МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДНІПРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

Кваліфікаційна наукова
праця на правах рукопису

РЯПОЛОВ АНТОН ПАВЛОВИЧ

УДК 342.1:321.011:65.012.8

ДИСЕРТАЦІЯ

ІНФОРМАЦІЙНА БЕЗПЕКА В УМОВАХ ВОЄННОГО СТАНУ: ТЕОРЕТИКО-ПРАВОВА ХАРАКТЕРИСТИКА

08 Право
081 Право

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ А. П. Ряполов

Науковий керівник:
Наливайко Лариса Романівна,
доктор юридичних наук, професор,
Заслужений юрист України,
академік Національної академії наук
вищої освіти України

Дніпро – 2026

АНОТАЦІЯ

Ряполов А. П. Інформаційна безпека в умовах воєнного стану: теоретико-правова характеристика. – *Кваліфікаційна наукова праця на правах рукопису.*

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 081 – Право. – Дніпровський державний університет внутрішніх справ Міністерства внутрішніх справ України, Дніпро, 2026.

Дисертація є однією із перших у вітчизняній науці, в якій здійснено комплексне теоретико-правове обґрунтування змісту, структури та механізмів забезпечення інформаційної безпеки України в умовах воєнного стану та євроінтеграції, систематизовано існуючі проблеми, розроблено науково обґрунтовані рекомендації щодо їх подолання, а також сформульовано практичні рекомендації, спрямовані на підвищення рівня кіберзахищеності та забезпечення інформаційного суверенітету держави

У роботі доведено, що інформаційна безпека є багатовимірним, динамічним і складним соціально-правовим явищем, яке охоплює правові, політичні, технологічні, організаційні та соціогуманітарні аспекти функціонування сучасної держави. Встановлено, що сучасні вітчизняні та зарубіжні наукові підходи до дослідження інформаційної безпеки відображають тенденцію до формування інтегрованих методологічних моделей, що ґрунтуються на міждисциплінарності, ризик-орієнтованому підході, концепції кіберстійкості, мережевому аналізі та багаторівневому безпековому врядуванні. Сформована методологічна конструкція дослідження інформаційної безпеки України створює теоретико-методологічне підґрунтя для подальшого розвитку правових засад її забезпечення, а також для вдосконалення нормативного та інституційного механізму функціонування системи інформаційної безпеки в умовах воєнного стану.

Обґрунтовано, що сучасний етап розвитку інформаційної безпеки України характеризується її трансформацією у самостійний функціональний елемент системи національної безпеки, який набуває особливого значення в умовах гібридної війни, збройної агресії та інтенсивного інформаційного протиборства. Інформаційний

простір розглядається як окремий стратегічний домен конфлікту, у межах якого реалізуються інформаційно-психологічні операції, кібератаки, дезінформаційні кампанії та інші форми впливу, що безпосередньо впливають на стабільність державних інституцій, суспільну свідомість та національну безпеку в цілому.

Встановлено, що у науковій літературі відсутній уніфікований підхід до розуміння інформаційної безпеки, що зумовлює домінування міждисциплінарної парадигми її дослідження. У межах цієї парадигми інформаційна безпека розглядається як інтегрована категорія, що поєднує правові, безпекові, політичні, соціально-комунікаційні та технологічні виміри. Доведено, що інформаційна безпека має бути осмислена не лише як об'єкт правового регулювання, а й як стратегічний ресурс держави, що визначає рівень її стійкості, ефективність системи публічного управління, здатність до протидії зовнішнім впливам та забезпечення інформаційного суверенітету.

Розкрито сутність інформаційної безпеки як складової національної безпеки України, що являє собою безперервний процес і результат забезпечення стану захищеності життєво важливих інтересів людини, суспільства і держави в інформаційній сфері від реальних і потенційних, внутрішніх і зовнішніх загроз. Визначено її основні ознаки, зокрема системність, багаторівневість, нормативну визначеність, динамічність, комплексність та взаємозв'язок з іншими складовими національної безпеки. Окремо обґрунтовано елементи інформаційної безпеки, які включають об'єкти захисту, систему загроз та механізми забезпечення.

Систематизовано загрози інформаційній безпеці України в умовах воєнного стану. Внутрішні загрози охоплюють недостатній рівень медіаграмотності населення, недосконаліть нормативно-правового та інституційного забезпечення, низьку ефективність державної інформаційної політики, вразливість критичної інформаційної інфраструктури, недостатній рівень захисту персональних даних та кіберпростору, а також неефективність реагування на інформаційні маніпуляції. Зовнішні загрози включають комплексну інформаційну агресію проти України, діяльність іноземних спецслужб, кібератаки, інформаційно-психологічні операції, дезінформаційні кампанії, втручання у внутрішньополітичні процеси, а також

поширення новітніх форм інформаційної та кібернетичної зброї в глобальному інформаційному просторі.

Адаптація зарубіжного досвіду забезпечення інформаційної безпеки ґрунтується на принципі пропорційності та спрямована на узгодження заходів національної безпеки з європейськими стандартами прав людини. Запропоновано системну нормативно-правову модель регулювання, характерну для низки європейських держав, яка поєднує норми інформаційного, безпекового та адміністративного права та підвищує узгодженість правового регулювання в умовах кризових і воєнних загроз. Наголошено на посиленні ролі стратегічних комунікацій як функції сектору безпеки і оборони, розвитку державно-приватного партнерства у сфері кібербезпеки та необхідності післявоєнного перегляду обмежувальних правових режимів для забезпечення балансу між безпекою та інформаційними правами. Поєднання публічно-правових інструментів із механізмами державно-приватного партнерства у сфері кібербезпеки дозволяє підвищити стійкість інформаційних систем без надмірного розширення державного контролю. Потрібен післявоєнний перегляд правових режимів, запроваджених у сфері інформаційної безпеки, через можливість існування ризику збереження надзвичайних обмежень поза межами їх фактичної необхідності, що зумовлює потребу забезпечення балансу між безпековими обмеженнями та гарантіями інформаційних прав.

Обґрунтовано необхідність системної модернізації правового забезпечення інформаційної безпеки України на основі гармонізації національного законодавства з міжнародними стандартами та правом Європейського Союзу. Правове забезпечення інформаційної безпеки здійснюється на трьох взаємопов’язаних рівнях: у сфері національної безпеки і оборони; у сфері інформаційних відносин та інформаційної безпеки; а також у сфері правового статусу суб’єктів забезпечення інформаційної безпеки. Нормативно-правову основу становлять Конституція та закони України, підзаконні нормативно-правові акти, а також міжнародні договори, згоду на обов’язковість яких надано ВРУ. Міжнародні стандарти у сфері інформаційної безпеки мають переважно орієнтовний характер і використовуються як важливий орієнтир для гармонізації та розвитку національної правової системи, тоді як держава

самостійно визначає способи та обсяг реалізації національних інтересів в інформаційній сфері з урахуванням характеру загроз і наявних можливостей. Актуальним є завдання систематизації, узгодження та гармонізації інформаційного законодавства, що передбачає уточнення термінології, вдосконалення механізмів реалізації правових норм та імплементацію європейських стандартів, зокрема через можливе прийняття єдиного кодифікованого акта – Інформаційного кодексу України.

Визначено, що інституційна складова забезпечення інформаційної безпеки становить організовану систему уповноважених суб'єктів, діяльність яких нормативно врегульована та спрямована на формування і реалізацію державної політики у сфері інформаційної безпеки, а також на забезпечення належного рівня захищеності життєво важливих інтересів особи, суспільства і держави в інформаційній сфері. Визначено, що система суб'єктів забезпечення інформаційної безпеки України включає інституції державного сектору (ВРУ, Президент України, РНБО України, КМУ, органи сектору безпеки і оборони та ін.) і недержавні інституції (органи місцевого самоврядування, інститути громадянського суспільства та ін.).

Встановлено, що в Україні відсутній єдиний централізований орган, відповідальний за забезпечення інформаційної безпеки, що в умовах воєнного стану зумовлює необхідність посилення спроможності наявних суб'єктів та удосконалення міжвідомчої координації. Доведено, що ключовими проблемами інституційного забезпечення є фрагментарність системи, недостатній рівень координації, нечіткий розподіл функцій і відповідальності між суб'єктами, обмежена інституційна спроможність окремих органів, слабка інтеграція недержавних акторів, а також низький рівень інформаційної та медіаграмотності населення. Обґрунтовано напрями удосконалення інституційного забезпечення інформаційної безпеки, які передбачають систематизацію та кодифікацію нормативно-правової бази, узгодження функцій і повноважень ключових суб'єктів, розвиток механізмів публічно-приватного партнерства та координації між державними і недержавними учасниками, зміцнення інституційної спроможності шляхом удосконалення кадрового, фінансового, наукового й технічного забезпечення, а також активізацію стратегічних комунікацій і підвищення рівня інформаційної та медіаграмотності населення.

Окремий блок дослідження присвячено розвитку кібербезпеки як ключового компонента інформаційної безпеки держави. Встановлено, що існуюча нормативно-правова та інституційна система кібербезпеки недостатньо враховує специфіку воєнного стану та сучасних кіберзагроз. Обґрунтовано необхідність закріплення принципу технологічного суверенітету, розвитку національних технологічних спроможностей, удосконалення системи кіберзахисту критичної інфраструктури, створення ефективного механізму реагування на кіберінциденти, а також формування єдиного національного координаційного центру кібербезпеки. Запропоновано напрями реформування, що включають нормативне регулювання кіберзагроз, розвиток кіберстійкості, посилення кадрового потенціалу, запровадження стандартів цифрових доказів і розширення міжнародного співробітництва.

Досліджено проблематику інформаційного та цифрового суверенітету України як стратегічної основи забезпечення державної незалежності в інформаційній сфері. Визначено їх політико-правову, організаційно-інституційну, технологічну та культурно-гуманітарну складові. Цифровий суверенітет – це категорія, що виходить за межі територіального підходу, тому потребує міжнародної співпраці та порозуміння, поваги до цифрових інтересів держави в умовах глобальної взаємодії. Суміжна категорія «суверенітет даних» передбачає, що дані мають бути підпорядковані національному законодавству держави, в якій дані збираються, зберігаються та обробляються. Глобалізаційні процеси, посилення інформаційної агресії, технологічна залежність і недостатній рівень розвитку національної інформаційної інфраструктури формують нові виклики для держави та потребують комплексної відповіді шляхом модернізації інформаційної політики, розвитку цифрових технологій, підвищення медіаграмотності населення та зміцнення міжнародного співробітництва.

Ключові слова: *інформаційна безпека, національна безпека, воєнний стан, законодавство, загрози інформаційній безпеці, інформаційні технології, інформаційний простір, кібербезпека, кіберпростір, інформаційний суверенітет, цифровий суверенітет, європейська інтеграція, Європейський Союз*

SUMMARY

Riapolov A. P. Information Security under Martial Law: a Theoretical and Legal Characterisation. – *Qualifying scientific work in manuscript form.*

Dissertation for the degree of Doctor of Philosophy in speciality 081 – Law. – Dnipro State University of Internal Affairs of the Ministry of Internal Affairs of Ukraine, Dnipro, 2026.

The dissertation is one of the first studies in Ukrainian legal scholarship to provide a comprehensive theoretical and legal substantiation of the content, structure and mechanisms for ensuring Ukraine's information security under martial law and in the context of European integration. The study systematises the existing problems, develops scientifically grounded recommendations for overcoming them, and formulates practical proposals aimed at increasing the level of cyber protection and ensuring the information sovereignty of the state.

The dissertation proves that information security is a multidimensional, dynamic and complex socio-legal phenomenon encompassing legal, political, technological, organisational, and socio-humanitarian aspects of the functioning of the modern state. It is established that contemporary Ukrainian and foreign scholarly approaches to the study of information security reflect a tendency towards the formation of integrated methodological models based on interdisciplinarity, a risk-oriented approach, the concept of cyber resilience, network analysis, and multi-level security governance. The methodological framework developed for the study of Ukraine's information security creates a theoretical and methodological basis for the further development of the legal foundations of its provision, as well as for improving the regulatory and institutional mechanism of the information security system under martial law.

It is substantiated that the current stage in the development of Ukraine's information security is characterised by its transformation into an independent functional element of the national security system, which acquires particular importance in the context of hybrid warfare, armed aggression and intensive information confrontation. The information space is considered as a separate strategic domain of conflict within which information and

psychological operations, cyberattacks, disinformation campaigns and other forms of influence are carried out, directly affecting the stability of state institutions, public consciousness and national security as a whole.

It is established that there is no unified approach in scholarly literature to understanding information security, which determines the dominance of an interdisciplinary paradigm in its study. Within this paradigm, information security is viewed as an integrated category combining legal, security-related, political, socio-communicative and technological dimensions. It is proven that information security should be understood not only as an object of legal regulation, but also as a strategic resource of the state, determining the level of its resilience, the effectiveness of the public administration system, its ability to counter external influences and to ensure information sovereignty.

The essence of information security as a component of Ukraine's national security is revealed as both a continuous process and a result of ensuring the protected state of the vital interests of the individual, society and the state in the information sphere against real and potential, internal and external threats. Its main features are identified, including systemic nature, multi-level structure, normative certainty, dynamism, complexity and interconnection with other components of national security. The elements of information security are separately substantiated, including objects of protection, the system of threats and mechanisms of provision.

Threats to Ukraine's information security under martial law are systematised. Internal threats include the insufficient level of media literacy among the population, shortcomings in regulatory and institutional support, the low effectiveness of state information policy, the vulnerability of critical information infrastructure, the insufficient level of protection of personal data and cyberspace, as well as the ineffective response to information manipulation. External threats include comprehensive information aggression against Ukraine, the activities of foreign special services, cyberattacks, information and psychological operations, disinformation campaigns, interference in domestic political processes, and the spread of new forms of information and cyber weapons in the global information space.

The adaptation of foreign experience in ensuring information security is based on the principle of proportionality and is aimed at aligning national security measures with European human rights standards. A systematic regulatory model, typical of a number of European states, is proposed. This model combines norms of information, security and administrative law and increases the coherence of legal regulation in the context of crisis and wartime threats. Emphasis is placed on strengthening the role of strategic communications as a function of the security and defence sector, developing public-private partnership in the field of cybersecurity, and ensuring the need for a post-war review of restrictive legal regimes in order to maintain a balance between security and information rights. The combination of public-law instruments with mechanisms of public-private partnership in cybersecurity makes it possible to increase the resilience of information systems without excessively expanding state control. A post-war review of the legal regimes introduced in the field of information security is necessary, since there is a risk that emergency restrictions may remain in force beyond the limits of their actual necessity. This determines the need to maintain a balance between security restrictions and guarantees of information rights.

The dissertation substantiates the need for the systematic modernisation of the legal framework for ensuring Ukraine's information security on the basis of harmonising national legislation with international standards and European Union law. The legal provision of information security is carried out at three interconnected levels: in the field of national security and defence; in the field of information relations and information security; and in the field of the legal status of entities responsible for ensuring information security. The regulatory basis consists of the Constitution and laws of Ukraine, subordinate regulatory legal acts, as well as international treaties consented to as binding by the Verkhovna Rada of Ukraine. International standards in the field of information security are mainly guiding in nature and are used as an important reference point for the harmonisation and development of the national legal system, whereas the state independently determines the means and scope of implementing national interests in the information sphere, taking into account the nature of threats and available capabilities. The task of systematising, coordinating and harmonising information legislation remains relevant. This includes

clarifying terminology, improving mechanisms for implementing legal norms and introducing European standards, including through the possible adoption of a single codified act, namely the Information Code of Ukraine.

It is determined that the institutional component of ensuring information security constitutes an organised system of authorised entities whose activities are regulated by law and aimed at the formation and implementation of state policy in the field of information security, as well as at ensuring an appropriate level of protection of the vital interests of the individual, society and the state in the information sphere. It is established that the system of entities responsible for ensuring Ukraine's information security includes institutions of the state sector, such as the Verkhovna Rada of Ukraine, the President of Ukraine, the National Security and Defence Council of Ukraine, the Cabinet of Ministers of Ukraine, bodies of the security and defence sector and others, as well as non-state institutions, including local self-government bodies, civil society institutions and others.

It is established that Ukraine lacks a single centralised body responsible for ensuring information security. Under martial law, this necessitates strengthening the capacity of existing entities and improving inter-agency coordination. It is proven that the key problems of institutional support are the fragmentation of the system, insufficient coordination, an unclear distribution of functions and responsibilities between entities, limited institutional capacity of individual bodies, weak integration of non-state actors, and a low level of information and media literacy among the population. The directions for improving the institutional support of information security are substantiated. They include the systematisation and codification of the regulatory framework, the coordination of the functions and powers of key entities, the development of mechanisms of public-private partnership and coordination between state and non-state participants, the strengthening of institutional capacity through the improvement of staffing, financial, scientific and technical support, as well as the intensification of strategic communications and the enhancement of information and media literacy among the population.

A separate part of the study is devoted to the development of cybersecurity as a key component of the state's information security. It is established that the existing regulatory and institutional system of cybersecurity does not sufficiently take into account the specific

nature of martial law and contemporary cyber threats. The need to enshrine the principle of technological sovereignty, develop national technological capabilities, improve the system of cyber protection of critical infrastructure, create an effective mechanism for responding to cyber incidents, and establish a single national cybersecurity coordination centre is substantiated. The dissertation proposes areas of reform, including the regulatory definition of cyber threats, the development of cyber resilience, the strengthening of human resources capacity, the introduction of standards for digital evidence, and the expansion of international cooperation.

The dissertation examines the issue of Ukraine's information and digital sovereignty as a strategic basis for ensuring state independence in the information sphere. Their political and legal, organisational and institutional, technological, and cultural-humanitarian components are identified. Digital sovereignty is a category that goes beyond the territorial approach and therefore requires international cooperation and mutual understanding, as well as respect for the digital interests of the state in the context of global interaction. The related category of data sovereignty means that data should be subject to the national legislation of the state in which such data are collected, stored and processed. Globalisation processes, the intensification of information aggression, technological dependence and the insufficient level of development of national information infrastructure create new challenges for the state and require a comprehensive response through the modernisation of information policy, the development of digital technologies, the improvement of media literacy among the population and the strengthening of international cooperation.

Keywords: *information security, national security, martial law, legislation, threats to information security, information technologies, information space, cybersecurity, cyberspace, information sovereignty, digital sovereignty, European integration, European Union.*

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковано основні наукові результати дисертації:

1. Ряполов А. П. Нормативно-правові основи інформаційної безпеки України в умовах гібридної агресії. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2025. Т. 3, № 89. С. 87-91. URL: https://visnyk-pravo.uzhnu.edu.ua/article/view/336476/325112

2. Ряполов А. П. Гібридна агресія проти України як виклик модернізації правової політики у сфері інформаційної безпеки. *Український політико-правовий дискурс.* 2025. № 10. С. 1-14. URL: https://ppdnz.com.ua/index.php/home/article/view/236/151

3. Ряполов А. П. Захист інформаційного простору України в умовах гібридної війни: межі між свободою слова та інформаційною безпекою. *Національні інтереси України.* 2025. № 5 (10). С. 746-757. URL: https://perspectives.pp.ua/index.php/niu/article/view/23746/23719

Наукові праці, які засвідчують апробацію матеріалів дисертації:

1. Ряполов А. П. Теоретико-правова характеристика інформаційної безпеки в умовах воєнного стану. *Modernization of science and its influence on global processes:* collection of scientific papers «SCIENTIA» with Proceedings of the III International Scientific and Theoretical Conference, Bern, April 14, 2023. Bern, Swiss Confederation : European Scientific Platform, 2023. P. 41-43.

2. Ряполов А. П. Окремі напрями удосконалення забезпечення інформаційної безпеки в умовах війни. *Science and Practice: Implementation to Modern Society:* with the Proceedingsof the 14 th International Scientific and Practical, Manchester, April 26-28, 2023. Manchester : Peal Press Ltd., 2023. P. 303-307.

3. Ряполов А. П. Співвідношення понять «інформаційна безпека» та «безпека інформації» у сучасному науковому просторі. *Актуальні проблеми державотворення та правозастосування :* матер. Всеукр. наук.-практ. конф., м. Дніпро, 7 груд. 2023 р. Дніпро : ДДУВС, 2024. С. 143-146.

4. Ряполов А. П. Організаційно-правові питання взаємодії органів публічної влади у сфері забезпечення інформаційної безпеки України. *Права людини і громадянина під час дії воєнного стану*: зб. наук. ст. за матеріалами наук.-практ. конф. з нагоди 75-ї річниці Заг. декларації прав людини, м. Харків, 8 груд. 2023 р.: електрон. наук. вид. Харків : Право, 2023. С. 260-264.

5. Ряполов А. П. Інформаційна безпека України в умовах воєнного стану: проблеми та перспективи. *Юридична весна: права людини в умовах воєнного стану:* збірник тез наук.-практ. конф., м. Харків, 15 квітня 2024 р. Харків : Національний юридичний університет імені Ярослава Мудрого, 2024. С. 170-175.

6. Ряполов А. П. Інституційне забезпечення інформаційної безпеки України. *Конституційні права і свободи людини та громадянина в умовах війни та післявоєнний період* : матер. наук. семінару, м. Львів, 21 червня 2024 р. Львів : ЛьвДУВС, 2024. С. 167-170.

7. Ряполов А. П. Суб'єкти забезпечення інформаційної безпеки України. *Проблеми юридичної науки очима молодих науковців*: матеріали XVIII Всеукр. наук.-практ. онлайн-конф., м. Рівне, 17 жовтня 2024 р. Рівне : Національний університет біоресурсів та природокористування України, 2024. С. 64-67.

8. Ряполов А. П. Інформаційна безпека людини та громадянина як складова національної безпеки держави: загрози та виклики. *Міжнародна та національна безпека: теоретичні і прикладні аспекти :* матер. IX Міжнар. наук.-практ. конф., м. Дніпро, 21 березня 2025 р. ; у 2-х ч. Ч. II. Дніпро : ДДУВС, 2025. С. 458-459.

9. Ряполов А. П. Теоретико-правові засади взаємодії інституту військової експертизи з органами державної влади. *Військова експертиза в умовах сьогодення: проблемні питання та шляхи їх вирішення*: матер. Всеукр. наук.-практ. конф., м. Дніпро, 25 квітня 2025 р. Дніпро : ДНДІСЕ МЮУ, 2025. С. 151-155.

10. Ряполов А. П. Свобода вибору та межі інформаційної безпеки в умовах воєнного стану: баланс між національною безпекою та свободою вираження поглядів. *Міжнародна та національна безпека: теоретичні і прикладні аспекти:* матер. ХМіжнар. наук.-практ. конф., м. Дніпро, 16 березня 2026 р. ; у 2-х ч. Ч. II. Дніпро : ДДУВС, 2026. С. 476-477.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ВРУ – Верховна Рада України

ЄС – Європейський Союз

ЄСПЛ – Європейський суд з прав людини

ІГС – інститути громадянського суспільства

КМУ – Кабінет Міністрів України

НАТО – Організація Північноатлантичного договору

ОМС – органи місцевого самоврядування

ООН – Організація Об’єднаних Націй

РЄ – Рада Європи

РНБО України – Рада національної безпеки і оборони України

СБУ – Служба безпеки України

ТОТ – тимчасово окуповані території

р. – рік

ст. – стаття

п. – пункт

ч. – частина

ВСТУП

Обґрунтування вибору теми дослідження. У сучасних воєнних конфліктах інформаційна сфера дедалі частіше перетворюється на самостійне поле протистояння. Стрімкий розвиток інформаційних технологій, глобалізації комунікаційних мереж та зростання кіберзагроз забезпечення захисту державної, суспільної та приватної інформації стає критично важливим для стабільного функціонування держави. В умовах воєнного стану питання інформаційної безпеки України виходить на перший план, адже саме вона забезпечує захист суспільства та держави від деструктивного впливу пропаганди, кіберзагроз, маніпуляцій та інформаційних атак.

Інформаційна безпека є одним із основних елементів національної безпеки сучасної держави. Гібридна агресія проти України поєднує в собі традиційні збройні методи із масованими кібератаками, дезінформаційними кампаніями, маніпулюванням суспільною свідомістю та цілеспрямованим руйнуванням інформаційної інфраструктури держави. За таких умов інформаційна безпека перетворюється з одного з елементів національної безпеки на її стратегічну основу, від якої залежить здатність держави зберігати суверенітет, мобілізовувати суспільство та ефективно протистояти агресору.

