необхідність поглибленого теоретико-правового осмислення феномену національної безпеки у публічно-інформаційній сфері як підгрунтя для розробки концептуальних підходів ефективної моделі державної політики у сфері інформаційної безпеки, здатної протидіяти викликам глобалізованого цифрового середовища та гарантувати стійкість демократичного розвитку України.

Аналіз останніх досліджень та публікацій. Значний внесок у розвиток дослідження проблематики національної безпеки в публічно-інформаційній сфері здійснили зокрема такі науковці: Димитрієв В., Воронкова О., Глазунова Н., Іванов В., Козлов Ю., Колпаков В., Кузенко Л., Лазарєв Б., Логінов О., Макаренко А., Малиновський В., Опришко В., Рябченко О. та інші. Наукові розробки цих дослідників формують теоретико-методологічну основу подальших досліджень державної інформаційної політики, спрямованої на зміцнення національної безпеки в публічно-інформаційній сфері та забезпечення стійкості інформаційного простору держави.

Метою статті є здійснення теоретико-правового аналізу концептуального розуміння національної безпеки у публічно-інформаційній сфері.

Виклад основного матеріалу дослідження. В умовах глобалізації та цифровізації національна безпека постає не лише як традиційний комплекс заходів у політичній, економічній чи військовій сферах, але й як система забезпечення стійкості держави у публічно-інформаційному просторі. Цифровізація публічних процесів підвищує прозорість діяльності влади, сприяє зменшенню бар'єрів між державою та громадянами, а також формує передумови для партнерської взаємодії. Правове регулювання у цій сфері спрямоване на координацію відносин між суб'єктами національної безпеки та створення умов для досягнення оптимального рівня захищеності у політичній, правовій, інформаційній та інших сферах [1, с. 73]. Цей вимір стає ключовим у формуванні суспільної свідомості, впливі на політичні процеси та гарантуванні дотримання прав і свобод людини в інформаційному суспільстві.

Інформаційна сфера постає як багатовимірний соціально-комунікаційний простір, що інтегрує процеси продукування, акумулювання, трансляції, збереження та практичного використання знань і даних у публічно-суспільному вимірі. Її функціонування водночас детермінує інноваційний розвиток держави та суспільства і формує спектр структурних уразливостей, здатних трансформуватися у загрози національній безпеці. Воронкова О. пропонує розглядати інформаційну сферу у двох площинах: у вузькому сенсі – як відносно самостійну систему, у широкому – як універсальний елемент, що охоплює всі інші сфери (економічну, політичну, культурну, соціальну) [2, с. 577]. Інформаційна сфера також розглядається як кінцевий обсяг осмисленого інформаційного простору; сукупність інформації, інформаційної інфраструктури, суб'єктів, які здійснюють збір, формування, розповсюдження і використання інформації, а

також системи регулювання громадських відносин, що виникають при цьому; сфера діяльності суб'єктів, пов'язана зі створенням, перетворенням і споживанням інформації; сукупність інформаційних ресурсів, системи формування, поширення і використання інформації, інформаційної інфраструктури; суспільних відносин, що складаються у зв'язку з формуванням, передачею, розповсюдженням і збереженням інформації тощо… [3; 4]. Водночас інформаційні технології визначають не лише вектори економічного й культурного розвитку, але й створюють нові комплексні загрози, які охоплюють поширення дезінформаційних потоків, трансляцію пропагандистських наративів, маніпулятивний вплив на суспільну свідомість, зовнішнє втручання у виборчі процеси, а також кіберзлочинність, кібершпигунство та масштабні психологічні операції, спрямовані на дестабілізацію соціально-політичних систем. У сучасному глобалізаційному контексті ці виклики набувають чітко вираженого геополітичного виміру, оскільки інформаційний простір стає ареною міждержавної конкуренції, гібридних протистоянь і боротьби за домінування у сфері комунікаційних ресурсів. У цій парадигмі інформаційна безпека постає як ключова складова національної безпеки, що інтегрує механізми захисту особи, суспільства і держави від деструктивних інформаційних впливів, одночасно забезпечуючи умови для вільного, об'єктивного й неупередженого доступу до достовірних даних та зміцнення інформаційного суверенітету у глобальному вимірі.