Проведене дослідження викликано необхідністю комплексного наукового аналізу правових механізмів та нормативно-правового забезпечення інформаційної безпеки в умовах воєнного стану. Актуальність теми визначається низкою чинників, а саме: зростанням кіберзагроз та кібератак, спрямованих на державні інформаційні системи, критичну інфраструктуру та стратегічні об’єкти, що створює безпосередню загрозу національній безпеці; необхідністю вдосконалення нормативно-правової бази, що регулює інформаційну безпеку в умовах воєнного стану, з урахуванням сучасних технологічних та військово-політичних викликів; важливістю удосконалення інституційних механізмів, що забезпечують функціонування системи інформаційної безпеки, підвищенням ефективності координації між державними органами, правоохоронними структурами та сектором критичної інфраструктури; недостатньою науково-правовою розробленістю окремих аспектів інформаційної

безпеки, особливо щодо інтеграції кібербезпеки, законодавчого регулювання та адаптації зарубіжного досвіду до умов воєнного стану.

До того ж актуальність теми обґрунтована взаємозумовленими вимірами: *правовим* – ведення воєнного стану спричинило суттєву трансформацію правового регулювання інформаційних відносин. Водночас чинна нормативно-правова база демонструє значні прогалини й суперечності, які знижують ефективність державної політики у сфері інформаційної безпеки в умовах воєнного стану; *інституційним* – система органів державної влади, відповідальних за забезпечення інформаційної безпеки, формувалася переважно в мирний час і виявилася недостатньо адаптованою до умов повномасштабної агресії; *доктринальним* – незважаючи на зростання практичної значущості питань інформаційної безпеки, вітчизняна правнича наука ще не сформувала усталеного понятійно-категоріального апарату у цій сфері, а теоретико-правові дослідження подекуди відстають від динаміки суспільних відносин та законодавчих змін. Вивчення досвіду інших держав, які стикалися із збройними конфліктами та інформаційною агресією, містить цінні моделі правового та інституційного реагування, адаптація яких до українських реалій є науково та практично виправданою.

Незважаючи на існування низки наукових праць у сфері інформаційної безпеки, сучасні виклики воєнного часу висувають нові завдання щодо захисту державних інформаційних ресурсів, інфраструктури та суспільного інформаційного простору, що потребує детального теоретико-правового дослідження. *Доктринальною основою* дослідження виступили дисертаційні роботи, монографії та інші наукові праці українських і зарубіжних учених у сфері права, національної та інформаційної безпеки, політології, соціології, кібербезпеки та теорії інформаційного суспільства. Серед українських авторів, які досліджували проблематику інформаційної безпеки, кібербезпеки, інформаційного суверенітету та інформаційного протиборства в умовах воєнних конфліктів, слід відзначити таких: А. Авер’янова, В. Аніщук, І. Арістова, О. Баранов, І. Березовська, В. Брижко, Н. Влажик, В. Горбулін, В. Гурковський, В. Демиденко, О. Дзьобань, О. Довгань, О. Додонов, І. Забара, Р. Калюжний, Є. Кобко, В. Конах, О. Косогов, Б. Кормич, І. Котерлін, В. Котляров, В. Кучер,

О. Кирилюк, О. Литвиненко, В. Ліпкан, Д. Лобода, Н. Лугіна, Ю. Максименко, А. Марущак, Л. Наливайко, А. Нашинець-Наумова, Н. Ніжник, В. Остроухов, М. Панов, А. Пазюк, О. Передерій, В. Пилипчук, В. Політанський, Г. Почепцов, М. Присяжнюк, А. Самотуга, Д. Селіхов, О. Сивак, С. Стрельцов, О. Тихомиров, П. Ткачук, В. Хорошко, В. Цимбалюк, О. Юдін, О. Юнін, М. Шевчук та ін.

Зарубіжні вчені, які здійснили вагомий внесок у розвиток теорії інформаційного суспільства, кібербезпеки та цифрового суверенітету, включають таких дослідників: А. Росс Андерсон (Ross J. Anderson), Д. Белл (Daniel Bell), Ю. Бенклер (Yochai Benkler), М. Кастельс (Manuel Castells), Л. Лессіг (Lawrence Lessig), Т. Рід (Thomas C. Reed), П. Сінгер (Peter W. Singer), Е. Тоффлер (Alvin Toffler), М. Хансен (Morten Hansen), К. Шеннон (Claude Shannon), Б. Шнайєр (Bruce Schneier) та ін.

Окрім сучасних викликів для національної безпеки та інформаційного простору, вибір теми дисертації зумовлений практичною необхідністю формування ефективних правових механізмів захисту інформації в умовах воєнного стану. Результати дослідження можуть стати основою для формування ефективних державних політик та правових механізмів захисту інформаційного простору, удосконалення нормативно-правової бази та підвищення готовності держави до протидії сучасним інформаційним загрозам. Зазначене і зумовило вибір теми дослідження, визначення мети та завдань дисертаційної роботи.

Нормативно-правовим підґрунтям дослідження є міжнародні договори у сфері інформаційної безпеки, згоду на обов'язковість яких надано Верховною Радою України, Конституція України, а також система національних нормативно-правових актів, що регулюють відносини у сфері інформаційної, кібернетичної безпеки та забезпечення інформаційного суверенітету в умовах воєнного стану. *Інформаційну та емпіричну основу* дисертації становлять аналітичні звіти національних та міжнародних організацій, інформаційно-довідкові видання, статистичні дані та ін.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дослідження виконано відповідно до Стратегії національної безпеки України, затвердженої Указом Президента України від 14 вересня 2020 р. № 392/2020; Стратегії воєнної безпеки України, затвердженої Указом Президента України від

25 березня 2021 р. № 121/2021; Стратегії забезпечення державної безпеки, затвердженої Указом Президента України від 16 лютого 2022 р. № 56/2022; Переліку пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 31 грудня року, наступного після припинення або скасування воєнного стану в Україні, затвердженого постановою Кабінету Міністрів України від 30 квітня 2024 р. № 476; Тематики наукових досліджень і науково-технічних (експериментальних) розробок на 2025-2029 роки, затвердженої Наказом Міністерства внутрішніх справ України від 21 травня 2024 р. № 326; Стратегії розвитку Національної академії правових наук України на 2021-2025 рр., затвердженої постановою загальних зборів НАПрН України від 26 березня 2021 р. № 12-21 (1.11. Правове забезпечення у сфері національної безпеки та оборони).

Мета і завдання дослідження. *Мета дослідження* полягає у комплексному теоретико-правовому аналізі інформаційної безпеки України в умовах воєнного стану, розкритті її сутності, структури та місця у системі національної безпеки, оцінці ефективності нормативно-правового та інституційного забезпечення, а також розробленні науково обґрунтованих пропозицій щодо їх удосконалення з урахуванням сучасних викликів, зокрема у сфері кібербезпеки та забезпечення інформаційного суверенітету.

Для досягнення зазначеної мети у дисертації поставлено такі *завдання:*

- розкрити методологічні засади дослідження інформаційної безпеки України;
- проаналізувати стан наукової розробленості проблеми інформаційної безпеки України у вітчизняній та зарубіжній науці;
- уточнити понятійно-категоріальний апарат, визначити сутність, ознаки, структуру інформаційної безпеки України та її місце у системі національної безпеки;
- дослідити зарубіжний досвід забезпечення інформаційної безпеки в умовах воєнного конфлікту та можливості його адаптації в Україні;
- проаналізувати нормативно-правове забезпечення інформаційної безпеки України в умовах воєнного стану, виявити основні проблеми та окреслити перспективи його вдосконалення;

- охарактеризувати інституційне забезпечення інформаційної безпеки України та визначити напрями його удосконалення;

- дослідити кібербезпеку та визначити її роль у забезпеченні національної безпеки в умовах воєнного стану;

- проаналізувати проблеми забезпечення інформаційного суверенітету України в умовах воєнного стану, визначити основні тенденції та перспективи його розвитку.

Об'єктом дослідження є суспільні відносини у сфері забезпечення інформаційної безпеки як елементу національної безпеки.

Предметом дослідження є теоретико-правова характеристика інформаційної безпеки в умовах воєнного стану.

Методи дослідження. Для вирішення поставлених завдань і досягнення мети було використано комплекс загальнофілософських підходів, загальнонаукових, спеціальних та власних методів правознавства. *Діалектичний підхід* сприяв дослідженню інформаційної безпеки у динаміці, що дало змогу виявити суперечності її функціонування в умовах воєнного стану та трансформацію інформаційної сфери у самостійний простір протиборства (підрозділи 1.1, 1.3, 2.4). *Герменевтичний підхід* застосовано для тлумачення норм законодавства у сфері інформаційної безпеки та виявлення особливостей їх реалізації в умовах воєнного стану (підрозділи 2.1, 2.4). *Антропологічний підхід* забезпечив аналіз інформаційної безпеки крізь призму захисту прав і свобод людини в інформаційній сфері (підрозділи 1.3, 2.1). *Аксіологічний підхід* сприяв визначенню ціннісних орієнтирів інформаційної безпеки, зокрема балансу між безпекою держави та правами людини (підрозділи 1.3, 2.4). *Синергетичний підхід* дозволив дослідити процеси самоорганізації системи інформаційної безпеки та її здатність до адаптації в умовах криз і воєнних загроз (підрозділи 1.1, 2.2, 2.4). Використання *системного підходу* дозволило розглядати інформаційну безпеку як цілісну багаторівневу систему, а також виявити взаємозв'язок її елементів (підрозділи 1.1, 1.3, 2.1-2.4). Застосування *структурно-функціонального методу* уможливило визначення елементів інформаційної безпеки та їх функціонального призначення у системі національної безпеки (підрозділи 1.3,

2.2, 2.3). За допомогою *інституційного підходу* досліджено діяльність суб'єктів забезпечення інформаційної безпеки, механізми їх взаємодії та напрями інституційного вдосконалення (підрозділ 2.2). *Історико-правовий метод* застосовано для дослідження еволюції наукових підходів і правового регулювання інформаційної безпеки (підрозділ 1.2, 2.1). Застосування *кібернетичного підходу* дало змогу розглянути інформаційну безпеку як систему управління інформаційними процесами та загрозами, що функціонує на основі принципів зворотного зв'язку та адаптивності (підрозділи 1.1, 2.3). *Формально-юридичний метод* забезпечив аналіз нормативно-правової бази та дозволив виявити її прогалини, колізії та напрями модернізації (підрозділи 2.1, 2.3, 2.4). *Порівняльно-правовий метод* використано для аналізу зарубіжного досвіду забезпечення інформаційної безпеки та можливостей його адаптації в Україні (підрозділ 1.4). *Метод аналізу та синтезу* дозволив узагальнити наукові підходи та сформувати цілісне бачення інформаційної безпеки (підрозділи 1.2, 1.3). *Метод прогнозування та моделювання* використано для визначення перспектив розвитку системи інформаційної безпеки України (підрозділи 2.1-2.4).

Наукова новизна одержаних результатів полягає в тому, що дисертація є однією із перших у вітчизняній науці, в якій здійснено комплексне теоретико-правове обґрунтування змісту, структури та механізмів забезпечення інформаційної безпеки України в умовах воєнного стану та євроінтеграції, систематизовано існуючі проблеми, розроблено науково обґрунтовані рекомендації щодо їх подолання, а також сформульовано практичні рекомендації, спрямовані на підвищення рівня кіберзахищеності та забезпечення інформаційного суверенітету держави. У результаті проведеного дослідження сформульовано та обґрунтовано низку нових наукових положень, висновків і пропозицій, зокрема:

уперше:

- методологію дослідження інформаційної безпеки України репрезентовано як цілісну концептуальну основу, що, на відміну від існуючих підходів, визначає логіку наукового аналізу та формує сучасне бачення інформаційної безпеки як системоутворюючого елемента національної безпеки; обґрунтовано її багатовимірну природу через сукупність взаємопов'язаних методологічних підходів і методів, що

забезпечують цілісний аналіз інформаційної безпеки як динамічної соціально-правової системи та інтегрують проблематику кібербезпеки, інформаційного суверенітету і захисту прав людини у єдину наукову конструкцію;

- кібербезпеку розкрито як системоутворюючу складову інформаційної безпеки держави, що поєднує правові, організаційні та політичні інструменти захисту, а також сформульовано пріоритетні напрями розвитку національної системи кібербезпеки в умовах воєнного стану, зокрема: нормативне визначення правових режимів кібербезпеки; кодифікацію категорій кіберзагроз; правове врегулювання діяльності добровольчих кібервійськ; створення єдиного координаційного центру; запровадження уніфікованого протоколу реагування на кіберінциденти; інтеграцію міжнародних стандартів; розвиток технологічного суверенітету та кадрового потенціалу; впровадження спеціального режиму цифрових доказів та міжнародного співробітництва у сфері кібердоказування;

- визначено структуру інформаційного суверенітету як багатокомпонентного явища, що включає політико-правову, організаційно-інституційну, інформаційно-технічну та культурно-гуманітарну складові, а також обґрунтовано систему напрямів його забезпечення в умовах воєнного стану, зокрема: модернізацію інформаційного законодавства; посилення інституційної спроможності суб’єктів; розвиток державної інформаційної політики; оновлення інформаційно-комунікаційної інфраструктури; підвищення медіаграмотності та національної консолідації; розширення міжнародного співробітництва у сфері протидії інформаційним загрозам;

удосконалено:

- положення щодо стратегічних комунікацій, які концептуалізовано як окрему функцію сектору безпеки і оборони, а не лише складову інформаційної політики; обґрунтовано, що їх ефективність залежить від інституційного закріплення, чіткого розмежування повноважень суб’єктів публічної влади та налагодження міжвідомчої координації; додатково аргументовано необхідність післявоєнного перегляду правових режимів у сфері інформаційної безпеки з метою недопущення збереження надмірних обмежень і забезпечення балансу між безпековими обмеженнями та гарантіями інформаційних прав;

- науковий підхід до адаптації зарубіжного досвіду забезпечення інформаційної безпеки в умовах воєнного конфлікту, який удосконалено шляхом застосування принципу пропорційності як базового критерію відбору правових механізмів, що дозволяє розмежовувати заходи, спрямовані на легітимний захист національної безпеки, та практики, несумісні з європейськими стандартами захисту прав людини. Обґрунтовано доцільність формування системної нормативно-правової моделі, яка інтегрує норми інформаційного, безпекового та адміністративного права (на прикладі Німеччини, Франції, Естонії, Іспанії та інших країн) і забезпечує узгодженість правового регулювання в умовах кризових і воєнних загроз;

- наукове розуміння інституційної складової забезпечення інформаційної безпеки як організованої системи уповноважених суб'єктів, діяльність яких нормативно врегульована та спрямована на формування і реалізацію державної політики у сфері інформаційної безпеки, а також на забезпечення належного рівня захищеності життєво важливих інтересів особи, суспільства і держави в інформаційній сфері; підхід до структурування системи суб'єктів забезпечення інформаційної безпеки України з урахуванням їх функціональної взаємодії, розподілу ролей та умов відсутності єдиного координаційного органу;

дістало подальшого розвитку:

- положення про інформаційну безпеку як складову національної безпеки України, яке, на відміну від наявних підходів, уточнено через визначення її як перманентного процесу і результату забезпечення стану захищеності національних інтересів, а також розширено шляхом виокремлення структурних складових (об'єкти, загрози, система забезпечення) та систематизації внутрішніх і зовнішніх загроз в умовах воєнного стану;

- теоретико-правове осмислення проблематики інформаційної безпеки, яке полягає в обґрунтуванні відсутності цілісної концепції її функціонування як складової національної безпеки, а також в узагальненні еволюції наукових підходів (від фрагментарного до міждисциплінарного) і розширенні методологічних засад дослідження шляхом інтеграції концепцій кіберстійкості, управління ризиками, протидії дезінформації та інформаційної стійкості суспільства;

- підходи до правового забезпечення інформаційної безпеки, які удосконалено шляхом виокремлення трирівневої структури (національна безпека і оборона; інформаційні відносини; правовий статус суб'єктів), а також набули розвитку через обґрунтування необхідності систематизації, гармонізації інформаційного законодавства та розробки єдиного кодифікованого акта – Інформаційного кодексу України;

- положення щодо виявлення ключових проблем інституційного забезпечення (фрагментарності, недостатньої координації, нечіткості розподілу повноважень, обмеженої спроможності суб'єктів, слабкої інтеграції недержавного сектору та низького рівня медіаграмотності населення) та обґрунтування пріоритетних напрямів їх вирішення.

Практичне значення одержаних результатів полягає у можливості їх використання:

– *у науково-дослідній роботі* – для подальшого розвитку теоретико-правових досліджень у сфері інформаційної безпеки, аналізу нормативно-правових механізмів, інституційного забезпечення та вдосконалення державної політики у сфері кібербезпеки;

– *в освітньому процесі* – при викладанні навчальних дисциплін «Теорія держави та права», «Конституційне право», «Інформаційне право», «Міжнародне право», «Міжнародний захист прав людини», а також при підготовці навчально-методичних матеріалів з цих дисциплін;

– *у сфері правотворчості* – у діяльності суб'єктів правотворчої діяльності як теоретичне підґрунтя для формування ефективних державних правових політик у сфері інформаційної безпеки та удосконалення законодавства щодо забезпечення кібербезпеки та захисту інформаційного суверенітету;

– *у практичній сфері* – у діяльності органів державної влади, силових структур та органів місцевого самоврядування під час реалізації заходів щодо забезпечення інформаційної безпеки, кіберзахисту, захисту критичної інфраструктури та інформаційного суверенітету України (акт впровадження у діяльність Дніпропетровського окружного адміністративного суду від 16 квітня 2026 р.).

Апробація результатів дисертації. Основні теоретичні положення, їх новизна та практична значущість дослідження обговорювалися на засіданнях кафедри теорії держави та права Дніпровського державного університету внутрішніх справ та були оприлюднені на таких науково-практичних конференціях: *міжнародних:* «Modernization of science and its influence on global processes» (Bern, 2023), «Science and Practice: Implementation to Modern Society» (Manchester, 2023), «Міжнародна та національна безпека: теоретичні і прикладні аспекти» (Дніпро, 2025), «Міжнародна та національна безпека: теоретичні і прикладні аспекти» (Дніпро, 2026); *всеукраїнських:* «Актуальні проблеми державотворення та правозастосування» (Дніпро, 2023), «Права людини і громадянина під час дії воєнного стану» (Харків, 2023), «Юридична весна: права людини в умовах воєнного стану» (Харків, 2024), «Конституційні права і свободи людини та громадянина в умовах війни та післявоєнний період» (Львів, 2024), «Проблеми юридичної науки очима молодих науковців» (Рівне, 2024), «Військова експертиза в умовах сьогодення: проблемні питання та шляхи їх вирішення» (Дніпро, 2025).

Публікації. Основні положення, теоретичні висновки та практичні рекомендації, що містяться у дисертації, висвітлені автором у 13 публікаціях, з яких 3 – наукові статті, опубліковані у фахових виданнях України категорії «Б» з юридичних наук; 10 – у збірниках тез доповідей на науково-практичних конференціях.

Структура та обсяг дисертації. Дисертація складається із основної частини (вступу, двох розділів, що включають вісім підрозділів, висновків), списку використаних джерел та додатків. Загальний обсяг дисертації становить 262 сторінки, з яких 201 сторінка основного тексту. Список використаних джерел складається із 390 найменувань і займає 39 сторінок. Додатки розміщено на 7 сторінках.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНА ОСНОВА ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

1.1. Методологія дослідження інформаційної безпеки України

Розвиток сучасної юридичної науки нерозривно пов’язаний із формуванням і вдосконаленням її методологічних засад. Методологія виступає фундаментальною основою будь-якого наукового дослідження, оскільки визначає логіку пізнання державно-правових явищ, систему принципів, підходів і методів наукового аналізу, а також забезпечує формування обґрунтованих теоретичних висновків і практичних рекомендацій. У цьому контексті дослідження інформаційної безпеки України потребує особливої уваги до методологічного інструментарію, оскільки зазначене явище має складну багатовимірну природу та охоплює широкий спектр правових, політичних, соціальних і технологічних процесів.

Разом із тим слід зазначити, що у сучасній юридичній науці методологія дослідження державно-правових явищ розглядається не лише як сукупність методів наукового пізнання, але й як складна інтелектуальна конструкція, що визначає логіку побудови дослідження, структуру аргументації та характер наукових висновків. У цьому контексті методологія виступає не лише інструментом пізнання, але й важливим чинником формування нових наукових концепцій та підходів до осмислення правової реальності. Саме тому вибір і обґрунтування методологічної основи дослідження інформаційної безпеки України набуває принципового значення для забезпечення наукової об’єктивності та достовірності отриманих результатів.

Сучасні процеси глобалізації, цифровізації суспільства та стрімкого розвитку інформаційно-комунікаційних технологій істотно змінюють характер суспільних відносин, формуючи нові виклики та загрози для національної безпеки держав. У цих умовах інформаційна безпека стає одним із ключових елементів забезпечення державного суверенітету, стабільності політичної системи та захисту прав і свобод людини. Особливої актуальності ця проблема набуває для України в умовах воєнного

стану, коли інформаційний простір перетворюється на один із головних інструментів ведення гібридної війни.

У сучасній юридичній науці питання методології дослідження державно-правових явищ розглядаються як один із ключових напрямів наукового пізнання. Значний внесок у розвиток методологічних засад правознавства зробили українські вчені О. Бандура, В. Битяк, С. Бобровник, О. Данильян, В. Денисов, О. Зайчук, М. Кельман, М. Козюбра, М. Костицький, М. Кресін, В. Лемак, Л. Луць, А. Мельник, Л. Наливайко, Н. Оніщенко, Ю. Оборотов, О. Петришин, П. Рабінович, О. Скрипнюк, В. Таційй, Ю. Тодика, Ю. Шемшученко та ін. Поряд із цим, вагомий вплив на формування сучасних методологічних підходів у правознавстві здійснили зарубіжні дослідники, зокрема R. Alexy, H. L. A. Hart, R. Dworkin, H. Kelsen, N. Luhmann, J. Raz, R. Posner та ін.

У контексті дослідження інформаційної безпеки особливого значення набувають наукові підходи, що поєднують правовий, міждисциплінарний та порівняльний аналіз. Відповідні методологічні орієнтири простежуються у працях як вітчизняних учених – О. Баранова, В. Бурячка, В. Горбуліна, С. Гнатюка, О. Дзьобаня, О. Довганя, О. Литвиненка, В. Пилипчука, Т. Ткачука, О. Тихомирова, С. Телешуна, О. Юдіна, М. Швеця та ін., так і зарубіжних дослідників, зокрема A. Serrano, H. Melaku, M. T. Rusydi, A. Jaber, R. Tang, W. Zhang, M. N. Schmitt, R. Anderson, а також M. Castells, у працях яких обґрунтовуються концептуальні, порівняльно-правові та системні підходи до аналізу кібербезпеки та інформаційного суспільства.

Аналіз наукових праць зазначених учених свідчить про поступове формування в українській правовій науці комплексного підходу до дослідження інформаційної безпеки, що передбачає поєднання правового, політичного, безпекового та технологічного вимірів цього явища. Водночас наявні наукові розробки засвідчують необхідність подальшого поглиблення методологічних засад дослідження інформаційної безпеки, зокрема з урахуванням сучасних трансформацій інформаційного середовища та умов воєнного стану, що суттєво змінюють характер інформаційних загроз та механізмів їх нейтралізації.

Як зазначає О. Петришин, методологія юридичної науки являє собою складну систему взаємопов’язаних принципів, підходів і методів, що забезпечують наукове пізнання державно-правових явищ і формування обґрунтованих теоретичних висновків [1, с. 25–35]. У свою чергу, П. Рабінович визначає методологію як систему загальних принципів і способів організації наукового пізнання, що спрямована на отримання достовірних знань про право та державу [2, с. 18–21]. Л. Наливайко підкреслює, що сучасні правові дослідження повинні базуватися на поєднанні різних наукових підходів, що дозволяє адекватно відобразити складність сучасних соціально-правових процесів [3, с. 37–39].

На підставі наведених наукових підходів можна дійти висновку, що сучасна методологія юридичних досліджень характеризується поступовим переходом від використання ізольованих методів до формування комплексних методологічних моделей пізнання державно-правових явищ. У цьому контексті дослідження інформаційної безпеки України потребує застосування інтегративної методології, що поєднує загальнонаукові, спеціально-юридичні та міждисциплінарні підходи. Саме така інтегративна методологічна конструкція дозволяє адекватно відобразити багатовимірну природу інформаційної безпеки, що формується на перетині правових норм, політичних процесів, технологічних інновацій та соціальних трансформацій сучасного інформаційного суспільства. У зв’язку з цим методологія дослідження інформаційної безпеки повинна розглядатися не лише як сукупність методів наукового пізнання, але й як цілісна концептуальна система організації дослідницького процесу, що визначає логіку наукового аналізу, структуру аргументації та спрямованість теоретичних узагальнень.

Також слід зазначити, що у контексті тенденцій розвитку сучасної загальної теорії держави та права [4, с. 3–9], методологію дослідження інформаційної безпеки України доцільно розглядати як комплекс взаємопов’язаних принципів, методологічних підходів і методів наукового пізнання, використання котрих забезпечує всебічне дослідження правової природи інформаційної безпеки, її структурних елементів, механізмів функціонування та ролі у системі національної безпеки держави.

Такий підхід дозволяє сформувати цілісну концепцію наукового дослідження інформаційної безпеки, у межах котрої поєднуються теоретичні положення юридичної науки [5, с. 279–280], досягнення суміжних галузей знань та практичний досвід функціонування системи національної безпеки держави. Водночас комплексний характер методології забезпечує можливість аналізу інформаційної безпеки як багаторівневого явища, що функціонує одночасно у правовому, політичному, технологічному та соціальному вимірах [6, с. 49–56].

Актуальність формування комплексної методології дослідження інформаційної безпеки зумовлена тим, що інформаційний простір у сучасних умовах перетворюється на один із ключових факторів міжнародної безпеки [7, с. 15–17]. Як зазначає В. Горбулін, інформаційні технології та комунікаційні системи дедалі частіше використовуються як інструменти геополітичного впливу, що робить інформаційний простір одним із головних напрямів сучасних конфліктів [8, с. 141–146]. У цьому контексті інформаційна безпека виступає важливим елементом забезпечення державного суверенітету та національної безпеки [9, с. 48–50].

Так, інформаційна безпека у сучасних умовах набуває системоутворюючого значення для функціонування держави та суспільства, що зумовлює необхідність переосмислення традиційних методологічних підходів до дослідження безпекової проблематики у юридичній науці. Інформаційна безпека вже не може розглядатися виключно як вузькоспеціалізована галузь правового регулювання, оскільки охоплює широкий спектр суспільних відносин, пов’язаних із функціонуванням інформаційного простору, розвитком цифрових технологій та забезпеченням інформаційного суверенітету держави. У зв’язку з цим методологія її дослідження повинна враховувати складну природу сучасних інформаційних процесів і базуватися на поєднанні правового аналізу з досягненнями політичної науки, інформаційних технологій та безпекових досліджень.

Одним із фундаментальних методів наукового пізнання є діалектичний метод. Його застосування дозволяє розглядати інформаційну безпеку як динамічне явище, що перебуває у постійному розвитку та зміні під впливом соціальних, політичних і технологічних факторів [10, с. 112–115]. Як зазначають О. Данильян та О. Дзьобань,

діалектичний метод у юридичній науці дозволяє досліджувати державно-правові явища у взаємозв'язку, взаємозалежності та розвитку [10, с. 118].

Застосування діалектичного методу у межах цього дослідження дозволяє виявити закономірності формування системи інформаційної безпеки України, визначити суперечності її розвитку та встановити основні тенденції вдосконалення правового регулювання у відповідній сфері [11, с. 51–56].

Крім того, діалектичний метод дозволяє дослідити взаємозв'язок між розвитком інформаційного суспільства та трансформацією правових механізмів забезпечення інформаційної безпеки [12, с. 33–35]. У сучасних умовах саме діалектичний підхід дає можливість виявити суперечності між необхідністю захисту державних інтересів у інформаційній сфері та забезпеченням конституційних прав і свобод людини, зокрема свободи слова, доступу до інформації та захисту персональних даних [13, с. 91–93].

Так, застосування діалектичного методу у дослідженні інформаційної безпеки має принципове значення, оскільки дозволяє розглядати відповідні правові явища не як статичні правові конструкції, а як динамічні процеси, що постійно трансформуються під впливом розвитку інформаційних технологій та змін у міжнародному безпековому середовищі. Саме діалектичний підхід дає можливість виявити внутрішні суперечності розвитку правового регулювання інформаційної сфери, зокрема між потребою забезпечення національної безпеки та необхідністю гарантування демократичних прав і свобод людини. У цьому контексті діалектичний метод виступає важливим інструментом наукового аналізу, що дозволяє визначити закономірності розвитку правових механізмів забезпечення інформаційної безпеки та окреслити перспективні напрями їх удосконалення.

Важливе значення має також системний підхід, що передбачає розгляд інформаційної безпеки як складної соціально-правової системи [14, с. 29]. Системний підхід широко використовується у сучасній юридичній науці, оскільки дозволяє досліджувати складні державно-правові явища у їх взаємозв'язку та взаємозалежності.

Як зазначає М. Козюбра, системний підхід дозволяє розглядати право як цілісну систему взаємопов'язаних елементів, що функціонують у межах певної соціальної структури [15, с. 13]. У контексті дослідження інформаційної безпеки застосування системного підходу дає можливість розглядати її як складову системи національної безпеки України. При цьому інформаційна безпека постає як багатокомпонентне явище, що включає нормативно-правові механізми регулювання інформаційних відносин, інституційну систему державних органів, інформаційну політику держави, технологічні засоби кібернетичного захисту та інші елементи функціонування інформаційного простору.

Застосування системного підходу дозволяє встановити не лише структурні елементи інформаційної безпеки, але й характер взаємодії між ними. Зокрема, правові механізми забезпечення інформаційної безпеки функціонують у тісному взаємозв'язку з діяльністю державних інституцій, розвитком інформаційної інфраструктури, міжнародним співробітництвом у сфері безпеки та реалізацією державної інформаційної політики. Такий комплексний аналіз сприяє більш глибокому розумінню механізму функціонування системи інформаційної безпеки держави.

Узагальнюючи значення системного підходу для дослідження інформаційної безпеки, слід зазначити, що його застосування створює методологічні передумови для комплексного аналізу правових, інституційних та технологічних аспектів забезпечення інформаційної безпеки. Відповідно, саме системний підхід дозволяє розглядати інформаційну безпеку як багаторівневу систему, у межах котрої взаємодіють правові норми, державні інституції, інформаційна інфраструктура та соціальні механізми протидії інформаційним загрозам, що має важливе значення для формування ефективної державної політики у відповідній сфері.

Значну роль у дослідженні відіграє структурно-функціональний метод. Його застосування дозволяє дослідити внутрішню структуру системи забезпечення інформаційної безпеки та визначити функції її окремих елементів [3, с. 41–42]. Як зазначає Л. Наливайко, структурно-функціональний аналіз дозволяє встановити роль

державних інституцій у забезпеченні стабільності конституційного ладу та реалізації державної політики у відповідній сфері [3, с. 43].

Використання структурно-функціонального методу дозволяє більш глибоко дослідити інституційний механізм забезпечення інформаційної безпеки держави. Завдяки цьому підходу стає можливим визначити функціональне призначення окремих державних органів у системі забезпечення інформаційної безпеки, а також проаналізувати ефективність їх взаємодії у процесі реалізації державної інформаційної політики. Такий аналіз має важливе значення для вдосконалення організаційної структури системи забезпечення інформаційної безпеки України та підвищення ефективності діяльності відповідних державних інституцій.

Важливе значення має також порівняльно-правовий метод. Порівняльно-правовий метод дозволяє зіставити правове регулювання інформаційної безпеки у різних державах та визначити можливості імплементації позитивних практик в Україні [16, с. 25–27]. Так, порівняльно-правові дослідження сприяють розвитку національної правової системи та дозволяють враховувати міжнародний досвід правового регулювання [16, с. 29].

У контексті дослідження інформаційної безпеки, порівняльно-правовий аналіз дозволяє виявити закономірності розвитку правового регулювання інформаційної сфери у різних державах та визначити перспективні напрями вдосконалення національного законодавства. Також важливо, що використання порівняльно-правового методу сприяє не лише запозиченню позитивного міжнародного досвіду, але й формуванню більш ефективної моделі правового забезпечення інформаційної безпеки, адаптованої до сучасних викликів глобального інформаційного середовища.

Не менш важливим є формально-юридичний (догматичний) метод, що традиційно застосовується у дослідженнях теорії права для аналізу змісту та структури нормативно-правових актів [17, с. 888-930] України у сфері інформаційної безпеки. Саме цей метод використовується для дослідження змісту та структури нормативно-правових актів, що регулюють відповідну сферу.

У межах дослідження формально-юридичний метод застосовується для аналізу Конституції України, Закону України «Про національну безпеку України», Закону

України «Про інформацію», Закону України «Про основні засади забезпечення кібербезпеки України», Доктрини інформаційної безпеки України та інших нормативно-правових актів.

Важливе місце у дослідженні займає історико-правовий метод, що дозволяє простежити еволюцію формування правових засад інформаційної безпеки України [18, с. 73–75] і визначити основні етапи розвитку відповідного законодавства.

Значення історико-правового методу для дослідження інформаційної безпеки полягає у тому, що його застосування дозволяє виявити закономірності формування та розвитку правового регулювання інформаційних відносин в Україні. Важливо, що використання історико-правового підходу створює можливість не лише простежити еволюцію нормативно-правових засад забезпечення інформаційної безпеки, але й визначити ключові фактори, що впливали на трансформацію державної політики у цій сфері. Такий метод сприяє більш глибокому розумінню сучасного стану правового регулювання інформаційної безпеки та дозволяє обґрунтувати напрями подальшого вдосконалення відповідного законодавства з урахуванням історичного досвіду розвитку інформаційної сфери.

Поряд із традиційними методами юридичного пізнання у дослідженні застосовуються сучасні методологічні підходи, використання котрих дозволяє більш глибоко розкрити складну природу інформаційної безпеки в умовах цифрової трансформації суспільства.

Зокрема, важливе значення має синергетичний підхід. Синергетика розглядає складні системи як відкриті структури, що здатні до самоорганізації [19, с. 17–19]. У контексті дослідження інформаційної безпеки синергетичний підхід дозволяє розглядати інформаційний простір як складну динамічну систему, у котрій взаємодіють державні інституції, суспільство, медіа та інформаційні технології.

Як зазначає О. Дзьобань, синергетичний підхід дозволяє дослідити процеси самоорганізації інформаційного простору та визначити фактори, що впливають на його стабільність [20, с. 88–90].

Особливого значення синергетичний підхід набуває в умовах інформаційної війни, коли інформаційний простір держави зазнає інтенсивного впливу зовнішніх

дестабілізаційних факторів. У таких умовах система інформаційної безпеки повинна демонструвати здатність до швидкої адаптації та самоорганізації, що передбачає гнучкість правових механізмів, ефективну координацію діяльності державних інституцій та активну участь громадянського суспільства у протидії інформаційним загрозам.

Отже, синергетичний підхід відкриває нові можливості для дослідження процесів функціонування інформаційного простору як складної відкритої системи. Його застосування дозволяє розглядати інформаційну безпеку не лише як результат діяльності державних інституцій, але й як результат взаємодії різних соціальних, політичних та технологічних факторів. Саме синергетичний підхід дає можливість дослідити процеси самоорганізації інформаційного середовища та визначити механізми підвищення стійкості інформаційної системи держави до зовнішніх дестабілізаційних впливів.

Важливе методологічне значення має герменевтичний підхід, що використовується для інтерпретації правових норм і текстів [21, с. 302–305]. Герменевтика у юридичній науці застосовується для глибокого аналізу змісту правових актів, а також для встановлення їх справжнього значення у контексті правозастосовної практики.

Щодо значення герменевтичного підходу для дослідження інформаційної безпеки, то слід зазначити, що його застосування дозволяє забезпечити більш глибоке розуміння змісту правових норм, котрі регулюють інформаційні відносини у сучасному цифровому середовищі. Герменевтичний підхід має особливе значення саме у сфері інформаційної безпеки, оскільки відповідне законодавство характеризується складністю, динамічністю та значною кількістю оціночних правових категорій. У таких умовах правильне тлумачення правових норм набуває принципового значення для їх ефективного застосування на практиці. Використання герменевтичного підходу дозволяє враховувати не лише буквальний зміст правових норм, але й їх цілі, принципи та контекст функціонування у системі національної безпеки держави. У цьому контексті герменевтичний аналіз сприяє більш повному розкриттю змісту законодавства у сфері інформаційної безпеки та дозволяє визначити

напрями його подальшого вдосконалення з урахуванням сучасних викликів розвитку інформаційного суспільства.

Не менш важливим є антропологічний підхід, що передбачає дослідження правових явищ крізь призму прав і свобод людини [22, с. 114–116]. У цьому контексті інформаційна безпека розглядається не лише як елемент державної безпеки, але й як механізм захисту інформаційних прав громадян.

Як зазначає В. Лемак, сучасна правова держава повинна забезпечувати баланс між захистом державних інтересів і гарантуванням прав людини у сфері інформаційних відносин [22, с. 119].

Антропологічний підхід також дозволяє акцентувати увагу на необхідності формування людиноцентричної інформаційної політики держави, в основі котрої лежить забезпечення інформаційної безпеки особи, суспільства та держави. У цьому контексті інформаційна безпека виступає не лише елементом державної безпеки, але й важливою гарантією реалізації інформаційних прав людини, що передбачає створення належних умов для вільного доступу до достовірної інформації та захисту особи від деструктивного інформаційного впливу.

Так, антропологічний метод дозволяє розглядати відповідну сферу правового регулювання через призму людиноцентричної парадигми розвитку сучасної правової держави. Такий підхід сприяє формуванню наукового розуміння інформаційної безпеки не лише як інструменту забезпечення державного суверенітету, але й як важливого механізму гарантування основоположних прав і свобод людини у цифровому середовищі. У цьому контексті антропологічний метод дозволяє визначити баланс між публічними інтересами держави у сфері забезпечення інформаційної безпеки та необхідністю захисту інформаційних прав особи, зокрема права на доступ до інформації, свободу вираження поглядів та захист персональних даних. Саме така людиноцентрична методологічна орієнтація сприяє формуванню сучасної моделі правового забезпечення інформаційної безпеки, у межах котрої пріоритетним завданням держави є створення безпечного та водночас відкритого інформаційного середовища для розвитку демократичного суспільства.

Окрему роль відіграє кібернетичний підхід, що дозволяє дослідити інформаційну безпеку з урахуванням розвитку інформаційно-комунікаційних технологій. Як зазначає О. Баранов, сучасна система інформаційної безпеки повинна враховувати кібернетичні аспекти функціонування інформаційних систем та мереж [23, с. 57–59].

Застосування кібернетичного підходу дозволяє дослідити взаємозв'язок між правовими механізмами забезпечення інформаційної безпеки та технологічними аспектами функціонування інформаційних систем [24, с. 39-40].

Використання кібернетичного підходу дозволяє також дослідити механізми управління інформаційними потоками та процесами обміну інформацією у сучасному цифровому середовищі. У цьому контексті інформаційна безпека розглядається як результат ефективного функціонування системи управління інформаційними ресурсами держави, що включає правові, організаційні та технологічні інструменти захисту інформаційної інфраструктури.

Так, застосування кібернетичного методу дозволяє інтегрувати юридичний аналіз із дослідженням технологічних аспектів функціонування інформаційних систем. Саме такий міждисциплінарний підхід є необхідною умовою формування сучасної наукової концепції інформаційної безпеки. Кібернетичний підхід дозволяє дослідити механізми управління інформаційними потоками, процеси обробки та передачі інформації, а також визначити роль правових механізмів у забезпеченні стабільності функціонування цифрової інфраструктури держави.

Окремо слід зазначити про важливі методологічні орієнтири для сучасних досліджень інформаційної безпеки формуються також у працях зарубіжних учених, які розглядають безпекову проблематику у контексті розвитку цифрового суспільства, трансформації міжнародного права та формування глобального кіберпростору. У сучасній науковій літературі дедалі більше уваги приділяється комплексному аналізу інформаційної та кібернетичної безпеки як міждисциплінарного феномену, що перебуває на перетині правових, політичних, технологічних і соціальних процесів. У цьому контексті значний інтерес становлять дослідження, присвячені формуванню нових підходів до правового регулювання

кіберпростору, а також розвитку концепції глобального кібербезпекового врядування.

Так, у сучасних дослідженнях міжнародного права кіберпростору наголошується, що стрімкий розвиток інформаційно-комунікаційних технологій призвів до суттєвої трансформації традиційних уявлень про безпеку держави. Як зазначає іспанський дослідник A. Segura-Serrano, формування глобального цифрового середовища спричинило появу нових правових викликів, пов’язаних із необхідністю регулювання державної поведінки у кіберпросторі, забезпечення міжнародної кібербезпеки та захисту прав людини в умовах цифровізації суспільства. Науковець підкреслює, що сучасні процеси кіберконфронтації між державами вимагають формування нових норм міжнародного права, котрі б визначали допустимі межі використання кібероперацій, регулювали питання відповідальності держав за кібернапади та забезпечували міжнародне співробітництво у сфері кібербезпеки [25, с. 12–18].

У свою чергу, сучасні дослідження у сфері кібербезпекового врядування підкреслюють важливість системного підходу до аналізу механізмів забезпечення безпеки цифрового середовища. Зокрема, H. Melaku зазначає, що ефективна система кібербезпеки повинна ґрунтуватися на інтеграції правових, організаційних і технологічних інструментів управління ризиками. На думку дослідника, сучасна модель кібербезпекового врядування передбачає формування адаптивної системи управління безпекою, що здатна оперативно реагувати на появу нових кіберзагроз та забезпечувати стійкість інформаційної інфраструктури держави. Такий підхід передбачає поєднання стратегічного планування, нормативного регулювання, моніторингу кіберризиків та ефективної взаємодії державних інституцій із приватним сектором [26, с. 329–335].

Питання правового забезпечення інформаційної безпеки у глобальному вимірі також активно досліджуються у сучасних працях, присвячених аналізу ефективності національних і міжнародних моделей регулювання кіберпростору. Так, M. Rusydi наголошує, що сучасна система правового регулювання кібербезпеки повинна враховувати транснаціональний характер інформаційних загроз, що обумовлює

необхідність розвитку міжнародного співробітництва у сфері протидії кіберзлочинності та захисту інформаційної інфраструктури. Науковець акцентує, що ефективність правових механізмів забезпечення кібербезпеки значною мірою залежить від рівня координації між державними органами, приватним сектором та міжнародними організаціями, а також від здатності правових систем адаптуватися до швидких технологічних змін у цифровому середовищі [27, с. 45–51; 302].

Важливе значення для розвитку методології дослідження інформаційної безпеки мають також праці, присвячені аналізу взаємозв'язку між політичними структурами держави та ефективністю її кібербезпекової політики. Зокрема, A. Jaber у своєму дослідженні кібербезпекового врядування підкреслює, що ефективність системи кіберзахисту значною мірою залежить від організаційної структури державного управління та рівня інституційної координації між органами влади. Дослідниця зазначає, що централізовані моделі управління кібербезпекою можуть забезпечувати більш швидке прийняття рішень у кризових ситуаціях, тоді як децентралізовані системи сприяють підвищенню гнучкості та інноваційності у сфері реагування на кіберзагрози. У цьому контексті особливого значення набуває розроблення ефективних механізмів координації між державними інституціями, що відповідають за формування та реалізацію політики у сфері інформаційної безпеки [28, с. 755–760].

Не менш важливими є сучасні дослідження, присвячені аналізу геополітичних аспектів кібербезпеки. Так, A. Adeyeri та H. Abroshan зазначають, що кіберпростір поступово перетворюється на один із ключових театрів геополітичного протистояння між державами. На думку дослідників, сучасні кіберконфлікти характеризуються високим рівнем складності, оскільки поєднують елементи інформаційної війни, кіберрозвідки, економічного шпигунства та деструктивних кібероперацій. У таких умовах забезпечення інформаційної безпеки держави потребує використання комплексних підходів, що поєднують правові механізми регулювання, розвиток міжнародного співробітництва та формування ефективних систем кіберзахисту на національному рівні [29, с. 4–9].

Крім того, сучасні дослідження у сфері цифровізації суспільства підкреслюють, що забезпечення інформаційної безпеки держави повинно базуватися на принципах стійкості та адаптивності інформаційних систем. Зокрема, дослідники R.Tang та W. Zhang наголошують, що сучасна система кібербезпеки повинна передбачати не лише захист інформаційних ресурсів, але й здатність інформаційної інфраструктури швидко відновлюватися після кіберінцидентів. У цьому контексті особливого значення набуває формування комплексної державної політики кіберстійкості, що передбачає розвиток інституційних механізмів управління ризиками, удосконалення нормативно-правової бази та впровадження сучасних технологічних рішень у сфері кіберзахисту [30, с. 6–12].

Слід також зазначити, що важливе значення для розвитку сучасної методології дослідження інформаційної безпеки мають наукові праці, присвячені формуванню концепції кіберстійкості (cyber resilience) як одного з ключових методологічних підходів до аналізу безпеки цифрового середовища. У сучасній науковій літературі наголошується, що традиційні моделі забезпечення безпеки, що базуються виключно на запобіганні загрозам, уже не відповідають сучасним умовам функціонування інформаційного простору. Зокрема, як зазначає британський дослідник T. Rid, сучасні кіберконфлікти характеризуються високим рівнем динамічності та непередбачуваності, що вимагає формування систем інформаційної безпеки, здатних не лише запобігати загрозам, але й ефективно адаптуватися до них та відновлювати функціонування інформаційної інфраструктури після кіберінцидентів. На думку науковця, саме концепція кіберстійкості дозволяє сформувати нову методологічну модель дослідження інформаційної безпеки, що поєднує правові, організаційні та технологічні аспекти забезпечення безпеки цифрового середовища [31, с. 214–218].

У цьому контексті значний науковий інтерес становлять дослідження, присвячені розвитку концепції багаторівневого управління кібербезпекою. Так, забезпечення інформаційної безпеки у цифровому середовищі потребує координації діяльності широкого кола суб’єктів, включаючи державні органи, міжнародні організації, приватний сектор та ІГС. Зокрема, у доповіді експертів World Economic Forum підкреслюється, що сучасна система кібербезпеки формується як

багаторівнева модель управління, у межах котрої взаємодіють національні політики кібербезпеки, міжнародні стандарти регулювання цифрового простору та механізми публічно-приватного партнерства у сфері захисту інформаційної інфраструктури. У таких умовах ефективна політика кібербезпеки повинна ґрунтуватися на комплексній методології, що поєднує правові, організаційні та технологічні інструменти протидії інформаційним загрозам. Використання такого підходу дозволяє розглядати інформаційну безпеку як складну систему багаторівневого управління, ефективність котрої залежить від узгодженості дій різних суб'єктів цифрового середовища [32].

Важливим напрямом розвитку методології дослідження інформаційної безпеки є використання ризик-орієнтованого підходу до аналізу інформаційних загроз. У сучасних дослідженнях підкреслюється, що ефективне управління інформаційною безпекою неможливе без системного аналізу ризиків, пов'язаних із функціонуванням інформаційних систем і мереж. Зокрема, британський дослідник R. Anderson зазначає, що управління інформаційною безпекою повинно базуватися на оцінюванні ризиків та визначенні найбільш уразливих елементів інформаційної інфраструктури. Такий підхід дозволяє оцінити потенційні загрози, визначити їх імовірність і наслідки та сформувати ефективні механізми захисту інформаційних систем [33, с. 35–40].