Шевченко М. пропонує виокремлювати три підходи до розуміння інформаційної безпеки: статичний (як стан захищеності інформаційного простору), діяльнісний (як процес її забезпечення) та комплексний (як поєднання стану і процесу). Найбільш адекватним сучасним умовам, на його думку, є саме комплексний підхід, адже він дозволяє розглядати інформаційну безпеку як стан і водночас як динамічну діяльність держави щодо збереження й розвитку інформаційної сфери навіть в умовах загроз [5, с. 138]. Дослідник також акцентує увагу на тому, що у рамках комплексного підходу інформаційну безпеку України доцільно розглядати як стан, за якого в умовах протидії реальним і потенційним загрозам забезпечуються самозбереження, сталий і прогресивний розвиток інформаційної сфери, захищеність інформаційної інфраструктури, простору, ресурсів, процесів та їх суб'єктів, а також досягнення національних цілей і реалізація національних інтересів у цій сфері [5, с. 138].

Загалом, аналізуючи концептуальні підходи до розуміння національної безпеки у публічно-інформаційній сфері, можна виокремити три ключових підходи:

– *традиційний*, в межах якого безпека розглядається як комплекс заходів щодо захисту суверенітету, територіальної цілісності та конституційного ладу держави від потенційних загроз [6, с. 161].

– *системний* – передбачає дослідження будь-якої системи крізь призму її цільових орієнтирів, суб'єктів, залучених до процесу функціонування та забезпечення, об'єктів, на які спрямовано механізми впливу, а також інституційно-організаційних і нормативно-регулятивних механізмів, що підтримують її стабільність та ефективність. У межах такого підходу інформаційна безпека визначається як багатовимірна система, метою якої є захист ключових об'єктів – інформації, знань та інформаційних систем, що функціонують у фінансово-господарській, політичній, військовій та технологічній сферах – від широкого спектра загроз, включно з несанкціонованим доступом, неправомірним використанням, несанкціонованим розкриттям, порушенням цілісності, модифікацією чи знищенням [7]. Тобто безпека інтерпретується як динамічна взаємодія цілей, суб'єктів, об'єктів і механізмів, а інформаційний компонент постає ключовою умовою збереження суспільної довіри до державних інституцій та ефективної протидії загрозам.

У цьому контексті системний підхід передбачає органічний взаємозв'язок політичних, економічних, соціальних та інформаційних детермінант безпеки, де публічно-інформаційна сфера виконує роль визначальної структурної складової. Саме від її якості залежить рівень упорядкованості національного інформаційного простору, ступінь суспільної довіри до владних інститутів, а також потенціал держави у протидії сучасним інформаційним загрозам. Відповідно, публічно-інформаційний вимір безпеки слід розглядати як ключовий для концептуалізації національної безпеки в умовах глобалізаційних трансформацій.

– *комплексний (інтегративний)* – передбачає синергетичне поєднання правових, технологічних та організаційних інструментів у єдиній концептуальній моделі протидії сучасним загрозам. Такий підхід ґрунтується на інтеграції механізмів правового регулювання, інституційних заходів держави, інноваційних технологічних рішень та соціальних практик, спрямованих на формування стійкої архітектоніки інформаційного простору.

У межах даного підходу національна безпека у публічно-інформаційній сфері інтерпретується як багаторівнева система, здатна нейтралізувати широкий спектр ризиків, серед яких: поширення дезінформації та фейкових повідомлень, організація та реалізація кібератак, маніпулятивний вплив на громадську свідомість, а також спроби зовнішнього втручання у політичні процеси. Ефективність функціонування цієї системи забезпечується завдяки скоординованій взаємодії державних інституцій, структур громадянського суспільства, суб'єктів приватного сектору та міжнародних партнерів.

Прикладом реалізації таких функцій є діяльність Центру стратегічних комунікацій та інформаційної безпеки, який здійснює протидію пропаганді, проводить моніторинг та аналітичне оцінювання загроз у публічно-інформаційній сфері, а також бере участь у формуванні державної стратегії інформаційної безпеки [8].

Комплексний підхід до розуміння національної безпеки у публічно-інформаційній сфері дозволяє

враховувати багатовимірність сучасних інформаційних загроз, забезпечує системність, інтеграцію різних інструментів і координацію суб'єктів, створюючи передумови не лише для нейтралізації ризиків, але й для сталого розвитку інформаційного простору.