Суттєвий внесок у розвиток сучасних методологічних підходів до дослідження інформаційної безпеки зробили також наукові праці, присвячені аналізу впливу цифрової трансформації державного управління на формування нових безпекових викликів. Наголошується, що розвиток цифрового врядування, електронних публічних послуг та цифрових платформ суттєво змінює характер інформаційних відносин між державою, суспільством і приватним сектором. Зокрема, у доповіді European Union Agency for Cybersecurity (ENISA) зазначається, що цифровізація державного управління супроводжується появою нових типів інформаційних загроз, пов'язаних із функціонуванням цифрової інфраструктури, обробкою великих масивів даних та використанням мережевих інформаційних систем. У таких умовах методологія дослідження інформаційної безпеки повинна враховувати не лише правові аспекти захисту інформації, але й інституційні механізми управління цифровими процесами, а також соціальні та технологічні наслідки цифрової

трансформації суспільства. Використання міждисциплінарного підходу дозволяє сформувати комплексне уявлення про механізми забезпечення інформаційної безпеки у сучасному цифровому середовищі та визначити ефективні інструменти державної політики у відповідній сфері [34].

Особливу увагу у сучасній науковій літературі приділено також розвитку методології дослідження міжнародно-правових аспектів інформаційної безпеки. Так, відомий дослідник міжнародного кіберправа M. Schmitt зазначає, що сучасний кіберпростір формує нову сферу правового регулювання, у межах котрої традиційні норми міжнародного права повинні адаптуватися до специфіки цифрового середовища. Науковець підкреслює, що дослідження правових аспектів кібербезпеки потребує використання комплексної методології, що поєднує доктринальний аналіз міжнародного права, порівняльно-правові дослідження та міждисциплінарні методи аналізу кіберконфліктів. Такий підхід дозволяє більш глибоко дослідити правову природу сучасних кібероперацій та визначити межі відповідальності держав за дії у кіберпросторі [35, с. 9–15].

У контексті розвитку методології дослідження інформаційної безпеки важливе значення мають також наукові праці, присвячені аналізу ролі приватного сектору у забезпеченні кібербезпеки. Як зазначає американський дослідник B. Buchanan, значна частина сучасної цифрової інфраструктури перебуває у власності приватних компаній, що обумовлює необхідність формування нових моделей публічно-приватного партнерства у сфері забезпечення інформаційної безпеки. На думку науковця, дослідження цієї проблематики потребує використання комплексних методологічних підходів, що дозволяють аналізувати взаємодію державних інституцій, технологічних корпорацій та громадянського суспільства у процесі формування політики кібербезпеки [36, с. 92–97].

Крім того, у сучасних дослідженнях акцентується увага на важливості використання мережевого підходу під час аналізу інформаційної безпеки. Зокрема, відомий соціолог M. Castells зазначає, що сучасне інформаційне суспільство функціонує у формі складних мережевих структур, у межах котрих взаємодіють державні інституції, економічні суб’єкти, медіа та громадянське суспільство. У таких

умовах інформаційна безпека повинна розглядатися як результат функціонування мережевих взаємозв'язків між різними суб'єктами інформаційного простору. Використання мережевого підходу дозволяє дослідити структуру сучасного інформаційного середовища та визначити ключові вузли впливу, що мають стратегічне значення для забезпечення інформаційної безпеки держави [7, с. 500–507].

Отже, аналіз сучасних наукових праць зарубіжних учених свідчить про активний розвиток нових методологічних підходів до дослідження інформаційної безпеки, що базуються на інтеграції правових, політичних, технологічних та управлінських аспектів аналізу цифрового середовища. У сучасних умовах саме міждисциплінарна методологія дозволяє найбільш повно дослідити складну природу інформаційної безпеки та визначити ефективні механізми її забезпечення у контексті розвитку цифрового суспільства та трансформації міжнародних безпекових відносин.

Підсумовуючи дослідження методології пізнання інформаційної безпеки в умовах воєнного стану, доцільно сформулювати такі висновки та узагальнення:

1. В умовах трансформації безпекового середовища, цифровізації та гібридних загроз методологія дослідження інформаційної безпеки України набуває самостійного теоретико-правового значення. Вона постає не лише як сукупність методів наукового пізнання, але як цілісна концептуальна основа дослідження, що визначає логіку наукового аналізу, формує сучасне бачення інформаційної безпеки як системоутворюючого елемента національної безпеки та орієнтує дослідження на врахування взаємодії правових, безпекових, технологічних і соціальних чинників.

2. Багатовимірна природа інформаційної безпеки розкривається через комплекс взаємопов'язаних методологічних підходів і методів наукового пізнання, що забезпечують її цілісний аналіз як динамічної соціально-правової системи. Застосування загальнонаукових і спеціально-юридичних методів у поєднанні із системним, синергетичним, герменевтичним, антропологічним і кібернетичним підходами дозволяє виявити структурні елементи інформаційної безпеки, закономірності їх функціонування, а також забезпечити інтеграцію проблематики

кібербезпеки, інформаційного суверенітету та захисту прав людини у єдину наукову конструкцію.

3. Сучасні вітчизняні та зарубіжні наукові підходи до дослідження інформаційної безпеки відображають тенденцію до формування інтегрованих методологічних моделей, що ґрунтуються на міждисциплінарності, ризик-орієнтованому підході, концепції кіберстійкості, мережевому аналізі та багаторівневому безпековому врядуванні. Їх використання розширює методологічні можливості юридичної науки та сприяє адаптації національних досліджень до умов глобалізованого інформаційного простору і сучасних воєнних викликів.

4. Сформована методологічна конструкція дослідження інформаційної безпеки України створює теоретико-методологічне підґрунтя для подальшого розвитку правових засад її забезпечення, а також для вдосконалення нормативного та інституційного механізму функціонування системи інформаційної безпеки в умовах воєнного стану.

1.2. Наукові дослідження інформаційної безпеки України

Проблематика інформаційної безпеки тривалий час розглядалася у вітчизняній правовій науці переважно як складова системи національної безпеки або як елемент державної інформаційної політики. У перші роки незалежності України дослідження в цій сфері мали поодинокий і фрагментарний характер та зосереджувалися переважно на питаннях інформаційного суверенітету, свободи слова, розвитку інформаційного суспільства і правового регулювання інформаційних відносин. Водночас, поступова цифровізація суспільства, глобалізація інформаційних процесів і поява нових форм інформаційних загроз зумовили суттєве зростання наукового інтересу до проблем забезпечення інформаційної безпеки держави.

Якісно новий етап розвитку досліджень інформаційної безпеки пов’язаний із початком російської збройної агресії проти України у 2014 р. та подальшим повномасштабним вторгненням у 2022 р. Зазначені події продемонстрували, що інформаційний простір перетворився на один із ключових просторів сучасного

протиборства, у межах котрого активно застосовуються інформаційні операції, пропаганда, кібератаки та маніпулятивні інформаційні кампанії. У зв'язку з цим, суттєво активізувалося наукове осмислення проблем інформаційної безпеки, що відобразилося у значній кількості сучасних наукових праць.

Разом із тим, у науковій літературі досі відсутнє єдине усталене розуміння сутності інформаційної безпеки, що зумовлює множинність підходів до її визначення. Зокрема, інформаційна безпека розглядається як стан захищеності інформаційного простору, як система правових, організаційних і технічних заходів, а також як процес управління інформаційними ризиками. Така варіативність свідчить про складну та багатовимірну природу цього явища й актуалізує необхідність систематизації наукових підходів та уточнення його теоретичних засад.

Еволюція наукових досліджень інформаційної безпеки в Україні відображає поступовий перехід від переважно нормативно-правового підходу до комплексного розуміння цього явища, що поєднує правові, безпекові, технологічні та соціально-комунікаційні аспекти. Такий підхід дозволяє розглядати інформаційну безпеку як інтегрований соціально-правовий феномен, що функціонує в умовах динамічної трансформації інформаційного середовища.

З огляду на зазначене, сучасні дослідження інформаційної безпеки формуються під впливом як внутрішніх процесів розвитку інформаційного суспільства, так і зовнішніх безпекових викликів, що зумовлює їх прикладну спрямованість та орієнтацію на розроблення ефективних механізмів протидії інформаційним загрозам. У зв'язку з цим, необхідним є аналіз стану наукової розробленості проблематики інформаційної безпеки, що дозволяє систематизувати існуючі підходи, визначити основні напрями досліджень та окреслити перспективи їх подальшого розвитку.

Так, формування сучасної доктрини інформаційної безпеки в Україні значною мірою пов'язане з розвитком загальної теорії інформаційного права. Одним із провідних дослідників у цій сфері є В. Цимбалюк, який у своїх працях системно досліджує правову природу інформаційних відносин, їх структуру, принципи правового регулювання та місце інформаційної безпеки у системі інформаційного права. У монографії «Інформаційне право України» (2011) автор обґрунтовує

необхідність формування відповідного правового механізму забезпечення інформаційної безпеки як складової національної безпеки держави [37].

Також вагомий внесок у дослідження теоретико-правових засад інформаційної безпеки здійснив О. Баранов. У низці наукових праць, зокрема у монографії «Інформаційне право України: стан, проблеми та перспективи розвитку» (2015), автор досліджує інформаційну безпеку як системне правове явище, аналізує її структуру, функції та механізми забезпечення в умовах розвитку інформаційного суспільства. О. Баранов підкреслює, що інформаційна безпека має розглядатися не лише як захист інформаційних ресурсів держави, але й як сукупність заходів щодо захисту інформаційного простору, прав і свобод людини у сфері інформації та забезпечення інформаційного суверенітету держави [38].

Характерною особливістю цих досліджень є прагнення до системного осмислення інформаційної безпеки через призму інформаційного права, що дозволяє інтегрувати питання захисту інформації, прав людини та інформаційного суверенітету держави в єдину концептуальну модель. Водночас, зазначені підходи свідчать про поступовий перехід від вузького розуміння інформаційної безпеки як захисту інформації до її трактування як категорії, що охоплює правові, політичні та соціальні аспекти функціонування інформаційного простору.

Важливим напрямом наукових досліджень є аналіз інформаційної безпеки у контексті забезпечення національної безпеки держави. Значний внесок у розвиток цього напряму зробив Л. Домбровський. У дослідженні «Інформаційна безпека держави у системі національної безпеки України» (2024) автор розглядає інформаційну політику держави як важливий регулятор публічних і приватних правовідносин, через котрий реалізуються стратегічні завдання державного розвитку.

Науковець підкреслює, що інформаційна безпека як складова національної безпеки охоплює широкий спектр суспільних відносин, що виникають у процесі функціонування держави, суспільства та особи. У зв’язку з цим ефективне забезпечення інформаційної безпеки потребує вдосконалення як публічно-правових механізмів регулювання, що ґрунтуються на імперативних приписах, так і приватноправових норм, побудованих на засадах диспозитивності. Автор також

звертає увагу на те, що процеси глобальної цифровізації та формування інформаційного суспільства, попри значні переваги для розвитку держави та суспільства, водночас зумовлюють появу нових ризиків та загроз у сфері інформаційних відносин [39]. За таких умов належний рівень інформаційної безпеки виступає важливою передумовою забезпечення законності, правопорядку та стабільності суспільного розвитку, що зумовлює актуальність подальших наукових досліджень у цій сфері.

Отже, дослідження інформаційної безпеки у контексті національної безпеки дозволяють сформувати цілісне уявлення про її місце у системі державного управління. У цьому аспекті інформаційна безпека виступає не лише як самостійний елемент безпекової системи, але й як інструмент забезпечення стабільності функціонування держави та суспільства в умовах сучасних викликів. Зазначене свідчить про необхідність подальшого вдосконалення правових та інституційних механізмів забезпечення інформаційної безпеки з урахуванням динаміки розвитку інформаційного середовища.

Суттєвий внесок у дослідження проблем інформаційної безпеки зробили О. Дєгтяр, О. Носков та К. Мілевський. У праці «Інформаційна безпека у сфері національної безпеки України в умовах сучасних викликів» (2025) автори здійснюють аналіз сучасних загроз інформаційній безпеці держави та їхнього впливу на систему національної безпеки України. У дослідженні наголошується, що сучасні конфлікти дедалі більше характеризуються активним використанням кібернетичних технологій для завдання шкоди критичній інфраструктурі держави та дестабілізації суспільно-політичних процесів.

Автори зазначають, що об’єктами кібератак можуть виступати ключові елементи державної інфраструктури, зокрема енергетичні системи, транспортна інфраструктура, фінансові установи та телекомунікаційні мережі. Порушення функціонування таких систем здатне спричинити значні соціально-економічні наслідки, включаючи перебої в енергопостачанні, дестабілізацію фінансової системи, порушення транспортного сполучення та ускладнення координації діяльності органів державної влади.

Окрему увагу в дослідженні приділено впливу сучасних конфліктів на інформаційну безпеку громадян. Автори підкреслюють, що в умовах цифровізації суспільства зростають ризики, пов’язані зі збором і незаконним використанням персональних даних, кіберзлочинністю, фішинговими атаками та онлайн-стеженням. У таких умовах підвищується ймовірність витоку конфіденційної інформації, що може використовуватися для шантажу, маніпуляцій або інших протиправних дій. Крім того, поширюються практики інформаційного та психологічного тиску на громадян у цифровому середовищі.

Науковці наголошують, що забезпечення інформаційної безпеки у сфері національної безпеки України в умовах сучасних викликів є складним і багатогранним завданням, що потребує комплексного підходу та узгоджених дій держави, суспільства і громадян. Серед ключових напрямів зміцнення інформаційної безпеки вони виокремлюють удосконалення законодавчого регулювання, посилення кіберзахисту критичної інфраструктури, протидію дезінформації, підвищення рівня інформаційної культури населення та розвиток міжнародного співробітництва у сфері безпеки [40].

Таким чином, сучасні наукові дослідження переконливо доводять, що кіберсфера набуває стратегічного значення для національної безпеки. Зростання кількості та складності кіберзагроз свідчить про необхідність переходу від реактивної моделі захисту до проактивної, що передбачає прогнозування ризиків та формування стійкості інформаційних систем. Окрім того, особливої уваги потребує забезпечення безпеки не лише державних інформаційних ресурсів, але й інформаційної безпеки громадян, що є невід’ємною складовою демократичного розвитку держави.

Окрім академічних досліджень, значну роль у формуванні наукового підґрунтя державної політики у сфері інформаційної безпеки відіграють аналітичні центри та науково-дослідні установи. Зокрема, системні дослідження проблем інформаційної безпеки здійснюються Національним інститутом стратегічних досліджень, Інститутом проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України [41], а також низкою профільних наукових установ і центрів стратегічних комунікацій. Результати таких досліджень використовуються при формуванні державної політики

у сфері інформаційної безпеки, розробленні стратегічних документів та вдосконаленні нормативно-правового регулювання інформаційної сфери.

Отже, діяльність аналітичних центрів і науково-дослідних установ відіграє важливу роль у формуванні доказової бази державної політики у сфері інформаційної безпеки. Саме такі інституції забезпечують зв'язок між теоретичними напрацюваннями та практикою їх реалізації, що є необхідною умовою ефективного функціонування системи національної безпеки.

Окремий напрям наукових досліджень присвячено правовому забезпеченню інформаційної безпеки. У цьому контексті варто відзначити праці Т. Костецької, яка досліджує проблеми правового регулювання інформаційних відносин, а також механізми забезпечення інформаційної безпеки в Україні. У роботі «До питання про державний контроль за дотриманням інформаційного законодавства: поняття, окремі види і форми» (2019) авторка підкреслює, що ефективна система інформаційної безпеки потребує належного нормативно-правового регулювання, що має враховувати як національні інтереси держави, так і міжнародні стандарти у сфері захисту інформації [42, с. 316].

Дослідження інформаційної безпеки активно здійснюються також у межах сучасної правової та міждисциплінарної наукової парадигми, що поєднує правові, організаційні та управлінські підходи до забезпечення захисту інформаційних ресурсів. Значний внесок у розвиток концепцій управління інформаційною безпекою здійснено в роботах зарубіжних дослідників, які розглядають інформаційну безпеку як складову системи корпоративного та державного управління ризиками. Зокрема, у монографії «Cybersecurity Governance: An Enterprise Risk Management Strategy for Cyber Risk Control» (2025) автори аналізують механізми управління кіберризиками на рівні організацій та державних інституцій, розглядаючи інформаційну безпеку як інтегровану систему управління ризиками, що включає правові, організаційні та технологічні інструменти забезпечення захисту інформаційних систем. У дослідженні обґрунтовується необхідність інтеграції політики кібербезпеки в систему стратегічного управління та формування моделі кібербезпекового врядування [43].

Значний науковий інтерес становлять також дослідження інформаційної безпеки в контексті розвитку цифрового суспільства та глобального управління інформаційними процесами. Зокрема, у праці «Understanding Cybersecurity Law in Data Sovereignty and Digital Governance» (2022) автори аналізують правові аспекти кібербезпеки, проблеми суверенітету даних та трансформацію правових механізмів регулювання інформаційних відносин у цифровому середовищі. Особлива увага приділяється впливу цифровізації на систему державного управління, формуванню нових моделей правового регулювання кіберпростору та розвитку міжнародних механізмів забезпечення інформаційної безпеки [44].

У сучасних умовах особливої актуальності набувають дослідження, присвячені впливу цифрової трансформації держави на систему інформаційної безпеки. Активне впровадження цифрових технологій, розвиток електронного урядування, поширення соціальних мереж та онлайн-платформ створюють нові можливості для інформаційної взаємодії, але водночас формують нові ризики та загрози для інформаційного простору держави. У зв’язку з цим у науковій літературі все частіше порушуються питання захисту цифрової інфраструктури, протидії дезінформації у соціальних мережах, забезпечення інформаційного суверенітету та формування стійкості суспільства до інформаційних впливів.

Окремий напрям наукових досліджень становлять праці, присвячені проблемам інформаційної безпеки в умовах гібридної війни. Зокрема, у дослідженні О. Беспалька, Ю. Кучеренка, С. Власік, З. Закірової та В. Ткаченка «Інформаційні війни сучасності та застосування мережецентричних систем управління військового призначення» (2023) розглядаються особливості ведення сучасних інформаційних війн та їх вплив на функціонування державних інформаційних систем і військових структур управління. Автори наголошують, що в сучасних умовах боротьба у сфері інформації набуває не меншого значення, ніж традиційне військове протистояння, оскільки контроль над інформаційною інфраструктурою, медіапростором, цифровими ресурсами та суспільною свідомістю дозволяє досягати стратегічних переваг у конфліктах.

У праці підкреслюється, що інформаційні операції, дезінформаційні кампанії та інші форми інформаційного впливу дедалі активніше використовуються державами й недержавними суб'єктами для дестабілізації політичної та соціальної ситуації в інших країнах. У зв'язку з цим спостерігається поступове зміщення протиборства у сферу інформаційного простору, де важливу роль відіграє захист інформаційної інфраструктури держави, державних електронних ресурсів, комунікаційних систем та суспільної свідомості від зовнішніх інформаційних впливів.

На думку авторів, ефективна протидія таким загрозам передбачає поєднання заходів інформаційного впливу та захисту, спрямованих на забезпечення стійкості інформаційної системи держави та її ключових елементів [45]. Отже, у сучасних умовах досягнення інформаційної переваги у конфліктах значною мірою залежить від ефективності функціонування систем управління, комунікаційних технологій та здатності держави протидіяти деструктивним інформаційним впливам.

У цьому контексті також заслуговує на увагу дослідження Є. Срібної, В. Ступницького, О. Крет та Р. Крет «Інформаційні війни та їх вплив на міжнародну репутацію країни» (2024), у котрому автори аналізують природу інформаційних війн, їх основні механізми та інструменти, зокрема дезінформаційні кампанії, пропаганду та стратегічне використання цифрових платформ. У праці обґрунтовується, що поширення дезінформації та маніпулятивних інформаційних впливів становить суттєву загрозу для міжнародної репутації держав, підриває довіру до суспільних інституцій і впливає на формування громадської думки як у середині країни, так і на міжнародній арені. Автори підкреслюють, що ефективна протидія таким загрозам потребує злагодженого підходу, що передбачає розвиток медіаграмотності, використання технологічних інструментів для виявлення та протидії дезінформації, зокрема засобів штучного інтелекту, а також посилення міжнародної співпраці та вдосконалення нормативно-правового регулювання у сфері інформаційної безпеки [46]. Такий підхід сприяє підвищенню стійкості держав до деструктивних інформаційних впливів і захисту їхньої міжнародної репутації.

Важливий внесок у дослідження інформаційної безпеки здійснили також такі українські науковці, як В. Марчук, С. Дерев'янко, Ю. Кобець, Т. Мадрига та інші.

Зокрема, вчені у виданні «Національна безпека України» (2025) комплексно розглядають систему національної безпеки України та акцентують увагу на інформаційній безпеці, як на одному з ключових її елементів та визначають її як стан захищеності інформаційного простору держави від внутрішніх і зовнішніх загроз [47].

У наукових працях зазначених авторів досліджуються різні аспекти інформаційної безпеки, зокрема правове регулювання інформаційних відносин, забезпечення інформаційного суверенітету держави, протидія інформаційним загрозам та формування державної політики у сфері інформаційної безпеки. Значну увагу науковці приділяють також проблемам інформаційної стійкості суспільства, захисту інформаційного простору від зовнішніх інформаційних впливів та розвитку стратегічних комунікацій як інструменту протидії інформаційним операціям.

О. Данильян та О. Дзьобань у своїх працях приділяють значну увагу філософсько-правовим аспектам інформаційної безпеки. У колективній монографії «Інформаційна безпека: філософське та організаційно-правове підґрунтя рефлексії національних інтересів України» (2024) автори досліджують інформаційну безпеку як складне соціальне явище, що формується на перетині політичних, соціальних та правових процесів [48].

Питання кібербезпеки як складової інформаційної безпеки активно досліджуються у працях Д. Селіхова. У наукових роботах автора розглядаються проблеми захисту інформаційно-телекомунікаційних систем, протидії кібератакам та формування державної політики у сфері кібербезпеки. У статті «Кібербезпека як складова інформаційної безпеки: теоретичні та прикладні аспекти» (2026) автор підкреслює, що кіберпростір став новим стратегічним середовищем протистояння держав [49].

Важливо зазначити, що розвиток вітчизняних наукових досліджень у сфері інформаційної безпеки відбувається у тісному взаємозв’язку із зарубіжною науковою думкою, що значною мірою визначає сучасні тенденції осмислення інформаційних процесів у глобальному вимірі. Аналіз зарубіжних підходів дозволяє не лише розширити теоретичне розуміння інформаційної безпеки, але й виявити нові

методологічні підходи до її дослідження, що можуть бути адаптовані в умовах України.

Зокрема, важливими є роботи J. Nye, який у книзі «The Future of Power» (2011) досліджує концепцію «м'якої сили» та інформаційного впливу у міжнародних відносинах [50]. Автор доводить, що контроль над інформаційними потоками та здатність формувати інформаційний порядок денний стають ключовими чинниками геополітичного впливу.

Значний внесок у дослідження інформаційних війн здійснив також M. Castells. У фундаментальній праці «The Rise of the Network Society» (2010) автор аналізує трансформацію сучасного суспільства під впливом інформаційних технологій та формування мережевої структури глобальної комунікації [7]. На думку дослідника, у сучасному світі влада дедалі більше пов'язана з контролем над інформаційними мережами.

Окрему увагу зарубіжні дослідники приділяють проблемам кібербезпеки та кіберконфліктів. У цьому контексті важливим є дослідження T. Rid «Cyber War Will Not Take Place» (2013), у котрому автор аналізує природу кіберконфліктів та їх відмінність від традиційних форм збройного протистояння [31]. Так, особливий акцент робиться на ролі інформації як ресурсу влади та інструменту геополітичного впливу, що дозволяє розглядати інформаційну безпеку не лише як внутрішню проблему держави, але і як складову міжнародної безпеки.

Слід також зазначити, що зарубіжні дослідження інформаційної безпеки значною мірою акцентують увагу на трансформації природи загроз у цифровому середовищі. Зокрема, у фундаментальній праці P. W. Singer та E. T. Brooking «LikeWar: The Weaponization of Social Media» (2018), що зберігає актуальність у сучасних дослідженнях, обґрунтовується, що соціальні мережі перетворилися не лише на інструмент комунікації, але й на ефективний засіб ведення інформаційної війни. Автори доводять, що маніпулятивні інформаційні кампанії, використання бот-мереж і алгоритмічне поширення контенту формують новий тип загроз, котрі складно нейтралізувати традиційними правовими механізмами [51]. Таким чином, інформаційна безпека в умовах стрімкого розвитку інформаційного середовища

виходить за межі суто технічного захисту та охоплює сферу соціальних комунікацій і впливу на суспільну свідомість.

Вагомий внесок у дослідження дезінформації як ключового елементу інформаційної безпеки здійснили C. Wardle та H. Derakhshan у доповіді «Information Disorder: toward an interdisciplinary framework for research and policy making» (2017), концептуальні положення котрої активно розвиваються у сучасних наукових працях 2019–2026 рр. Автори запропонували класифікацію інформаційних загроз, розмежувавши поняття «misinformation», «disinformation» та «malinformation», що дозволяє більш точно ідентифікувати характер деструктивних інформаційних впливів [52]. Отже, сучасні інформаційні загрози мають інтегрований характер і потребують диференційованих підходів до їх аналізу та протидії.

У дослідженні S. Bradshaw та P. N. Howard « The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation» (2019) здійснено ґрунтовний аналіз організованих інформаційних кампаній, що реалізуються державами та недержавними акторами у цифровому середовищі. Дослідники встановили, що у значній кількості країн світу застосовуються технології маніпуляції громадською думкою через соціальні мережі та цифрові платформи, що свідчить про глобальний характер проблеми [53]. У зв’язку з цим інформаційна безпека набуває транснаціонального виміру та потребує узгоджених міжнародних механізмів реагування.

Суттєвий розвиток у сучасній науці отримали дослідження кібербезпеки як складової інформаційної безпеки. Зокрема, у праці R. A. Clarke та R. K. Knake «Cybersecurity and Cyberwar: What Everyone Needs to Know» (2010) обґрунтовується, що кіберпростір став самостійним доменом ведення конфліктів поряд із традиційними середовищами. Автори підкреслюють, що кібератаки можуть мати стратегічні наслідки, включаючи порушення функціонування державних інституцій і критичної інфраструктури [54]. З огляду на викладене, кібербезпека виступає ключовим елементом сучасної системи інформаційної та національної безпеки.

Етичний вимір інформаційної безпеки розкрито у праці L. Floridi «Ethics after the information revolution» (2013), що залишається однією з базових у дослідженні

інформаційної етики та активно використовується у сучасних наукових розвідках. Автор обґрунтовує, що забезпечення інформаційної безпеки пов’язане не лише з технічними чи правовими аспектами, але й із проблемами відповідальності, довіри та етичного використання даних [55]. У цьому контексті інформаційна безпека постає як комплексне явище, що включає також ціннісні та гуманітарні компоненти.

Окремо варто зазначити, що зарубіжні наукові розвідки значною мірою орієнтовані на аналіз глобальних інформаційних процесів та транснаціональних загроз. На відміну від вітчизняної науки, де домінує правовий підхід, у зарубіжних дослідженнях інформаційна безпека розглядається як явище, що охоплює політичні, соціальні, технологічні та психологічні аспекти. Такий підхід дозволяє більш системно оцінювати сучасні виклики інформаційної безпеки, зокрема в умовах цифрової еволюції та глобалізації, що є важливим для подальшого розвитку національної наукової школи.

Так, важливим напрямом сучасних досліджень є захист критичної інформаційної інфраструктури. У звіті European Union Agency for Cybersecurity « ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected» та наступних аналітичних доповідях (2021–2025) підкреслюється, що атаки на енергетичні, транспортні та фінансові системи можуть спричиняти системні збої та масштабні соціально-економічні наслідки [56]. У зв’язку з цим у науковій літературі активно розвивається концепція стійкості (resilience) як ключового елементу забезпечення кібербезпеки. Отже, ефективне забезпечення інформаційної безпеки передбачає не лише захист, але й здатність систем до відновлення та адаптації.

У працях N. Dunn Cavelty, зокрема у монографії «Cyber-Security and Threat Politics: US Efforts to Secure the Information Age» (2007) та подальших наукових розвідках авторки, досліджується процес сек’юритизації кіберпростору, тобто перетворення кібербезпеки на пріоритет державної політики [57]. Авторка зазначає, що держави дедалі активніше інтегрують питання інформаційної безпеки у стратегії національної безпеки, що супроводжується посиленням ролі державних інституцій.

Таким чином, інформаційна безпека набуває стратегічного значення у системі державного управління.

У дослідженні L. Kello «The Virtual Weapon and International Order» (2019) проаналізовано вплив кіберзброї на сучасну систему міжнародних відносин. Автор доводить, що кібероперації формують так звану «сіру зону» між війною та миром, що ускладнює застосування традиційних норм міжнародного права [58]. Це зумовлює необхідність переосмислення правових механізмів забезпечення безпеки у цифрову епоху.

Окремий напрям досліджень пов'язаний із впливом штучного інтелекту на інформаційну безпеку. У доповіді «The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation» (2018), підготовленій M. Brundage та іншими дослідниками, обґрунтовується, що штучний інтелект може використовуватися для автоматизації дезінформації, створення синтетичного контенту та здійснення складних кібератак [59]. У подальших наукових публікаціях наголошується на зростанні ризиків, пов'язаних із розвитком генеративних технологій [60]. Отже, новітні технології суттєво ускладнюють систему інформаційної безпеки, формуючи нові типи загроз.

Саме тому сьогодні особливої уваги потребує проблема використання технологій штучного інтелекту для створення дезінформаційного контенту, зокрема deepfake-технологій, що дозволяють генерувати реалістичні, але неправдиві аудіо- та відеоматеріали. Такі технології суттєво ускладнюють процес ідентифікації достовірної інформації та створюють нові виклики для правового регулювання. У зв'язку з цим виникає необхідність розроблення нових підходів до забезпечення інформаційної безпеки, що враховують специфіку функціонування штучного інтелекту та його вплив на інформаційне середовище.

У сучасних дослідженнях також значна увага приділяється концепції інформаційної стійкості суспільства (societal resilience). Зокрема, в аналітичних матеріалах OECD акцентується, що ефективна протидія інформаційним загрозам неможлива без розвитку медіаграмотності, критичного мислення та підвищення рівня довіри до інституцій [61]. Доведено, що суспільства з високим рівнем інформаційної

культури є менш вразливими до дезінформації. Відтак, ключовим елементом інформаційної безпеки є не лише технічний захист, але й формування стійкості суспільства до інформаційних впливів.

Важливо акцентувати, що сучасний етап розвитку інформаційної безпеки характеризується появою принципово нових викликів, пов’язаних із технологічними змінами, розвитком штучного інтелекту та глобалізацією інформаційних процесів. У цих умовах традиційні підходи до забезпечення безпеки виявляються недостатніми, що зумовлює необхідність формування нових концепцій, орієнтованих на забезпечення стійкості інформаційних систем та суспільства загалом.

Загалом аналіз сучасних зарубіжних наукових джерел свідчить про формування підходу до розуміння інформаційної безпеки, що поєднує правові, технологічні, соціальні та політичні аспекти. У наукових працях послідовно обґрунтовується необхідність інтеграції різних рівнів забезпечення безпеки – від технічного захисту до стратегічного управління інформаційним простором [62]. Таким чином, інформаційна безпека постає як багатовимірний феномен, що потребує злагодженої державної політики.

Важливо, що значний вплив на формування сучасних підходів до дослідження інформаційної безпеки мають також міжнародні аналітичні центри та організації, зокрема НАТО, Європейський Союз та Організація Об’єднаних Націй. У доповідях НАТО неодноразово підкреслюється, що інформаційні операції, кібератаки та дезінформація є ключовими загрозами сучасній безпеці держав [63].

Зокрема, у звітах Центру передового досвіду НАТО з питань стратегічних комунікацій (NATO Strategic Communications Centre of Excellence) аналізуються сучасні інформаційні кампанії, спрямовані на дестабілізацію демократичних інституцій та вплив на громадську думку [64].

Важливу роль у розвитку досліджень інформаційної безпеки відіграють також міжнародні організації, такі як Рада Європи та Європейський Союз, що здійснюють всебічні дослідження у сфері боротьби з дезінформацією, захисту інформаційного простору та забезпечення кібербезпеки. У документах Європейської Комісії неодноразово підкреслюється необхідність розроблення політики протидії

інформаційним загрозам у цифровому середовищі [65]. Безумовно, міжнародний досвід у сфері забезпечення інформаційної безпеки має важливе значення для вдосконалення національної політики України. Використання кращих практик міжнародних організацій сприяє підвищенню ефективності протидії інформаційним загрозам та інтеграції України у глобальну систему безпеки.

Слід зазначити, що сучасний стан наукових досліджень інформаційної безпеки характеризується значною різноманітністю наукових підходів. Дослідження здійснюються у межах різних галузей науки – права, політології, соціології, інформаційних технологій та міжнародних відносин. Це зумовлено складною природою інформаційної безпеки, що охоплює широкий спектр суспільних відносин та безпекових викликів сучасності.

Аналіз наукових джерел свідчить, що інформаційна безпека поступово перетворилася на один із ключових напрямів сучасних безпекових досліджень. Її наукове осмислення відбувається у контексті глобальних трансформацій інформаційного середовища, стрімкого розвитку цифрових технологій та посилення інформаційного протиборства між державами. У цих умовах інформаційна безпека розглядається не лише як технічна або правова категорія, але і як комплексне соціально-політичне явище, що безпосередньо впливає на стабільність держави, функціонування демократичних інститутів та забезпечення національних інтересів.

Вагомий внесок у розвиток наукових досліджень проблем національної, інформаційної безпеки та демократичного врядування здійснила Л. Наливайко. У наукових працях дослідниці значна увага приділяється проблемам забезпечення прозорості діяльності органів публічної влади, розвитку механізмів громадського контролю та реалізації права громадян на доступ до інформації як важливої передумови функціонування демократичної правової держави. У цьому контексті інформаційна відкритість держави розглядається авторкою як один із ключових чинників забезпечення ефективної взаємодії між державою та суспільством, а також як важливий елемент системи національної безпеки.

Зокрема, у науковій статті «Право на доступ до публічної інформації в контексті контролю громадян за діяльністю держави» (2014) Л. Наливайко та С. Вітвіцький

досліджують роль доступу до публічної інформації як механізму забезпечення прозорості діяльності органів влади та реалізації принципів відкритості державного управління. Автори підкреслюють, що забезпечення ефективних механізмів доступу до інформації сприяє підвищенню рівня довіри громадян до державних інституцій, формуванню ефективного громадського контролю та зміцненню демократичних засад функціонування держави [66].

Важливе значення для дослідження проблем інформаційної відкритості держави має також праця Л. Наливайко «Transparency as a democratic standard of the government functioning» (2014), у якій авторка розглядає прозорість діяльності органів влади як один із ключових демократичних стандартів сучасного державного управління. На думку дослідниці, забезпечення відкритості та підзвітності органів публічної влади сприяє підвищенню ефективності державного управління, зміцненню принципу верховенства права та формуванню ефективних механізмів захисту прав і свобод людини [67].

Окрему увагу у наукових працях Л. Наливайко приділено ролі інститутів громадянського суспільства у забезпеченні демократичного розвитку держави та захисті прав людини. Так, у навчальному посібнику «Неурядові правозахисні організації України» (2014) авторка, зокрема комплексно досліджує діяльність правозахисних інституцій, їх роль у формуванні громадянського контролю за діяльністю державних органів, а також їх значення у розвитку демократичних механізмів захисту прав і свобод людини [68].

Наукові підходи Л. Наливайко сприяють формуванню сучасного розуміння інформаційної відкритості держави як важливого елементу демократичного врядування та системи національної безпеки. Її наукові напрацювання створюють вагоме теоретичне підґрунтя для подальших досліджень проблем інформаційної безпеки, розвитку інформаційного суспільства та вдосконалення механізмів взаємодії держави і громадянського суспільства.

Узагальнення наукових підходів до дослідження інформаційної безпеки дозволяє виділити кілька основних теоретичних концепцій її розуміння. По-перше, правовий підхід, у межах котрого інформаційна безпека розглядається як стан

правового захисту інформаційних відносин, інформаційних ресурсів та інформаційних прав громадян. По-друге, безпековий підхід, відповідно до котрого інформаційна безпека трактується як складова системи національної безпеки держави та пов'язується із захистом національних інтересів у інформаційній сфері. По-третє, соціально-комунікаційний підхід, що акцентує увагу на інформаційних впливах, комунікаційних процесах та інформаційній взаємодії у суспільстві. По-четверте, технологічний підхід, у межах котрого досліджуються проблеми захисту інформаційно-телекомунікаційних систем, кіберпростору та цифрової інфраструктури.

Зазначені підходи дозволяють також здійснити класифікацію наукових досліджень інформаційної безпеки за різними критеріями, зокрема за галузевою приналежністю (правові, політичні, соціологічні, технологічні) та за територіальним підходом (вітчизняні та зарубіжні).

Таким чином, наукові підходи до розуміння інформаційної безпеки характеризуються концептуальною різноманітністю, що зумовлено складністю самого об'єкта дослідження. Зазначена багатовекторність підходів не є недоліком, а навпаки свідчить про формування інтегрованого підходу до дослідження інформаційної безпеки. Це, у свою чергу, обумовлює необхідність застосування відповідного методологічного інструментарію, що поєднує правові, соціологічні, політичні та технологічні методи аналізу.

Важливо, що на сучасному етапі наукових розвідок, окремі аспекти інформаційної безпеки досліджуються в межах різних галузей науки. У науковій літературі сформовано значну кількість підходів до розуміння цього явища, що свідчить про його складну природу. Водночас така концептуальна різноманітність не лише ускладнює формування уніфікованої теоретичної моделі, але й свідчить про об'єктивну багатовимірність інформаційної безпеки як наукової категорії, що потребує узгодження існуючих підходів у межах інтегративної концепції.

Аналіз наукових праць вітчизняних і зарубіжних учених, монографічних досліджень, дисертаційних робіт, аналітичних доповідей міжнародних організацій та

інших джерел у сфері інформаційної безпеки дає змогу виділити такі узагальнені положення:

1. Наукові дослідження інформаційної безпеки в Україні формувалися як поступовий перехід від її фрагментарного розгляду у межах інформаційної політики та системи національної безпеки до становлення як самостійного напряму наукового пізнання. Така трансформація зумовлена як внутрішніми процесами розвитку інформаційного суспільства, так і впливом безпекових викликів, пов'язаних із воєнними конфліктами, що актуалізували розуміння інформаційної безпеки як інтегрованого елементу системи національної безпеки держави.

2. Ретроспективний та сучасний аналіз наукових підходів свідчить про відсутність уніфікованого трактування сутності інформаційної безпеки, що проявляється у поєднанні правового, безпекового, технологічного та соціально-комунікаційного підходів. Зазначена концептуальна множинність, з одного боку, ускладнює формування єдиної теоретичної моделі, а з іншого –об'єктивно відображає багатовимірний характер інформаційної безпеки як складної соціально-правової категорії. У зв'язку з цим, обґрунтованою є необхідність її розгляду як комплексного феномену, що охоплює захист інформаційного простору, інформаційних прав людини та забезпечення інформаційного суверенітету держави.

3. Сучасний етап розвитку наукових досліджень характеризується посиленням міждисциплінарного підходу до аналізу інформаційної безпеки, що виявляється у поєднанні правових, політичних, соціальних і технологічних аспектів. У цьому контексті інформаційну безпеку доцільно розглядати не лише як об'єкт правового регулювання, але і як стратегічний ресурс держави, що визначає стійкість її інституцій, ефективність публічного управління та здатність протидіяти сучасним інформаційним загрозам.

4. Вплив воєнного стану та гібридних форм протиборства зумовив переосмислення ролі інформаційної безпеки у системі національної безпеки, у межах котрої вона набуває ознак самостійного функціонального елементу, тісно пов'язаного з кібербезпекою, інформаційною політикою та стратегічними комунікаціями. За таких умов інформаційний простір постає як окремий домен протиборства, що

потребує відповідного теоретико-правового осмислення та вдосконалення механізмів державного регулювання.

5. Наукові напрацювання вітчизняних і зарубіжних дослідників, а також аналітичні матеріали міжнародних організацій формують підґрунтя для розширення методологічних меж дослідження інформаційної безпеки, зокрема шляхом інтеграції концепцій кіберстійкості, управління ризиками, протидії дезінформації та забезпечення інформаційної стійкості суспільства. Зазначений підхід орієнтує на формування сучасної моделі інформаційної безпеки, адаптованої до умов цифровізації та безпекових викликів.

6. Попри значний масив наукових досліджень, проблематика інформаційної безпеки, зокрема в умовах воєнного стану, не отримала належної систематизації у теоретико-правовому вимірі, що проявляється у відсутності цілісної концепції її функціонування як складової національної безпеки. Це зумовлює необхідність подальшого розвитку наукового підходу, спрямованого на узгодження існуючих теоретичних положень та формування єдиної концептуальної моделі забезпечення інформаційної безпеки держави, що становить перспективний напрям подальших досліджень.

1.3. Поняття, ознаки, складові інформаційної безпеки України та її місце у системі національної безпеки в умовах воєнного стану

Інформація є потужним засобом контролю над людиною і людськими спільнотами, альтернативи якому ніколи не існувало в історії. Інформаційний вплив здатний змінювати і руйнувати стабільні соціальні, політичні та психологічні конструкції суспільства. В умовах ведення відсічі воєнній агресії, інформація може дестабілізувати політичну ситуацію, сформувати викривлену картину реальності в суспільстві. Інформаційний вплив ворога може бути спрямований на зміну ціннісних орієнтирів, переконань та моделей поведінки, що у довгостроковій перспективі призводить до руйнування національної ідентичності, соціальної згуртованості та психологічної стійкості суспільства.

Це чітко усвідомлює держава-агресор та використовує увесь потенціал інформаційно-психологічних операцій як проти українського суспільства, так і проти громадян держав-партнерів України.

Отож, значення інформаційної безпеки в умовах воєнного стану є пріоритетним, безальтернативно важливим. Захищеність інформаційного простору держави, стабільність та недоторканість інформаційної сфери є не менш важливими ніж воєнна безпека.

Питанням інформаційної безпеки в правничій науці завжди приділялось вагоме значення.

Результати дослідження різних аспектів інформаційної безпеки отримали розкриття у наукових працях таких вчених, як І. Арістова, О. Баранов, І. Березовська, В. Брижко, В. Василюк, Н. Влажик, В. Голубєв, В. Горбулін, В. Гурковський, В. Демиденко, О. Дзьобань, О. Довгань, О. Додонов, В. Ємельянов, І. Забара, Р. Калюжний, Н. Камінська, В. Конах, О. Косогов, Б. Кормич, О. Кирилюк, О. Литвиненко, В. Ліпкан, Ю. Максименко, А. Марущак, Л. Наливайко, А. Нашинець-Наумова, Н. Ніжник, Г. Новицький, В. Остроухов, А. Пазюк, М. Панов, В. Пилипчук, В. Політанський, М. Потрубач, Г. Почепцов, М. Присяжнюк, А. Прозоров, В. Рубан, О. Сивак, С. Стрельцов, О. Тихомиров, П. Ткачук, В. Хорошко, Ю. Хохлачова, В. Цимбалюк, О. Юдін та багатьох інших. Особливості забезпечення інформаційної безпеки в умовах воєнного стану досліджували: Н. Авер'янова, В. Аніщук, Т. Воропаєва, А. Клочко, І. Котерлін, В. Котляров, В. Кучер, Д. Лобода, Н, Лугіна, І. Милосердна, В. Новицький, Н. Прямухіна, А. Русакевич, Є. Соломін, О. Старостін, М. Шевчук та ін. Проте, відсутні комплексні наукові дослідження із застосуванням міждисциплінарного підходу, присвячені інформаційній безпеці України та її місцю у системі національної безпеки в умовах воєнного стану.

Отож, зазначене обумовлює мету наукового пошуку в рамках цього підрозділу, а саме розкрити поняття, ознаки, складові інформаційної безпеки України та її місце у системі національної безпеки в умовах воєнного стану.

Інформація набуває властивості потужного засобу впливу на громадсько-політичні, ідеологічні та соціально-економічні процеси, стає свого роду зброєю, яка

вимагає створення системи протидії, захисту інформаційних ресурсів, які належать державним органам, що становлять державну, професійну, особисту таємницю [69, с. 21]. Воєнні конфлікти в сучасному світі включають в себе не лише бойові дії на полі бою, але й активну діяльність в сфері «інформаційної експансії» – що полягає в досягненні національних інтересів методом безконфліктного проникнення в чужу інформаційну сферу і розширення власних можливостей із використанням інформаційних ресурсів [70, с. 37; 385]. Попри те, що рф тривалий час здійснює вплив на інформаційну безпеку України, наша держава не була готовою реагувати на деякі інформаційні загрози після початку повномасштабного вторгнення. Показово, що і розпочалось воно в супроводі інформаційних маніпуляцій.

Оскільки інформаційний простір стає значущим полем боротьби в умовах воєнних конфліктів, розуміння інформаційної безпеки дає змогу виробляти необхідні стратегії в умовах нестабільності та загроз [71]. Український інформаційний простір не захищений від зовнішньої негативної пропаганди та маніпулятивних впливів і стає об’єктом інформаційної експансії. Інформаційно-комунікаційна політика України у сфері національної безпеки потребує невідкладного перегляду та вдосконалення. Рівень інформаційної безпеки держави багато в чому залежить від рівня її інформаційної інфраструктури [72, с. 348; 380]. Відсіч інформаційних загроз потребує унікальних та інноваційних рішень, але часто такі рішення впливають на права людини, обмежуючи їх.

Підходи щодо забезпечення інформаційної безпеки не відповідають рівню сучасного інформаційного прогресу, що ускладнює спроможність держави ефективно реагувати на нові інформаційні загрози. Попри значні темпи розвитку інформаційної сфери, суб’єкти забезпечення інформаційної безпеки демонструють низьку оперативність і гнучкість. Такий розрив посилюється в умовах воєнного стану та зростання інтенсивності інформаційних атак.

Еволюція національної безпеки держави відбувається відповідно до викликів, з якими вона стикається, і засобів, які вона може застосувати для боротьби з цими викликами. Нетрадиційні виклики безпеці та питання інформаційної безпеки посіли важливе місце в дискурсі національної безпеки країн та світу загалом [73]. Сутність і

зміст інформаційної безпеки трансформується під впливом обставин. Це повсякчас обумовлює потребу її переосмислення.

На сьогодні серед вчених відсутнє єдине розуміння категорії «національна безпека», що розглядається за допомогою широкого спектру підходів. Тим більше, не сформовано єдиного розуміння її похідних, зокрема інформаційної безпеки.

Перш за все, слід відзначити, що поняття «інформаційна безпека» застосовується в технічних і суспільно-гуманітарних науках по-різному.

Так, представник сфери технічних досліджень Дж. Фрулінгер зауважує, шо інформаційна безпека – це набір методів, призначених для захисту даних від несанкціонованого доступу або змін, як при зберіганні, так і при передачі з одного приладу або фізичного розташування на інше. Іноді під ІБ також розуміють безпеку даних (від англ. Data security) [74]. С. Кавун, В. Носов та О. Манжай зазначають, що організація захисту інформації здійснюється за допомогою системи правових, організаційних та інженерно-технічних заходів. Реалізація організаційних та інженерно-технічних заходів становить суть процесів технічного захисту інформації [75]. І. Сопілко узагальнює, що інформаційна безпека – це набір інструментів і методик, розроблених і використовуваних для захисту конфіденційної інформації від зміни, порушення, знищення і перевірки [76]. Інформаційна безпека – багатогранне явище, що має і матеріально-технічну, і соціально-гуманітарну, і політичну та економічну, культурну сторони. Тому ця наукова проблематика має міжгалузевий характер, однак саме суспільні науки розглядають інформаційну безпеку як широку, змістовно наповнену, багатофункціональну категорію.

Правова основа інформаційної безпеки є тим базисом, на якому будується вся система її забезпечення. Отож, важливим є розгляд поняття, ознак та структури інформаційної безпеки з позиції теорії права.

Категорія «інформаційна безпека» складається з двох самостійних термінів, що мають власний зміст. В довідниковій літературі поняття «безпека» визначається як стан, коли кому-, чому-небудь ніщо не загрожує [77, с. 137; 78 с. 43]. Поняття «інформація» (від лат. informatio – роз'яснення) визначено, як відомості про які-

небудь події, чиюсь діяльність і т. ін.; повідомлення про щось [79]. У поєднанні ці два терміни позначають нове явище, достатньо широке і конкретне.