В контексті наведеного особливої актуальності набуває врахування та імплементація позитивного міжнародного досвіду, насамперед європейського. Перспективи імплементації європейського досвіду в Україні залишаються значними, водночас вимагають системного й комплексного підходу. Зокрема, у науковій літературі виокремлюється низка ключових напрямів адаптації європейських практик, серед яких: гармонізація національного законодавства з нормами Європейського Союзу у сфері захисту персональних даних і цифрової безпеки; розвиток електронного урядування, зокрема подальше розширення функціональних можливостей платформи «Дія»; інституціоналізація кіберзахисту шляхом створення Національного центру кібербезпеки та запровадження стандартів безпеки відповідно до європейських норм; налагодження партнерства з міжнародними ІТ-компаніями для протидії дезінформаційним кампаніям; подолання цифрової нерівності між регіонами шляхом реалізації інфраструктурних проєктів і програм цифрової освіти; удосконалення механізмів публічного управління інформаційною сферою шляхом формування єдиного координаційного органу, відповідального за розроблення та впровадження цифрових стратегій [9]. Реалізація зазначених заходів створить передумови для наближення України до європейських стандартів у сфері інформаційної політики, водночас забезпечуючи підвищення рівня цифровізації публічного управління, зміцнення системи кіберзахисту та формування конкурентоспроможного інформаційного суспільства. З огляду на стратегічне значення інформаційного простору для гарантування національної безпеки та сталого економічного розвитку, адаптація європейських практик має розглядатися як один із пріоритетних напрямів державної політики України у середньо- та довгостроковій перспективі.

Узагальнюючи, можемо зробити **висновок**, що концептуальне розуміння національної безпеки у публічно-інформаційній має ґрунтуватися саме на комплексному підході, який є найбільш релевантним у сучасних умовах зростання гібридних загроз, оскільки він: 1) поєднує елементи традиційного (захист держави від реальних і потенційних загроз, насамперед воєнно-політичного характеру) та системного (узгодженість цілей, суб'єктів, об'єктів і механізмів забезпечення безпеки) підходів, але водночас виходить за їхні межі, дозволяючи розглядати безпеку не лише крізь призму воєнно-політичних аспектів, але й у більш широкому контексті – правовому, соціальному, економічному, інформаційно-технологічному вимірах; 2) розглядає національну безпеку у публічно-інформаційній сфері як динамічну поліструктурну систему, здатну протидіяти як технологічним (кібератаки, несанкціонований доступ, деструктивне втручання у критичні інформаційні інфраструктури), так і соціально-психологічним (маніпуляції суспільною свідомістю, поширення пропаганди, дезінформації) загрозам, що відповідає реаліям сучасного інформаційного суспільства; 3) забезпечує гнучкість та адаптивність відповідно до швидкої динаміки інформаційного середовища, інтегруючи правові механізми, інституційні рішення, інноваційні технології та соціальні практики, що створює умови для оперативної реакції на нові форми інформаційних атак, які традиційні підходи не завжди враховують; 4) передбачає системну кооперацію та взаємодію держави, інституцій громадянського суспільства, бізнесу та міжнародних партнерів, що створює синергію, без якої неможливо забезпечити стійкість інформаційного простору в умовах глобальної взаємозалежності; 5) спрямований на формування стійкої інформаційної екосистеми, яка забезпечує не лише захищеність від загроз, але й створює передумови для інноваційного науково-технологічного розвитку держави та суспільства, збереження культурної ідентичності, формування критичного мислення у суспільстві та підвищення рівня інформаційної грамотності громадян у довгостроковій перспективі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Новікова Н., Бойко Л. Цифровізація та національна безпека: тенденції та виклики. *Національна безпека: право та економіка*. 2024. № 1(1). С. 72–77.

2. Воронкова О. Інформаційна сфера України в умовах сталого розвитку. *Юридичний науковий електронний журнал*. 2024. № 11. С. 574–579

3. Дубняк К. Інформаційний простір: структура та функціональні параметри. *Держава та регіони.* Серія: Соціальні комунікації. 2015. № 4. С. 21–25.

4. Кізляр В. До питання визначення змісту поняття «інформаційні відносини». *Університетські наукові записки*. 2019. № 69–70. С. 114–123

5. Шевчук М. До питання ґенези поняття інформаційної безпеки як складової національної безпеки. *Науковий вісник Ужгородського Національного Університету. Серія ПРАВО.* 2023. Вип. 78. Ч. 2. С. 134–139.

6. Козьяков І. Законодавче визначення державної безпеки: проблеми теорії та практики. *Підприємство, господарство і право.* 2019. № 9. С. 160–164.

7. Яровенко Г. Системний підхід до формалізації поняття «інформаційна безпека». *Причорноморські економічні студії.* 2018. № 34. С. 239–244.

8. Протидія дезінформації в умовах гібридної війни: український досвід. Центр стратегічних комунікацій та інформаційної безпеки. 2023. URL: https://spravdi.gov.ua/

9. Димитрієв В. Державна політика розвитку інформаційної сфери в Україні: дис. ... канд. наук з держ. упр.: 25.00.02 – механізми державного управління. Житомир, 2024. 200 с.