У правничій літературі термін «інформаційна безпека» наділено широким діапазоном значень, що вироблені у результаті тривалого наукового пошуку.

Можна виокремити декілька самостійних етапів наукової розробки доктрини інформаційної безпеки, що обумовлені політико-правовими і безпековими аспектами: 1) початковий етап (1991 – 2000 рр.), коли з моменту набуття незалежності України розпочалось формування власних концептуальних засад інформаційної безпеки, вибір стратегічного курсу держави в інформаційній сфері та здійснено перші спроби правового врегулювання інформаційної безпеки; 2) етап концептуалізації та реалізації державної політики в інформаційній сфері (2001 – 2013 рр.). На цей етап припадає значна кількість наукових досліджень концепції національної інформаційної безпеки, а також ухвалення ключових законів України у сфері інформації, кібербезпеки, захисту персональних даних тощо; 3) етап протидії гібридній агресії рф (2014-2021 рр.), що докорінно змінив розуміння концепту інформаційної безпеки та обумовив розвиток практики в цій сфері. У зв’язку з агресією рф проти України відкрились конкретні, чіткі загрози інформаційній безпеці, отож вчені перейшли до осмислення відповідних засобів протидії; 4) етап протидії інформаційним загрозам в умовах повномасштабної агресії рф та введеного воєнного стану (2022 р. – по т.ч.). На цьому етапі відбулась друга хвиля фундаментального переосмисленням ролі інформаційної безпеки у контексті відновлення національної безпеки та відсічі гібридної агресії.

Отже, частина наукових досліджень, проведених в проміжку з 1991 р. до 2014 р. утворили фундаментальну основу інформаційної безпеки як наукового конструкту. Але вони були підготовлені без усвідомлення реального контексту гірбидної агресії, особливостей впливу конкретних інформаційних загроз на українське суспільство і державу в цілому. Наукові праці, підготовлені після 2014 р. врахували цей аспект. Проте, інформаційна сфера дуже багатогранна і складна, тому ворог активно вдається до креативних, системних, дієвих заходів деструктивного впливу на неї. Отож, подальше вивчення інформаційної безпеки ніколи не втрачатиме актуальності.

Загалом, склалося декілька підходів до розуміння інформаційної безпеки, що базуються на відповідних підходах до визначення сутності національної безпеки, як родової категорії.

А. Нашинець-Наумова, проаналізувавши зміст та напрями досліджень інформаційної безпеки, виокремила декілька підходів її розуміння в якості: стану захищеності інформаційного простору; процесу управління загрозами та небезпеками, що забезпечує інформаційний суверенітет України; стану захищеності національних інтересів України в інформаційному середовищі; захищеності встановлених законом правил, за якими відбуваються інформаційні процеси в державі; стану захищеності національних інтересів країни в інформаційній сфері; до суспільних відносин, пов'язаних із захистом життєвоважливих інтересів людини і громадянина, суспільства та держави від реальних та потенційних загроз в інформаційному просторі; важливої функції держави; невід'ємної частини політичної, економічної, оборонної та інших складових національної безпеки [80, с. 15]. В. Шемчук зазначає, що цю категорію можна розглядати через такі підходи, як: 1) статичний (безпека як стан захищеності інформаційного середовища/інформації, система гарантій тощо); 2) діяльнісний (безпека як процес її забезпечення, здатність держави ефективно захистити національні інтереси й цінності); 3) комплексний (безпека як стан і процес) [81]. Дійсно, інформаційна безпека – це складна конструкція, розкриття якої за допомогою єдиного підходу не може надати релевантного, об'єктивного результату.

Більш традиційним у правничій літературі є *статичний підхід* до розуміння інформаційної безпеки як стану захищеності її об'єктів від загроз. Його підтримує низка авторитетних вчених.

Так, Г. Сащук, зазначає, що інформаційна безпека – це такий стан захищеності життєво-важливих інтересів, а, отже, й інформаційної озброєності держави, суспільства, особистості, за якого ніякі інформаційні впливи на них неспроможні викликати деструктивні думки і дії, що призводять до негативних відхилень на шляху стійкого прогресивного розвитку названих суб'єктів [82]. В. Гур'єв, Д. Мехед, Ю. Ткач та І. Фірсова визначають її як захищеність (стан захищеності) основних

інтересів особи, суспільства і держави у сфері інформації, включаючи інформаційну й телекомунікаційну інфраструктуру і власне інформацію та її параметри, такі як повнота, об'єктивність, доступність і конфіденційність [83]. Б. Кормич – як захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані конституцією умови існування і розвитку людини, всього суспільства і держави [84, с. 92]. В. Лук'янова та А. Лаутар – як стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави [85, с. 97]. О. Данільян, О. Дзьобань, М. Панов визначають інформаційну безпеку як безпеку об'єкта від інформаційних загроз або негативних впливів, пов'язаних з інформацією та нерозголошення даних про той чи інший об'єкт, що є державною таємницею [86]. О. Баранов розуміє інформаційну безпеку як стан захищеності національних інтересів України в інформаційному середовищі, за якого не допускається (або зводиться до мінімуму) завдання шкоди особі, суспільству, державі через неповноту, несвоєчасність, недостовірність інформації й несанкціоноване її поширення та використання, а також через негативний інформаційний вплив та негативні наслідки функціонування інформаційних технологій [87, с. 60-62]. В. Петрик, зауважує, що – це стан захищеності особи, суспільства і держави, при якому досягається інформаційний розвиток, технічний, інтелектуальний, соціально-політичний, морально-етичний, за якого сторонні інформаційні впливи не завдають їм суттєвої шкоди [88, с. 49-52]. О. Тихомиров зазначає, що інформаційна безпека – це стан інформаційної системи загалом та її елементів зокрема, що характеризується сукупністю умов оптимального функціонування і розвитку в інформаційній сфері та можливостями їх усвідомлення та контролю [89, с. 74]. К. Фокіна-Мезенцева зауважує, що – це стан захищеності інформації всередині суспільства, який забезпечує її формування, використання та розвиток в інтересах громадян, організації, держави; захист конфіденційності, цілісності та доступності інформації [90]. Аналіз наукових підходів до визначення сутності інформаційної безпеки з точки зору статичного підходу свідчить про її складний, комплексний характер та багатовимірність.

Отже, на думку авторів стан захищеності інформаційної сфери держави, суспільства і людини робить можливим: функціонування інформаційного середовища та інформаційних відносин; повноцінну реалізацію життєво важливих інтересів у інформаційні сфері; забезпечення правопорядку і законності у цій сфері; недопущення інформаційних загроз та мінімізацію завдання ворогом шкоди інформаційній сфері; сталий інформаційний та соціальний розвиток. В розрізі воєнного стану до цього переліку варто додати: інформаційну стійкість суспільства; забезпеченість населення достовірною та актуальною інформацією; стабільність критичної інформаційної та комунікаційної інфраструктури та ін.

Незважаючи на свою популярність та поширеність, статичний підхід до розуміння інформаційної безпеки піддається критиці.

В. Ліпкан, Ю. Максименко та В. Желіховський підкреслюють, що конструкція «стан захищеності (захисту)» сформувалося в часи, коли «безпека» мала конкретне вираження, переважно в речах, і вимірювалася їх станом. Стан речей (матеріальних цінностей), їх властивостей був чітко визначений, здебільшого не змінювався, а зміна зумовлювала новий сталий стан. Вищезгадана конструкція справедливо критикується й через те, що віддзеркалює безпекознавчу парадигму, що існувала за радянських часів, коли пріоритет надавався захисту щодо попередження. Національна безпека розглядається в якості інтегративної сукупності різних сфер життєдіяльності суспільства, однією з яких є інформаційна сфера [91]. О. Малашко та М. Ковалів відзначають, що такий підхід набуває певне протиріччя з однією з її основних характеристик – динамічністю. Інформаційна безпека, будучи частиною системи національної безпеки, сама є системою. Так знаходить вияв її дуалістична сутність [92]. К. Ісмайлов аргументує, що термін «інформаційна безпека» на даний момент часу не є коректним по своїй суті. Замість нього він пропонує вживати термін «інформаційна захищеність» і використовувати для нього таке визначення: інформаційна захищеність – це захист конфіденційності, цілісності та доступності інформації [93]. Загалом погоджуючись з окремими недоліками статичного підходу, зауважимо що він все ж не позбавлений об’єктивності і обґрунтованості.

У Законі України «Про національну безпеку України» від 21 червня 2018 р. [94] визначено поняття «воєнна безпека», «громадська безпека і порядок», «державна безпека», «національна безпека України» через словосполучення «стан захищеності».

Також, що чинна Стратегія інформаційної безпеки, затверджена Указом Президента України від 28 грудня 2021 р. № 685/2021 закріплює статичний підхід до розуміння інформаційної безпеки України, як складової частина національної безпеки України, стану захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом [95].

Узагальнюючи, підкреслимо, що статичний підхід відображає одну, конкретну сторону інформаційної безпеки, хоча вона не може існувати відокремлено від динамічної сторони.

Динамічний підхід до розуміння інформаційної безпеки зміщує акцент на процес, діяльність щодо її забезпечення та уможливлення.

Л. Наливайко визначає інформаційну безпеку як сукупність засобів забезпечення інформаційного суверенітету України, захист інформаційної сфери від зовнішніх і внутрішніх інформаційних загроз [96]. Г. Гончаренко констатує, що інформаційна безпека охоплює більш широкий спектр заходів і підходів, включаючи політику, процеси та людський фактор [97]. Л. Харченко, В. Ліпкан та О. Логінов визначають, що інформаційна безпека – це складник національної безпеки, процес управління загрозами та небезпеками, державними й недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України [98, с. 47]. О. Литвиненко визначає інформаційну безпеку як забезпечення захисту інформації; забезпечення захисту й контролю національного інформаційного

простору; забезпечення належного рівня інформаційної достатності [99]. Т. Ткачук тлумачить інформаційну безпеку як перманентний процес діяльності компетентних органів, спрямований на запобігання і протидію загрозам в інформаційній сфері, застосування активних заходів інформаційного впливу, а також сукупність умов такої діяльності, які реалізуються й здатні контролюватися тривалий час. Основною метою забезпечення інформаційної безпеки є створення безпечного інформаційного середовища [100, с. 379]. Отже, динамічний підхід до розуміння інформаційної безпеки відображає сучасні тенденції її наукового осмислення, акцентуючи увагу не лише на стані захищеності інформаційної сфери, а й на постійному, цілеспрямованому процесі його забезпеченні. В проаналізованих наукових позиціях дослідників інформаційна безпека розглядається не як статична категорія, а як комплексна динамічна система заходів, політик, активностей державних та недержавних інституцій, що спрямовані на захист інформаційної сфери від внутрішніх і зовнішніх загроз.

При цьому, за динамічного підходу залишається неуточненим розмежування понять «інформаційна безпека» та «забезпечення інформаційної безпеки». Останнє є хоч і похідною, але самостійною категорією.

Існують і підходи, які складно однозначно віднести до статичного чи динамічного. Автори вдаються до визначення сутності інформаційної безпеки, зокрема, через перелік її складників чи значущих характеристик.

Так, А. Марущак визначає інформаційну безпеку через комплекс прав людини вільно, безперешкодно, на власний розсуд бути суб'єктом інформаційних процесів (шукати, одержувати та поширювати інформацію) та отримувати захист від неправомірного інформаційного втручання [101, с. 82]. А. Нашинець-Наумова розкриває інформаційну безпеку України як сукупність життєво важливих умов функціонування суб'єктів (особи, суспільства, держави) в інформаційній сфері та суб'єктивних (правових, політичних, інформаційних, наукових, оперативно-розшукових) можливостей їх усвідомлення й контролю [80, с. 10]. Т. Перун пропонує розглядати інформаційну безпеку як систему суспільних відносин, що виражає зв'язок між інтересами особи, суспільства та держави в сфері інформації та правового

забезпечення їхнього захисту, що охоплює стан захищеності інформаційного простору, інформації і інформаційних ресурсів держави, інформаційно-телекомунікаційної інфраструктури від можливих внутрішніх і зовнішніх загроз [102, с. 198]. Зазначені підходи демонструють тенденцію розширеного розуміння інформаційної безпеки, орієнтацію на комплексне бачення цього явища як багатогранної соціально-правової конструкції.

Поряд зі статичним та динамічним підходами в науковій літературі існують концепції, які можна віднести до комплексного підходу. Вони поєднують в собі як елементи статики, так і динаміки, а також звертаються до ключових характеристик цього явища.

В умовах воєнного стану та відсічі повномасштабної воєнної агресії рф відбувається формування інтегративного, міждисциплінарного бачення сутності інформаційної безпеки, що враховує як стан захищеності інформаційної сфери, так і необхідності постійної діяльності щодо забезпечення захисту інформаційного простору та збалансування інформаційних інтересів особи, суспільства та держави.

Прикладом комплексного підходу є запропоноване Т. Воропаєвою та Н. Авер'яновою визначення інформаційної безпеки як багатопланового, багатокомпонентного та багаторівневого феномену: 1) як системи, що складається інформаційно-технологічної та інформаційно-психологічної підсистеми; 2) як системи, що має кілька вимірів (правовий, політичний, управлінський, технічний, соціально-комунікаційний, ідеологічний, світоглядний, психологічний, науковий, освітній тощо). На думку дослідниць, інтегративний підхід уможливлює цілісне бачення системи інформаційної безпеки України і дає релевантний інструментарій для її трансдисциплінарного дослідження з урахуванням тісного взаємозв'язку її підсистем та основних вимірів [103]. О. Золотар зауважує, що інформаційна безпека являє собою складну, динамічну, цілісну соціальну систему, компонентами якої є підсистеми безпеки особистості, держави і суспільства. Саме взаємозалежна, системна інформаційна єдність останніх складає якісну визначеність, покликану здійснити захист життєво важливих інтересів людини, суспільства і держави, забезпечити їх конкурентноздатний, прогресивний розвиток [104, с. 154].

Комплексний підхід відображає сучасні виклики в умовах воєнного стану, технологічного розвитку та інформаційної глобалізації. Ми підтримуємо комплексне розуміння інформаційної безпеки, яку слід розуміти як складний, багатоелементний конструкт.

Осмислення поняття та ознак інформаційної безпеки в умовах воєнного стану не можливе без визначення її місця в системі національної безпеки України.

Інформаційна безпека як явище існує не ізольовано, а в тісному взаємозв'язку з іншими сферами, що забезпечують суверенітет, територіальну цілісність, стабільність та захищеність держави. Отож, важливо окреслити місце інформаційної безпеки в системі національної безпеки України.

О. Косогов вважає інформаційну безпеку складовою воєнної безпеки України та акцентує на залежності реалізації найбільш важливих інтересів України у воєнній сфері від інформаційних загроз [105]. Інформаційна сфера виступає системоутворюючим чинником, поєднуючи в єдиному інформаційному просторі всі інші сфери військової безпеки держави [106-107]. Інформаційна безпека виконує функцію інтеграції та консолідації всіх інших складових національної безпеки, зокрема і воєнної.

Н. Нижник, Г. Ситник та В. Білоус відносить інформаційну безпеку до складових національної безпеки України [108, с. 5]. Такий підхід підтримують В. Аніщук [109]; Н. Авер'янова, Т Воропаєва [110]; І. Бондар [111]. А. Войціховський [112]; П. Біленчук, Л. Борисова, І. Неклонський, В. Собина [113]. М. Гаврильців [114]; Л. Домбровський [39]; В. Кононенко, Л. Новікова, П. Копицька [115]; В. Котляров [116]; В. Конах [117]; В. Кучер [118]; Ф. Медвідь [119]; О. Малашко, М. Ковалів [92]; Т. Мужанова [121, с. 11-12]; І. Милосердна [73, с. 187]; Л. Наливайко [96]; О. Панченко [122]; А. Русакевич [123]; Г. Сащук [82]; О. Старостін [124]; В. Супрун [125]; В. Торяник [126]. Л. Харченко, В. Ліпкан, О. Логінов [98, с. 47]; М. Шевчук [127]. Погоджуючись із позицією вчених, зауважимо, що інформаційна безпека посідає стратегічно важливе місце в системі національної безпеки України, вона є невід'ємною умовою збереження державності та сталого розвитку суспільства.

Існує думка, що у концептуальному плані національна безпека становить собою цілісний екзистенціальний феномен, відтак не може бути репрезентована сукупністю корелятивно пов'язаних складових (економічна, інформаційна, політична безпека тощо). Національну безпеку слід аналізувати крізь призму її системних властивостей, отже доцільно казати про національну безпеку в інформаційній сфері, екологічній та ін. Адже із появою інших «складових» національна безпека як така не змінить своєї сутності. Водночас, коли йтиметься про прояви національної безпеки у різних сферах життєдіяльності, то поява чи то нових суспільних відносин, чи то сфер життєдіяльності жодним чином не вплине на зміст національної безпеки, лише змінить її форму, оскільки національна безпека знаходитиме свій прояв в нових сферах. Органічна ж сукупність елементів, що входять до національного середовища, поєднані між собою кореляційними зв'язками, утворюють систему національної безпеки. Саме у цьому полягає основні відхилення наукових досліджень безпекової проблематики, котрі при дослідженні даного феномену не використовують евристичний потенціал національнознавчого підходу [91]. Зазначений підхід заперечує фрагментарне уявлення про національну безпеку як сукупності окремих складових (економічної, інформаційної, політичної тощо), натомість пропонує розглядати її крізь призму системних властивостей, що проявляються у різних сферах. У цьому контексті інформаційна безпека постає не окремою складовою, а формою прояву національної безпеки в інформаційній сфері. Взаємопов'язаність елементів національної безпеки утворює складну, динамічну систему, де інформаційна безпека є органічною складовою національного середовища.

Особливістю інформаційної безпеки є те, що вона, як невід'ємна частина, входить до інших складових національної безпеки: економічної, воєнної, політичної безпеки тощо [83]. Роль інформаційної безпеки та її місце в системі національної безпеки держави стає все значнішою. Це відбувається внаслідок таких чинників: національні інтереси, загрози їм і забезпечення захисту від цих загроз у всіх галузях національної безпеки виражаються, реалізуються і здійснюються через інформацію та інформаційну сферу; особа та її права, інформація та інформаційні системи і права

на них – це основні об'єкти не тільки інформаційної безпеки, а й основні елементи всіх об'єктів безпеки в усіх її галузях; вирішення завдань національної безпеки пов'язане з використанням інформаційно-комунікаційних засобів та технологій як основних на сучасному етапі; проблема національної безпеки має яскраво виражений інформаційний характер [121, с. 11-12]. Необхідність гарантування інформаційної безпеки зумовлюється: 1) потребою забезпечення національної безпеки України в цілому; 2) існуванням таких загроз інформаційній сфері країни, які можуть завдавати значної шкоди загальним національним інтересам; 3) врахуванням того, що за допомогою інформації можна впливати на зміну свідомості і поведінку людей [111]. Отже, інформаційна безпека посідає особливе, системоутворююче місце в структурі національної безпеки України, оскільки інтегрується у всі без винятку сфери.

Отже, на основі проведеного дослідження, пропонуються наступні ознаки інформаційної безпеки: 1) є об'єктивним, цілісним явищем, що обумовлене розвитком інформаційної сфери конкретної держави і суспільства; 2) має складну структуру; 3) є багаторівневою; 4) є складовою національної безпеки, формою її прояву в інформаційній сфері та виконує функцію консолідації всіх інших складових національної безпеки; 5) поєднує в собі статичний та динамічний аспект; 6) існує не ізольовано, а в тісному взаємозв'язку з іншими сферами, що забезпечують суверенітет, територіальну цілісність, стабільність та захищеність держави; 7) регламентована нормативно-правовими актами; 8) має матеріально-технічну, соціально-гуманітарну, правову, політичну, економічну та культурну сторони; 9) в умовах воєнного стану розвивається шляхом впровадження нових стратегій реагування на інформаційні загрози та ін.

Інформаційна безпека – складова національної безпеки України, що включає перманентний процес і результат забезпечення стану захищеності національних інтересів та інших життєво важливих інтересів людини, суспільства і держави в інформаційній сфері України від зовнішніх і внутрішніх, реальних та потенційних загроз.

Як системне і складне явище, інформаційна безпека має складові.

П. Біленчук зауважує, що інформаційна безпека включає в себе сукупність організаційних, соціально-економічних, юридичних заходів, спрямованих на забезпечення сталого розвитку суспільства і держави [128, с. 64]. О. Остапенко та О. Баїк ототожнюють структуру інформаційної безпеки з її адміністративно-правовим регулюванням і виділяють такі елементи: 1) фізичні та юридичні особи, суспільство, держава, які є формальними носіями прав, свобод і законних інтересів у сфері інформаційної безпеки; 2) формально визначені у Конституції України та інших нормативно-правових актах інформаційні права, свободи і законні інтереси громадян; 3) формально позначені типізовані умови (ситуації), що виникають та стають шкідливими і небезпечними у інформаційних відносин та їх забезпечення [129, с. 173]. Б. Кормич зазначає, що інформаційна безпека має суб'єктно-об'єктний склад, відтак з точки зору критерію основного об'єкту система інформаційної безпеки складається з інформаційної безпеки особи, інформаційної безпеки суспільства та інформаційної безпеки держави. Крім того, держава, людина та суспільство одночасно виступають і як суб'єкти інформаційної безпеки, здійснюючи своїми діями захист важливої для них інформації та інформаційних процесів [130, с. 28-32]. О. Малашко та М. Ковалів у структурі інформаційної безпеки виділяють: об'єкт безпеки, загрози цьому об'єкту, забезпечення безпеки об'єкта від прояву загроз [92]. Основним елементом інформаційної безпеки є життєво важливі інтереси соціальної системи, які співвідносяться із зовнішніми чинниками у вигляді інтересів наднаціональних або інших національно-державних структур в рамках міжнародного співтовариства. Зсередини національно-державного утворення його життєво важливі інтереси перебувають у взаємодії з інтересами елементів, які складають дане утворення. В якості останніх виступають соціальні групи, еліта, організації, партії, релігійні та етнічні утворення, рухи тощо [91, с. 24-25]. Особливо велике значення для збереження основ інформаційної безпеки як системи має відносна її самостійність, стійкість структури, причому як на рівні вертикальних зв'язків (система державного управління від президента до місцевих органів влади, включаючи як законодавчу, так і виконавчу гілки), так і на рівні зв'язків горизонтальних (система взаємовідносин між елементами суспільства: соціальними

інститутами, колективами тощо). Без стійких зв'язків, взаємодії компонентів, тобто без структури, інформаційна безпека соціальної системи, очевидно, перестає існувати як конкретне ціле [131]. Отож, в правничій літературі не склалося єдиного бачення щодо структури інформаційної безпеки як об'єктивного явища. Крім того, навіть не всі вчені визнають, що інформаційній безпеці притаманна структура.

Вироблення теорії інформаційної безпеки як складного, структурованого і системного явища є досягненням системного підходу.

Системний підхід в аналізі інформаційної безпеки є своєрідним розвитком комплексного підходу, оскільки при ньому більш глибоко, більш точно відображаються внутрішні і суттєві зв'язки й відношення компонентів суспільної системи, закономірності її функціонування, що є основою створення більш повної теорії об'єкта, що досліджується. Поняття «системність» у деякому смислі ширше, глибше, аніж «комплексність». Воно охоплює зв'язки всередині одного рівня (горизонтальні) і між різними рівнями (вертикальні), в той час як поняття «комплексність» охоплює переважно зв'язки одного або суміжних рівнів ієрархічної структури системи [131]. Емпіричний потенціал системного підходу у дослідженні інформаційної безпеки полягає у здатності всебічно осмислити її складну природу, виявляти внутрішні і зовнішні взаємозв'язки між елементами. Системний підхід дозволяє розглядати інформаційну безпеку не як ізольоване, просте явище, а як систему взаємопов'язаних елементів правової, технічної, організаційної, соціальної природи тощо.

Синергія системного і комплексного підходів до розуміння інформаційної безпеки надає можливість зробити висновок про те, що ця категорія одночасно поєднує динамічний і статичний аспект, а також має власну унікальну структуру.

Отже, ключовими складовими інформаційної безпеки пропонуємо вважати: 1) об'єкти, які оберігаються від загроз; 2) загрози (реальні й потенційні, внутрішні та зовнішні); 3) систему забезпечення інформаційної безпеки, що включає: інформаційну політику та нормативно-правову основу; заходи, методи, принципи забезпечення безпеки об'єктів; суб'єктів, їх права та інтереси, інформаційні

відносини в які вони вступають; процесуально-процедурний компонент діяльності суб'єктів; інформаційні ресурси та технології.

Розвиток систем інформаційної безпеки характеризується єдністю минулого, сучасного й майбутнього. Прогнозування, планування та визначення напрямів і засобів зміцнення інформаційної безпеки у сучасних умовах у зв'язку зі складністю та суперечливістю розвитку міжнародних відносин у світі не можуть здійснюватися без координації та узгодженості. Тільки синхронний розвиток усіх елементів (підсистем) системи інформаційної безпеки забезпечить її найвищу ефективність [131]. Отже, ефективне забезпечення інформаційної безпеки можливе лише за умов комплексного підходу до захисту об'єктів, нейтралізації загроз і узгодженого розвитку всіх елементів системи в контексті динамічних змін в умовах воєнного стану в Україні.

Суб'єкти забезпечення інформаційної безпеки та засоби, якими вони послуговуються потребують комплексного розкриття в окремому підрозділі. Отож, зупинимось на характеристиці об'єктів інформаційної безпеки, розуміння яких є важливим для розкриття цієї категорії загалом.

Об'єктом безпеки є те, що захищається від загроз. Його сутність визначає зміст явища «безпека», певною мірою обумовлюючи можливі загрози, характеристики стану захищеності від загроз. Безпека об'єкта проявляється через безпеку найбільш важливих властивостей або властивостей структурних складових. Загроза безпеки є явища, що існують самостійно, проявляючись через взаємодії об'єкта безпеки з іншими об'єктами, здатне завдати шкоди функціонуванню та властивостями, або подібний прояв взаємодії підсистем і елементів самого об'єкта безпеки [92]. В науковій літературі розділись погляди на те, що слід віднести до об'єктів інформаційної безпеки. Проте, об'єкти інформаційної безпеки загалом визначають її змістовний і ціннісний аспект, оскільки саме на їх недоторканість, стабільність та захищеність спрямоване існування всієї системи.

Частіше до об'єктів інформаційної безпеки відносять людину, суспільство і державу.

Так, до об’єктів національної безпеки відносять: людину і громадянина – їхні конституційні права і свободи та обов’язки; суспільство – його духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності, інформаційне і навколишнє природне середовище і природні ресурси; державу – її конституційний лад, суверенітет, територіальна цілісність і недоторканність [113, с. 43; 112]. Національна безпека є родовим поняттям відносно інформаційної безпеки, отож і їх об’єкти є спільними.

Однак, наявні й інші позиції стосовно об’єкту інформаційної безпеки, що не позбавлені об’єктивності.

В. Лизанчук вважає об’єктом інформаційного впливу окремих осіб, групи осіб, так і цілі держави [132, с. 290]. В. Ліпкан, Ю. Максименко та В. Желіховський зауважують, що юдина та її права, інформація та інформаційні системи та права на них – це основні об’єкти не лише національної безпеки в інформаційній сфері, але й основні елементи всіх об’єктів безпеки в усіх галузях [91, с. 24-25]. Розширює перелік об’єктів О. Довгань та відносить до них: конституційні права і свободи людини і громадянина, фізичне та психологічне здоров’я населення, захищеність людини від деструктивного та маніпулятивного інформаційного впливів; інформаційне забезпечення, гарантії інформаційних прав та права на розвиток населення всіх регіонів України; інформаційний суверенітет, безпека національного сегмента глобального інформаційного простору, інформаційної інфраструктури, захищеність, цілісність, доступність та безпечність інформаційних ресурсів, продукції і послуг [133, с. 13]. В. Фурашев зауважує, що об’єктами інформаційної безпеки є інформація у всіх її проявах, джерела інформації, механізми та засоби її створення, доступу і розповсюдження та наслідки її використання, а також установчі і регуляторні нормативно-правові та адміністративно-організаційні норми і правила, які визначають процеси і процедури формування, використання та припинення дії цих механізмів та засобів, людина, суспільство та держава, а суб’єктами – держава, людина, суспільство. Об’єктом захисту інформації є інформація, а суб`єктами – дії з інформацією на всіх стадіях її «життєвого циклу» (створення, розповсюдження, збереження, знищення, спотворення, фальсифікація та ін.) [134]. Принагідно

зазначимо, що серед об'єктів інформаційної безпеки, що наведені авторами, прослідковуються дві умовні категорії – соціальні та технічні.

Найбільш раціональним видається підхід Т. Мужанової, яка узагальнює та наводить дві групи об'єктів інформаційної безпеки: 1) соціальні: особа – її права та свободи в інформаційній сфері, психіка, в т.ч. свідомість та підсвідоме, особиста інформація; суспільство – його духовні цінності, засади солідарної діяльності; держава – її конституційний лад, суверенітет, ефективне функціонування; 2) технічні: інформаційні ресурси, інформаційно-комунікаційна інфраструктура, в тому числі інформаційно-комунікаційні системи різного масштабу і різного призначення, технології та засоби обробки, зберігання, передавання інформації [121, с. 13]. Погоджуючись із раціональною позицією дослідниці, акцентуємо що в умовах воєнного стану особливої актуальності набуває захист як соціальних, так і технічних об'єктів інформаційної безпеки, оскільки комплексна гібридна агресія рф спрямована не лише на інформаційну дестабілізацію людини, суспільства і держави, але й на враження критичної інформаційно-комунікаційної інфраструктури.

Отже, об'єктами інформаційної безпеки є людина, суспільство та держава, а також інформаційна матеріально-технічна інфраструктура.

Інформаційна безпека – це багаторівневе явище. Рівні інформаційної безпеки відображають організацію захисту інформаційної сфери на конкретних щаблях суспільного життя. Розмежування рівнів інформаційної безпеки дозволяє комплексно оцінювати наявні для них загрози, а також обирати відповідні підходи щодо реагування та захисту. Рівні інформаційної безпеки є похідними від її об'єкту, але це не тотожні категорії

Так, І. Милосердна зауважує, що інформаційна безпека виступає інтегративною складовою національної безпеки та має формуватися на захищеності інтересів особистості, суспільства і держави [73, с. 187] І. Боднар розкриває національну безпеку України в інформаційній сфері розглядати як інтегральну цілісність чотирьох складових – персональної, публічної (суспільної), комерційної (корпоративної) й державної безпеки [135]. Схожий підхід підтримує А. Кузьменко та виокремлює наступні рівні забезпечення інформаційної безпеки: рівень особи (формування

раціонального, критичного мислення на основі принципів свободи вибору); суспільний рівень (формування якісного інформаційно-аналітичного простору, плюралізм, багатоканальність отримання інформації, незалежні потужні ЗМІ, які належать вітчизняним власникам); державний рівень (інформаційно-аналітичне забезпечення діяльності державних органів, інформаційне забезпечення внутрішньої і зовнішньої політики на міждержавному рівні, система захисту інформації з обмеженим доступом, протидія правопорушенням в інформаційній сфері, комп'ютерним злочинам) [136, с. 318]. Важливим рівнем забезпечення інформаційної безпеки є міжнародний.

Коли йдеться про інформаційну безпеку людини – то це насамперед потреби людини, можливість реалізації яких в правовому полі закріплюється через її права і свободи [104, с. 400]. Основні аспекти права людини на інформаційну безпеку охоплюють захист конфіденційності її персональних даних, гарантування безпеки в онлайн-середовищі, боротьбу з кіберзлочинністю, захист від незаконного доступу до інформації та захист інтелектуальної власності, урахування впливу інформації на фізичний і психічний стан людини, а також на її моральні й духовні цінності [137, с. 560]. В умовах воєнного стану Україні доводиться протидіяти численним інформаційно-психологічним операціям рф, спрямованим саме на психологічну стійкість особи та підрив морального духу населення, створення атмосфери паніки тощо.

Інтереси суспільства в інформаційній сфері полягають у забезпеченні інтересів особистості в цій сфері, зміцненні демократії, створенні правової соціальної держави в Україні. Інтереси держави в інформаційній сфері визначаються створенням умов для гармонійного розвитку вітчизняної інформаційної інфраструктури, реалізації конституційних прав і свобод людини і громадянина у сфері отримання інформації й користування нею з метою забезпечення непорушності конституційного ладу, суверенітету і територіальної цілісності держави, політичної, економічної, державно-управлінської та соціальної стабільності, у безумовному забезпеченні законності та правопорядку, розвитку рівноправного і взаємовигідного міжнародного співробітництва [138, с. 258]. Інформаційна безпека передбачає: належний рівень

інформаційної культури; здатність держави створити умови для гармонійного розвитку й задоволення потреб особи в інформації незалежно від наявності інформаційних загроз; гарантування, розвиток і використання інформаційного середовища в інтересах особистості; захищеність від різного роду інформаційних загроз [139, с. 766]. Для її гарантування важливий постійний моніторинг потенційних загроз та вразливостей, а також проведення аудитів для оцінки рівня безпеки.

Сучасні загрози інформаційній безпеці є викликом далеко за межі нашої держави та посягають не лише на національний простір, а й мають важкі глобальні наслідки [140]. Міжнародний рівень інформаційної безпеки зосереджується на забезпеченні стану стабільності і захищеності глобального інформаційного простору.

Забезпечення інформаційної безпеки має здійснюватися одночасно на чотирьох рівнях: 1) рівень особи; 2) рівень суспільства; 3) рівень держави; 4) міжнародний рівень.

Інформаційна безпека є складним, системним, багаторівневим явищем, на стан і перспективи розвитку якого мають безпосередній вплив зовнішні і внутрішні чинники, найважливішими з яких є: 1) політична обстановка у світі; 2) наявність потенційних зовнішніх і внутрішніх загроз; 3) стан і рівень інформаційно-комунікаційного розвитку країни; 4) внутрішньополітична обстановка в державі [141] Науковці виокремлюють різні рівні формування системи інформаційної безпеки України: 1) законодавчий (закони, нормативні акти, стандарти тощо), 2) адміністративний (який запроваджується керівництвом організації), 3) процедурний, 4) програмно-технічний [103]. Саме поєднання правових, інституційних і технічних складових створює основу ефективної системи забезпечення інформаційної безпеки на всіх її рівнях.

Ключова категорія, до якої звертаються дослідники і практики в процесі осмислення та забезпечення інформаційної безпеки в умовах воєнного стану є «загрози інформаційній безпеці».

Слово «загроза» в інформаційній безпеці означає, що будь-хто або будь-що підпадає під небезпеку будь-яких негативних впливів у сфері інформаційної діяльності. Загрози можуть бути внутрішніми, спричиненими суб’єктом

інформаційних відносин через недостатню кваліфікованість, розуміння процесів і наслідків чи злочинним умислом, так і зовнішнім [142, с. 147]. Інформаційна загроза – потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою ускладнення реалізації національних інтересів України. Загрози, як правило, мають комплексний характер, відтак їхні прояви дуже різноманітні [143]. Теоретична конструкція «загроза інформаційній безпеці» в узагальненому вигляді означає наявність або ймовірність деструктивного впливу на інформаційне середовище, яке може завдати шкоди людині, суспільству чи державі.

Загрози інформаційній безпеці досить динамічна і мінлива сукупність негативних явищ, особливо в умовах відсічі повномасштабної російської агресії. Отож, необхідно звернутись до їх наукової систематизації.

Головна інформаційна загроза національній безпеці – це загроза впливу іншої сторони на інформаційну інфраструктуру країни, інформаційні ресурси, на суспільство, свідомість, підсвідомість особистості, з метою нав’язати державі бажану (для іншої сторони) систему цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної й державної діяльності, керувати їхньою поведінкою і розвитком у бажаному для іншої сторони напрямку [111, с. 69]. Саме з боку держави-агресора Україна зазнала найбільш руйнівного, систематичного впливу на інформаційну безпеку, який тривав десятки років до повномасштабного вторгнення та набув комплексного характеру після його початку.

Після початку російської гібридної інтервенції в 2014 р., що призвела до окупації Криму та військових дій на Сході України, відбулось переосмислення сутності та впливу загроз інформаційній безпеці.

В. Пилипчук та О. Дзьобань (2014 р.) віднесли до основних видів загроз інформаційній безпеці: витіснення вітчизняних інформаційних агентств, засобів масової інформації із внутрішнього інформаційного ринку та посилення залежності духовної, економічної і політичної сфер громадського життя України від закордонних інформаційних структур; маніпулювання інформацією; інформаційний вплив іноземних політичних, економічних, військових та інформаційних структур на

розробку і реалізацію зовнішньої політики держави; поширення за кордоном дезінформації про зовнішню політику України; порушення прав громадян і юридичних осіб в інформаційній сфері в Україні й за кордоном; спроби несанкціонованого доступу до інформації і впливу на інформаційні ресурси, інформаційну інфраструктуру органів державної влади, що реалізують державну зовнішню політику, українських представництв і організацій за кордоном, представництв України при міжнародних організаціях [145, с. 47-48]. О. Панченко (2019 р.) до основних джерел зовнішніх ризиків відносить: введення іноземними державами обмежень Україні на поширення інформації і нових інформаційних технологій; розвідувальну діяльність іноземних державних органів і спеціальних служб; протиправну діяльність різних іноземних формувань і окремих особистостей в сфері інтересів України; стихійні катаклізми і катастрофи. А до основних джерел внутрішніх ризиків: відсутність науково обґрунтованої політики інформаційної безпеки держави; недосконаліть законодавчої бази в галузі інформаційних відносин та інформаційної безпеки; недосконаліть державної структури забезпечення інформаційної безпеки; протиправні дії державних органів, політичних і економічних структур, окремих громадян в інформаційній сфері; виникнення позаштатних, непередбачених ситуацій в системах, процесах; недосконаліть або відсутність засобів забезпечення інформаційної безпеки [122]. О. Малашко та М. Ковалів (2020 р.) до загроз інформаційної безпеки віднесли: загрози, пов'язані з розширенням маніпулювання свідомістю людини, інформаційним перевантаженням, з ростом інтернет-залежності і розвитком форм психосоціальної депривації; використання на шкоду персональних даних; розширення масштабів маніпуляції громадською думкою, поява можливостей ефективної організації деструктивних процесів в ціннісних системах суспільства; діяльність мережевих структур вітчизняної та міжнародної злочинності та тероризму; ведення інформаційних війн, неконтрольоване поширення інформаційно-психологічної зброї, її застосування в інформаційних війнах; загрози стабільності існуючих політичних режимів влади: системні та периферійні, обумовлені мережевий логікою соціальних процесів в Інтернеті. Зазначені загрози утворюють певну систему,

яка характеризується соціально- історичними та економічними чинниками [92]. Аналіз наукових підходів свідчить про багатовимірний характер загроз інформаційній безпеці України. Вони включають як зовнішні джерела ризику, так і внутрішні. Акцентується увага на таких загрозах, як маніпуляція свідомістю, деструктивний вплив на цінності суспільства, кібератаки тощо.

На сьогодні, загрози інформаційній безпеці України задекларовані на рівні Стратегії національної безпеки України, затвердженої Указом Президента України від 14 вересня 2020 р. № 392; Стратегії забезпечення державної безпеки, затвердженої Указом Президента України від 16 лютого 2022 р. № 56/2022; Стратегії інформаційної безпеки, затвердженої Указом Президента України від 28 грудня 2021 р. № 685/2021; Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 р. № 447/2021.

Стратегічними документами визначено низку загроз, зокрема: збільшення кількості глобальних дезінформаційних кампаній, інформаційна політика російської федерації, соціальні мережі як суб'єкти впливу в інформаційному просторі, недостатній рівень медіаграмотності (медіакультури) в умовах стрімкого розвитку цифрових технологій, інформаційний вплив російської федерації як держави-агресора на населення України, інформаційне домінування російської федерації як держави-агресора на тимчасово окупованих територіях України, обмежені можливості реагувати на дезінформаційні кампанії, несформованість системи стратегічних комунікацій, недосконаліть регулювання відносин у сфері інформаційної діяльності та захисту професійної діяльності журналістів, спроби маніпуляції свідомістю громадян України щодо європейської та євроатлантичної інтеграції України та ін. [95]. Хоча вказані загрози визначені до повномасштабного вторгнення рф, вони не втрачають актуальності й на сьогоднішній день. Помітним є акцент на внутрішні загрози інформаційній безпеці, що обумовлені слабким розвитком інформаційної політики та інфраструктури. Однак, слід визнати потребу їх переосмислення та конкретизації у розрізі сучасних обставин.

Хоча низка загроз є універсальними і застосовуються протягом тривалого часу, після воєнного вторгнення рф у 2022 р. такі загрози суттєво примножились та масштабувались.

В. Новицький (2022 р.) до переліку таких загроз та викликів відносить: повноформатну експансійну інформаційну політику рф; низький рівень медіаграмотності громадян; динамічне збільшення кількості глобальних дезінформаційних кампаній; інформаційне домінування рф на ТОТ; використання технологій маніпулювання свідомістю пересічних громадян щодо наслідків вступу України в НАТО та ЄС тощо [146, с. 11]. В. Аніщук (2023 р.) зауважує на спеціальних інформаційних операціях рф, більшість із яких спрямовані на підрив національної безпеки України, її національних інтересів, ліквідацію української державності та знищення української ідентичності, провокування проявів екстремізму, панічних настроїв у суспільстві, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації в Україні [109]. І. Милосердна (2024 р.) обґрунтовує такі групи інформаційно-технічних загроз інформаційної безпеки та розвитку держави в цілому: 1) пов’язані з розвитком новітньої інформаційної зброї, здатної впливати як на психіку та свідомість людей, так і на інформаційно-технічну інфраструктуру суспільства. Йдеться про поширення пропаганди та дезінформації, які можуть призводити до маніпуляції даними або їх фальсифікації, що впливає на політичні процеси, сприяє дестабілізації режимів тощо; 2) ті, що стосуються нового класу соціальних злочинів, що базуються на використанні сучасних ІКТ, таких як махінації з електронними коштами та комп’ютерне хуліганство. Особливо актуальним стає питання інформаційної безпеки в контексті зростання транснаціональної кіберзлочинності та кібертероризму; 3) загрози, пов’язані із використанням ІКТ у політичних цілях на національному та міжнародному рівнях, що обумовлено зростанням впливу ЗМІ на процес розроблення, прийняття та реалізацію політичних рішень, функціонування механізму політичної влади та розвитку політичного процесу [73]. Отже, безпека в інформаційній сфері України характеризується значним ускладненням та ескалацією загроз, що набули системного, цілеспрямованого і комплексного характеру.

Просування наративів «руского міра» в Україні відбувалось засобами гібридної війни, системного втручання в інформаційне поле та його розбалансування. Для російської пропаганди національний телерадіопростір з початку війни виявився закритим, натомість телеграм-канали, різні сайти та месенджери стали основними платформами для дезінформації, фейків, втручань та фактично ведення інформаційного тероризму [147, с. 45]. Саме тому, вкрай актуальним є перегляд підходів щодо посилення медіаграмотності населення.

Медіаграмотність в Україні, як і в багатьох інших країнах, є важливим аспектом захисту від інформаційних загроз, особливо ІПСО. Вона передбачає здатність людини аналізувати, критично оцінювати та достовірно розуміти інформацію, яку вона споживає через різні медіа, що ускладнює інформаційний вплив ворога. Особливо важливо розвивати медіаграмотність населення у період поширення дезінформації через мережу «Інтернет», соціальні мережі та інші цифрові платформи.

Стан медіаграмотності в Україні є різним серед різних вікових груп населення та у розрізі регіонів. Українське суспільство має проблеми з медійною концентрацією, через монополізацію інформаційного простору та вплив на об’єктивність і різноманіття інформації. Частина населення має обмежені навички щодо роботи з цифровими технологіями та розумінням медійних реалій.

Україна активно працює над підвищенням рівня медіаграмотності в суспільстві через різноманітні заходи, проте це є тривалим процесом, що в умовах воєнного стану утворює проблему. Вкрай актуальними є проєкти, які спрямовані на підвищення медіаграмотності, такі як факт-чекінгові сайти, тренінги для журналістів та громадян. Крім того, Україна співпрацює з міжнародними організаціями та іншими країнами для обміну досвідом та найкращими практиками з медіаграмотності.

Отже, підсумовуючи, пропонуємо вважати загрозами інформаційній безпеці в умовах воєнного стану наступне:

1) внутрішні загрози: низький рівень медіаграмотності та інформаційної компетентності населення; недосконалість нормативно-правового та організаційного забезпечення інформаційної безпеки; низька ефективність державної інформаційної політики; низький рівень захищеності критичної інформаційної інфраструктури;

правопорушення посадових осіб у інформаційній сфері; неефективність державного реагування на маніпулювання інформацією та суспільною думкою; слабка захищеність кіберпростору; слабка захищеність персональних даних громадян; брак цілеспрямованого інформування міжнародної спільноти про російську агресію в Україні;

2) зовнішні загрози: комплексна інформаційна агресія рф проти України (інформаційно-психологічні операції, маніпулювання суспільною думкою, дезінформаційні кампанії, системна пропаганда та поширення фейків, інформаційне домінування рф на ТОТ та ін.); інформаційний вплив держав-партнерів рф на Україну та міжнародне співтовариство; розвідувальна діяльність іноземних спецслужб; втручання у внутрішньополітичні процеси через інформаційно-комунікаційні технології; кібератаки, загрози кіберзлочинності та кібертероризму; дезінформація міжнародної спільноти про російську агресію в Україні; розробка та поширення нової інформаційно-психологічної зброї; неконтрольовані інформаційні деструктивні процеси в глобальній мережі «Інтернет».

Принагідно зауважимо, що такий перелік не претендує на вичерпність, а інформаційні загрози в цілому заслуговують окремих комплексних наукових досліджень, особливо в умовах воєнного стану.

З метою попередження і протидії існуючим та ймовірним загрозам інформаційній безпеці стратегічне завдання держави полягає у створенні та функціонуванні механізму забезпечення інформаційної безпеки. Він передбачає послідовну системну діяльність, сукупність заходів і державно-правових інституцій, що покликані гарантувати безперешкодну реалізацію національних інтересів держави в інформаційній сфері, відповідних інтересів людини і суспільства, попередження інформаційних конфліктів та оперативне їх подолання [148, с. 41]. У воєнний час захист інформаційної безпеки держави є пріоритетним оскільки безпосередньо від нього залежить безпека суспільства і людини. У час війни публічно-правовий захист виходить за межі традиційного регулювання і поглинає приватно-правові відносини [142, с. 149]. В умовах воєнного стану вкрай важливо посилювати організаційні заходи забезпечення інформаційної безпеки, ефективно протидіяти кіберзагрозам.

Впровадження новітніх заходів забезпечення інформаційної безпеки України під час воєнного стану має відбуватися в межах правового поля, отож важливими є дослідження проблем та перспектив їх правового забезпечення [149].

На основі проведеного дослідження пропонуються наступні висновки та узагальнення:

1. Інформаційна безпека – складова національної безпеки України, що включає перманентний процес і результат забезпечення стану захищеності національних інтересів та інших життєво важливих інтересів людини, суспільства і держави в інформаційній сфері України від зовнішніх і внутрішніх, реальних та потенційних загроз. Їй характерні наступні ознаки: 1) є об'єктивним, цілісним явищем, що обумовлене розвитком інформаційної сфери конкретної держави і суспільства; 2) має складну структуру; 3) є багаторівневою; 4) є складовою національної безпеки, формою її прояву в інформаційній сфері та виконує функцію консолідації всіх інших складових національної безпеки; 5) поєднує в собі статичний та динамічний аспект; 6) існує не ізольовано, а в тісному взаємозв'язку з іншими сферами, що забезпечують суверенітет, територіальну цілісність, стабільність та захищеність держави; 7) регламентована нормативно-правовими актами; 8) має матеріально-технічну, соціально-гуманітарну, правову, політичну, економічну та культурну сторони; 9) в умовах воєнного стану розвивається шляхом впровадження нових стратегій реагування на інформаційні загрози та ін.