REFERENCES:

1. Novikova, N., Boiko, L. (2024). Tsyfrovizatsiia ta natsionalna bezpeka: tendentsii ta vyklyky. [Digitalization and national security: trends and challenges]. *Natsionalna bezpeka: pravo ta ekonomika. №1(1).* 72–77. [in Ukrainian].
2. Voronkova, O. (2024). Informatsiina sfera Ukrainy v umovakh staloho rozvytku. [Information sphere of Ukraine in conditions of sustainable development]. *Yurydychnyi naukovyi elektronnyi zhurnal. №11.* 574–579. [in Ukrainian].
3. Dubniak, K. (2015). Informatsiinyi prostir: struktura ta funktsionalni parametry. [Information space: structure and functional parameters]. *Derzhava ta rehiony. Seriia: Sotsialni komunikatsii. №4*. 21–25. [in Ukrainian].
4. Kizliar, V. (2019). Do pytannia vyznachennia zmistu poniattia «informatsiini vidnosyny». [On the issue of defining the content of the concept of "information relations"]. *Universytetski naukovi zapysky. № 69–70.* 114–123. [in Ukrainian].
5. Shevchuk, M. (2023). Do pytannia genezy poniattia informatsiinoi bezpeky yak skladovoi natsionalnoi bezpeky. [On the question of the genesis of the concept of information security as a component of national security]. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu. Seriia PRAVO. Vyp. 78. Ch. 2.* 134–139. [in Ukrainian].
6. Koziakov, I. (2019). Zakonodavche vyznachennia derzhavnoi bezpeky: problemy teorii ta praktyky. [Legislative definition of state security: problems of theory and practice]. *Pidpryiemstvo, hospodarstvo i pravo. №9.* 160–164. [in Ukrainian].
7. Yarovenko, H. (2018). Systemnyi pidkhid do formalizatsii poniattia «informatsiina bezpeka». [A systematic approach to formalizing the concept of "information security"]. *Prychornomorski ekonomichni studii. №34.* 239–244. [in Ukrainian].
8. Protydiia dezinformatsii v umovakh hibrydnoi viiny: ukrainskyi dosvid. (2023). [Countering disinformation in the context of hybrid warfare: Ukrainian experience]. Tsentr stratehichnykh komunikatsii ta informatsiinoi bezpeky. Retrieved from: https://spravdi.gov.ua/ [in Ukrainian].
9. Dymytriiev, V. (2024). Derzhavna polityka rozvytku informatsiinoi sfery v Ukraini. [State policy for the development of the information sphere in Ukraine]. *Dys. kand. nauk z derzh. upr. 25.00.02 – mekhanizmy derzhavnoho upravlinnia.* 200. [in Ukrainian].

Стаття надійшла до редакції 14.06.2025

УДК 343.2
DOI: 10.36550/2522-9230-2025-18-347-351

Кричун Юрій Анатолійович,
кандидат юридичних наук, доцент,
доцент кафедри права та правоохоронної діяльності, адвокат
Центральноукраїнського державного університет
імені Володимира Винниченка
uriykrichun@gmail.com
ORCID ID: 0000-0002-9441-3003

РОЛЬ КРИМІНАЛЬНО-ПРАВОВОЇ ПОЛІТИКИ У ЗАБЕЗПЕЧЕННІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В УМОВАХ ВІЙНИ

У статті досліджено роль кримінально-правової політики України у забезпеченні національної безпеки в умовах воєнного стану. Акцент зроблено на її багатофункціональному призначенні, яке виходить за межі традиційних каральної та охоронної функцій. Наголошено, що в сучасних умовах кримінально-правова політика має стратегічне значення, оскільки формує передумови для відновлення правопорядку, забезпечення справедливості, довіри громадян до державних інституцій та інтеграції України в міжнародні механізми захисту прав людини й протидії злочинності.

У роботі встановлено, що у період дії режиму воєнного стану суб'єкти формування кримінально-правової політики продемонстрували високу продуктивність нормотворчої діяльності. Зокрема, проаналізовано ухвалення 24 законів, спрямованих на реалізацію завдань кримінального права у сфері охорони національної безпеки. Разом з тим звернено увагу на наявність проблем у забезпеченні належної якості цих нормативно-правових актів, що ускладнює їх практичне застосування та знижує ефективність кримінально-правового впливу.

Значну увагу приділено практиці застосування кримінального законодавства у період війни. Відзначено різке зростання кількості кримінальних проваджень, пов'язаних із злочинами проти основ національної безпеки України, зокрема тих, що завершилися постановленням обвинувальних вироків. Це свідчить про адаптацію правоохоронних