2. Ключовими складовими інформаційної безпеки пропонуємо вважати: 1) об'єкти, які оберігаються від загроз; 2) загрози (реальні й потенційні, внутрішні та зовнішні); 3) систему забезпечення інформаційної безпеки, що включає: інформаційну політику та нормативно-правову основу; заходи, методи, принципи забезпечення безпеки об'єктів; суб'єктів, їх права та інтереси, інформаційні відносини, в які вони вступають; процесуально-процедурний компонент діяльності суб'єктів; інформаційні ресурси та технології. Об'єктами інформаційної безпеки є людини, суспільство та держава, а також інформаційна матеріально-технічна інфраструктура. Забезпечення інформаційної безпеки здійснюватися одночасно на

чотирьох рівнях: 1) рівень особи; 2) рівень суспільства; 3) рівень держави; 4) міжнародний рівень.

3. «Загроза інформаційній безпеці» в узагальненому вигляді означає наявність або ймовірність деструктивного впливу на інформаційне середовище, що може завдати шкоди людині, суспільству чи державі.

Загрозами інформаційній безпеці в умовах воєнного стану є наступні: *1) внутрішні загрози*: низький рівень медіаграмотності та інформаційної компетентності населення; недосконаліть нормативно-правового та організаційного забезпечення інформаційної безпеки; низька ефективність державної інформаційної політики; низький рівень захищеності критичної інформаційної інфраструктури; правопорушення посадових осіб у інформаційній сфері; неефективність державного реагування на маніпулювання інформацією та суспільною думкою; слабка захищеність кіберпростору; слабка захищеність персональних даних громадян; брак цілеспрямованого інформування міжнародної спільноти про російську агресію в Україні. *2) зовнішні загрози:* комплексна інформаційна агресія рф проти України (інформаційно-психологічні операції, маніпулювання суспільною думкою, дезінформаційні кампанії, системна пропаганда та поширення фейків, інформаційне домінування рф на ТОТ та ін.); інформаційний вплив держав-партнерів рф на Україну та міжнародне співтовариство; розвідувальна діяльність іноземних спецслужб; втручання у внутрішньополітичні процеси через інформаційно-комунікаційні технології; кібератаки, загрози кіберзлочинності та кібертероризму; дезінформація міжнародної спільноти про російську агресію в Україні; розробка та поширення нової інформаційно-психологічної зброї; неконтрольовані інформаційні деструктивні процеси в глобальній мережі «Інтернет».

1.4. Зарубіжний досвід забезпечення інформаційної безпеки в умовах воєнного конфлікту

Проблематика інформаційної безпеки в умовах воєнного конфлікту сформувалася як наслідок розвитку теорії міжнародних відносин, права національної безпеки, інформаційного права та інших галузей. Її концептуалізація відбувалася завдяки розумінню складних процесів інформації в системі військової діяльності. Сьогоднішнє визнання інформаційної безпеки як самостійної сфери відносин та протиборства між відповідними суб'єктами потребує розробки спеціальних правових та інституційних механізмів.

У західній науці значний вплив на формування сучасних уявлень про інформаційну безпеку справили праці представників так званої копенгагенської школи безпекових досліджень. Книга, видана у 1997 р. за авторством Б. Б'юзана, О. Вевера та Я. де Уайльда «Безпека: нова основа аналізу» [150], що вважається провідним текстом, де викладаються погляди цієї школи, розвиває концепцію сек'юритизації і мультисекторного підходу до безпеки. Подальший розвиток цієї теми пов'язаний із роботами Т. Ріда та М. Лібіцкі, які зосередили увагу на трансформації війни в умовах цифровізації. Так, Т. Рід, аналізуючи феномен «кібервійни», скептично оцінює можливість ототожнення класичних воєнних дій із кібератаками, однак водночас визнає їхню здатність завдавати стратегічної шкоди критичній інфраструктурі та системам управління [31]. М. Лібіцкі пропонує більш диференційований підхід, розмежовуючи інформаційну війну, кібероперації, психологічні операції та операції впливу, що дозволяє точніше визначати об'єкти правового регулювання та межі відповідальності держав у цій сфері [151].

Вагомий внесок у розуміння інформації в конфліктах зробив Дж. Най, який, розвиваючи концепцію «м'якої сили», підкреслив роль інформаційних наративів і символів у досягненні стратегічних цілей без прямого застосування збройного насильства [152]. У цьому сенсі інформаційна безпека тісно пов'язується із захистом інформаційного суверенітету, довіри до державних інституцій та стійкості суспільства до зовнішнього впливу.

Дослідження сучасного часу мають явний вираз реакції на російську агресію. Зарубіжні автори все частіше звертають увагу на модернізацію засад забезпечення інформаційної безпеки в умовах воєнного конфлікту. Так, у своїй статті Б. Ван Нікерк визначає структуру ролей кібероперацій на різних етапах військового конфлікту, засновану на сучасних поглядах на корисність кібероперацій, а також на практичних прикладах [153]. Т. Лібетрау аналізує практику трьох європейських членів НАТО – Нідерландів, Франції та Норвегії, розширюючи існуючий фокус дослідження кіберконфлікту, що пов'язаний з війною, за межі його домінуючого контексту в США. Автор порівнює та оцінює як ці країни сприймають та реагують на зміну стратегічного середовища, що характеризується зростанням кіберконфлікту, що пов'язаний з війною [154].

Дж. Руохонен, К. Ріндделл та С. Бусетті досліджують проблемні аспекти управління інцидентами в кібербезпеці на рівні Європейського Союзу. Автори розглядають зв'язок між інцидентами та кризами в кібербезпеці, а також те, як підготовка до можливих кіберінцендентів відображена в нових законах ЄС про кібербезпеку [155]. З. Гулієв робить внесок у розуміння динаміки інформаційної війни та пропонує методи для майбутніх досліджень впливу соціальних мереж у військових конфліктах [156]. Робота І. Фищук, М. Ноесгаарда та Дж. Нільсена пропонує нове розуміння викликів управління кібератаками в екстремальних ситуаціях. Автори опановують практичні знання про кібератаки та зусилля з кібербезпеки у надзвичайних умовах [157]. Актуальні проблеми становлення нової геополітики кібербезпеки ЄС обговорюють у своєму дослідженні Х. Каррапіко та Б. Фарранд [158]. Отже, при дослідженні забезпечення інформаційної безпеки в умовах воєнного конфлікту зарубіжними авторами інформаційна сфера розглядається як самостійний сектор безпеки, а питання кібербезпеки на сьогодні становить підвищену актуальність.

Представники української науки в силу об'єктивних причин аналізують проблематику забезпечення інформаційної безпеки більш комплексно. Так, у працях О. Радутного інформаційна безпека розглядається як складова національної безпеки, що охоплює не лише технічний захист інформаційних систем, а й кримінально-

правову охорону інформаційних відносин від деструктивного впливу [159-161]. В. Ліпкан акцентує увагу на системному характері інформаційної безпеки, визначаючи її як стан захищеності життєво важливих інтересів особи, суспільства і держави в інформаційній сфері, що досягається сукупністю правових, організаційних, технічних та ідеологічних заходів [162; 373].

Після 2022 р. в українській науці з'являється низка публікацій, де інформаційна безпека постає об'єктом захисту в умовах воєнного конфлікту. Авторами розглядаються такі питання як розробка ефективних стратегій інформаційної безпеки на тлі сучасних збройних конфліктів [163]; вплив мас-медіа на формування суспільної думки та нові підходи до основ інформаційної боротьби [164]; удосконалення організації кібероперацій у військовому контексті шляхом використання основних принципів управління [165]; запровадження комплексної системи аналітики кібербезпеки в режимі реального часу для захисту критично важливої інфраструктури [166]; основні особливості інформаційної війни та їх вплив на кібербезпеку в усьому світі та в межах конкретних організацій та держав [167] тощо. Розгорнутий і точний аналіз аспектів інформаційної безпеки здійснює О. Пархоменко-Куцевіл [168]. Ці та інші роботи можна вважати сучасним поглядом на проблему забезпечення інформаційної безпеки в умовах воєнного конфлікту.

Доцільним і корисним є звернення дослідників до зарубіжного досвіду забезпечення інформаційної безпеки. Так, правові аспекти у регулюванні забезпечення інформаційної безпеки вивчає Н. Грабар 169] та К. Ковальов [170]; В. Шемчук здійснює порівняльно-правовий аналіз забезпечення інформаційної безпеки сучасних держав [171], а А. Войціховський досліджує зарубіжний досвід організації забезпечення інформаційної безпеки [112]. Ряд авторів звужують свій пошук до аналізу конкретних країн щодо забезпечення інформаційної безпеки, звертаючись, зокрема, до досвіду США [172], Німеччини [173], Франції [174], Європейського Союзу [175-176].

Корисними є роботи тих авторів, які пропонують механізми імплементації зарубіжного досвіду в Україні за сучасних обставин зовнішньої агресії. Так, Я. Ізмайлов і І. Єгорова вивчають можливість адаптації досвіду ЄС у сфері

інформаційної безпеки до умов України [177], О. Пугачов [178] та І. Недохлєбов [176] обґрунтовують тезу про необхідність застосування кращого зарубіжного досвіду в цій сфері. Отже, опанування згаданих та інших робіт засвідчує наявність певних результатів, що, однак, не виключає необхідність подальшого аналізу малодосліджених аспектів забезпечення інформаційної безпеки за сучасних умов воєнного конфлікту.

Аналізуючи праці зарубіжних та українських авторів, які досліджують окремі питання забезпечення інформаційної безпеки, можна констатувати відсутність уніфікованого визначення цього поняття, що є наслідком багатомірності самого явища. У правовій науці поступово формується розуміння інформаційної безпеки як комплексної правової та соціальної категорії, яка виходить за межі суто кібернетичного або технологічного підходу. Звернемо увагу на співвідношення таких суміжних понять як інформаційна безпека, кібербезпека, інформаційна та гібридна війни.

Кібербезпека є функціонально вужчим поняттям і стосується насамперед захисту інформаційно-телекомунікаційних систем, мереж і даних від несанкціонованого втручання. Інформаційна війна, на відміну від інформаційної безпеки, описує не стан захищеності, а форму конфліктної взаємодії, що включає цілеспрямоване використання інформації для дезорганізації управління, деморалізації населення та впливу на процеси прийняття рішень. Гібридна війна є більш широким явищем, у межах якого інформаційні та кібероперації поєднуються з військовими, економічними, дипломатичними та іншими засобами впливу. *Інформаційна безпека в умовах воєнного конфлікту* має найбільш широкий зміст і охоплює весь спектр суспільних відносин, пов’язаних зі створенням, обігом, використанням і захистом інформації.

Вважаємо, що інформаційна безпека в умовах воєнного конфлікту має розглядатися не лише як складова національної безпеки, а як самостійний багатовимірний феномен, що поєднує правові, інституційні, технологічні та комунікативні елементи. Ми виходимо з тих аргументів, що у зарубіжній і національній науці простежується відхід від вузького технократичного розуміння

інформаційної безпеки як захисту інформаційних систем, натомість утверджується позиція, відповідно до якої ключовим об'єктом захисту стає «національний інформаційний простір» [176, с. 19; 382], включно з процесами формування суспільної свідомості, прийняття політичних рішень та створенням правових засобів впливу. Зокрема, представник копенгагенської школи безпекових досліджень Б. Б'юзан, розвиваючи концепцію сек'юритизації, обґрунтував тезу про можливість віднесення інформаційної сфери до самостійного сектору безпеки поряд із військовим, політичним, економічним та соціальним [179]. У цьому контексті інформаційна безпека постає не лише як технічна або комунікаційна проблема, а як результат політико-правового процесу, у межах якого певні інформаційні загрози визнаються екзистенційними для держави чи суспільства та виправдовують застосування надзвичайних заходів [179].

Широке тлумачення інформаційної безпеки простежується при спробі нормативізувати відносини в цій сфері. Наприклад, НАТО визначає інформаційне протиборство як елемент багатовимірних операцій, що поєднують військові, кібернетичні та когнітивні складові. Так, документ, схвалений міністрами оборони країн-членів Альянсу, окреслює сучасне бачення інформаційного простору як домену для протидії інформаційним загрозам і підкреслює інтегровану оцінку, запобігання, стримування та протидію інформаційним операціям [180]. Стратегічні концепції НАТО виходять з того, що інформаційна сфера є повноцінним операційним простором поряд із суходолом, морем, повітрям і кіберпростором. У цьому контексті захист інформаційної безпеки розглядається як система превентивних дій і заходів впливу, спрямованих на забезпечення стійкості суспільств до зовнішнього інформаційного впливу.

Право Європейського Союзу формує більш детальну і нормативно орієнтовану модель інформаційної безпеки. Документи ЄС у сфері безпеки акцентують увагу на захисті демократичних процесів, свободи вираження поглядів і цілісності інформаційної системи навіть в умовах надзвичайних та воєнних режимів. Наприклад, Стратегічний компас для безпеки та оборони ЄС, документ Європейської Ради, встановлює спільне бачення та ключові пріоритети ЄС у сфері безпеки, серед

яких посилення стійкості до гібридних загроз, включно з інформаційними атаками, дезінформацією та зовнішнім впливом [181; 384]. При цьому інформаційна безпека трактується як баланс між необхідністю протидії дезінформації та збереженням фундаментальних прав людини. Саме цей баланс залишається предметом дискусій, оскільки межі допустимого втручання держави в інформаційну сферу в умовах війни не мають універсального вирішення.

Підходи Організації Об'єднаних Націй до тлумачення інформаційної безпеки традиційно вирізняються прагненням до універсалізації стандартів її забезпечення. У резолюціях Генеральної Асамблеї та звітах спеціалізованих груп експертів інформаційна безпека розглядається крізь призму захисту прав людини. Наприклад, в резолюції ГА ООН A/RES/79/93 містяться положення щодо сприяння співробітництву у сфері інформаційних потоків та зниження інформаційних нерівностей для забезпечення інформаційної безпеки та захисту прав людини в умовах конфліктів [182]. Наголошується, що навіть у період воєнного конфлікту інформаційні операції не повинні призводити до масових порушень прав цивільного населення, зокрема через поширення паніки, мови ненависті або підрив довіри до гуманітарних інститутів.

Аналіз досліджень інформаційної безпеки в умовах війни виявляє акцент на гібридному характері сучасних конфліктів, у яких інформаційні впливи виконують не допоміжну, а визначальну роль. При цьому інформаційна безпека держави не може зводитися виключно до протидії зовнішнім загрозам. Слід приймати до уваги, у тому числі як об'єкт наукового дослідження, внутрішні інформаційні вразливості, такі, наприклад, як низький рівень медіаграмотності у населення, фрагментованість інформаційного простору, недовіра до інституцій та інші фактори, що істотно посилюють ефективність ворожих операцій.

Узагальнюючи дослідницькі праці у сфері забезпечення інформаційної безпеки [176, с. 3], доцільно виокремити ключові загрози, які набувають системного характеру в умовах воєнного конфлікту (табл.). Їх аналіз дозволяє перейти від абстрактних концепцій до вироблення належних механізмів правового регулювання та формування засад державної політики в цій сфері.

Таблиця

Ключові загрози інформаційній безпеці в умовах воєнного конфлікту

Вид загрози	Характеристика	Потенційні правові наслідки
Дезінформація	Систематичне поширення завідомо неправдивої або маніпулятивної інформації з метою впливу на громадську думку	Обмеження свободи слова, спеціальні режими регулювання медіа
Психологічні операції	Цілеспрямований вплив на емоційний та когнітивний стан населення і військових	Необхідність правового регулювання стратегічних комунікацій
Кібератаки	Втручання в роботу інформаційних систем та критичної інфраструктури	Запровадження режимів кіберзахисту та кібероборони
Втручання в інформаційну інфраструктуру	Порушення функціонування засобів зв'язку, мовлення, цифрових платформ	Тимчасові обмеження доступу та спеціальні повноваження держави

Джерело: сформовано автором

Концептуалізація інформаційної безпеки в умовах воєнного конфлікту не може бути повною в межах виключно юридичного аналізу. Наприклад, Б. Ван Нікерк, переосмислюючи моделі кіберзброї як елементу інформаційної безпеки, звертає увагу на необхідності застосування міждисциплінарного підходу у дослідженні цієї теми, що враховує технічні, правові, соціальні та міжнародно-безпекові аспекти [153]. Сучасна наука виходить із того, що інформаційна безпека є за своєю природою *міждисциплінарною категорією*, яка формується на перетині права, політології, соціології, психології, теорії комунікацій, кібернетики та військових наук. Це зумовлено самою сутністю інформаційного протиборства, яке спрямоване не лише на порушення правових режимів або функціонування інформаційних систем, а, насамперед, на трансформацію моделей поведінки, сприйняття та колективних уявлень. Цікаво простежити роль юридичної науки в універсальному розвитку досліджень проблем забезпечення інформаційної безпеки в умовах воєнного конфлікту.

З позицій політичної науки інформаційна безпека в умовах війни розглядається як елемент боротьби за легітимність влади та контроль над публічним простором. У цьому контексті інформаційні операції аналізуються як інструменти впливу на політичні рішення, міжнародну підтримку та внутрішню стабільність держави. Психологічні та соціологічні дослідження, у свою чергу, акцентують увагу на вразливості індивідуальної та масової свідомості в умовах, що визначають

ефективність дезінформації, психологічних операцій та маніпулятивних комунікацій. Для юридичної науки це має значення, оскільки дозволяє пояснити, чому традиційні механізми правового регулювання виявляються недостатніми без урахування політичної логіки конфлікту та реального соціального ефекту, який може мати довготривалий характер.

Окремий міждисциплінарний характер у дослідженні питань забезпечення інформаційної безпеки в умовах воєнного конфлікту формують кібернетика та інформаційні технології, без яких неможливе розуміння сучасних загроз інформаційній безпеці. Кібератаки, втручання в алгоритми поширення інформації, використання штучного інтелекту для створення маніпулятивного контенту істотно ускладнюють традиційні юридичні конструкції відповідальності, юрисдикції та доказування. У військовій науці інформаційна безпека розглядається як складова інформаційних і когнітивних операцій, що інтегруються у загальну систему оборони держави. Для юридичної науки це означає потребу адаптації правових категорій до технічної реальності цифрового середовища, а також осмислення співвідношення норм міжнародного гуманітарного права, національного безпекового законодавства та спеціальних режимів правового регулювання, які застосовуються в умовах воєнного стану.

В умовах воєнного конфлікту інформаційна безпека набуває якісно нового значення, виходячи за межі суто технічного або комунікаційного процесу та трансформуючись у самостійний об’єкт правового регулювання, тісно пов’язаний із національною безпекою, обороною та захистом конституційного ладу. Зарубіжний досвід свідчить, що ефективність протидії інформаційним загрозам значною мірою визначається наявністю спеціальних нормативно-правових механізмів, які активуються в умовах надзвичайного або воєнного стану та допускають тимчасове відхилення від загальних стандартів правового регулювання.

Так, у Сполучених Штатах Америки нормативна модель забезпечення інформаційної безпеки в кризових умовах має фрагментарний, але функціонально узгоджений характер. Закон США «Про об’єднання та зміцнення Америки шляхом надання належних інструментів, необхідних для перехоплення та запобігання

тероризму» (USA PATRIOT Act), у разі загроз національній безпеці, передбачає розширення повноважень державних органів щодо доступу до інформації та моніторингу інформаційного простору [183]. Актом визначаються повноваження щодо перехоплення та розкриття електронних комунікацій, включно з розширеним доступом до електронних записів та правоохоронними інструментами моніторингу цифрових комунікацій для протидії тероризму (частини 201–215 розділу II) [183]. Ці нормативні положення надають федеральним агентствам право перехоплювати, отримувати і обмінюватися електронними даними, що є важливими для запобігання і розслідування терористичної діяльності.

Окрім цього, для активації механізмів захисту національної безпеки при надзвичайних ситуаціях застосовуються положення Закону США «Про національні надзвичайні стани» [184], що дозволяють Президенту запроваджувати спеціальні режими управління інформаційними ресурсами та критичною інфраструктурою. Закон дає Президенту США право оголосити національний надзвичайний стан і активувати спеціальні повноваження, передбачені іншими федеральними законами, у тому числі щодо управління критичною інфраструктурою та інформаційними системами під час кризових ситуацій (§ 1621) [184]. При цьому американська модель зберігає акцент на судовому контролі як інструменті стримування надмірного втручання держави в приватне життя.

Правова система Великої Британії характеризується більш централізованим підходом. Закон «Про цивільні надзвичайні ситуації» 2004 р. передбачає можливість ухвалення надзвичайних регуляторних актів (ст. 22), зокрема щодо обмеження поширення інформації, яка може завдати шкоди обороні або громадському порядку [185]. В умовах надзвичайної ситуації уряд може запроваджувати тимчасові положення, що містять регуляції будь-якого характеру, які здаються необхідними для попередження, контролю чи пом’якшення наслідків надзвичайної ситуації, включно з обмеженням доступу до певної інформації чи встановленням особливих вимог щодо інформаційних ресурсів.

Інший нормативний документ, Закон Великої Британії «Про повноваження у сфері розслідувальної діяльності» 2016 р., створює правову основу для розширеного

державного нагляду за цифровими комунікаціями, що в умовах війни використовується як елемент протидії дезінформації та іноземному впливу [186]. Так, частини 3–5 закону передбачають положення про право та процедуру перехоплення комунікацій і отримання даних про комунікації [186]. Таким чином, законодавчо створюється єдиний правовий режим для перехоплення електронних повідомлень, доступу до даних про комунікації та втручання в обладнання з обов'язковим судовим контролем для розширених повноважень у сфері національної безпеки і кримінального розслідування

Ізраїль демонструє одну з найбільш жорстких і водночас інституційно врівноважених моделей правого регулювання відносин у сфері захисту інформаційної безпеки. Так, Регуляції з питань оборони (надзвичайного стану), прийняті ще у 1945 р., дозволяють державі здійснювати попередню цензуру військової інформації, обмежувати роботу ЗМІ та контролювати інформаційні потоки [187]. Ці нормативні положення дають виконавчій владі повноваження обмежувати свободу публікацій, забороняти випуск та розповсюдження матеріалів, які можуть завдати шкоди безпеці, включно з вимогою передавати матеріали на попередню перевірку військовою цензурою.

Основна роль у попередженні і реагуванні на надзвичайні ситуації в Ізраїлі відведено уряду. Так, ст. 50 розділу 3.2 Регуляцій визначено, що під час оголошеного надзвичайного стану уряд має право видавати «регуляції надзвичайного стану» для захисту держави та безпеки [187]. Такого типу регуляції тимчасово змінюють або призупиняють чинні закони за умов, що це необхідно для захисту держави, безпеки або життєво важливих послуг, але таке втручання повинно відповідати межам надзвичайного стану. Водночас ці механізми функціонують у поєднанні з активною роллю Верховного суду Ізраїлю, що формує практику пропорційності втручання у свободу вираження поглядів.

У Франції правове регулювання інформаційної безпеки в умовах надзвичайних ситуацій ґрунтується на положеннях Кодексу внутрішньої безпеки та режимі надзвичайного стану, унормованому, зокрема, Законом № 55-385 від 3 квітня 1955 р. «Про надзвичайний стан» [188]. У період дії надзвичайного стану держава отримує

додаткові повноваження щодо блокування онлайн-контенту, який становить загрозу національній безпеці, що активно застосовується у сфері боротьби з інформаційними операціями іноземного походження. Так, ст. 3 Закону «Про надзвичайний стан» та інші положення щодо режиму надзвичайного стану надають Президенту додаткові повноваження для забезпечення безпеки та громадського порядку [188]. За режиму надзвичайного стану державні органи можуть встановлювати обмеження на свободу пересування, збирати інформацію, контролювати доступ до певних медіа чи контенту, якщо це необхідно для захисту національної безпеки та громадського порядку.

Німеччина, з огляду на історичний досвід, обрала більш стриману модель правового регулювання відносин у сфері захисту інформаційної безпеки. Основний закон ФРН передбачає спеціальні положення про стан оборони (Verteidigungsfall), зокрема у ст.ст. 115a–115l [189]. Під час оголошення стану оборони федеральний уряд отримує спеціальні повноваження щодо захисту держави, а обмеження інформаційних прав мають ґрунтуватися на чітких правових підставах з врахуванням конституційних гарантій прав людини. Прямі обмеження інформаційних прав сформульовані у німецькому законодавстві обережно і дещо загально, але нормативні акти про захист конституції та кібербезпеку дозволяють розширене втручання у разі загроз інформаційній інфраструктурі.

Окремої уваги заслуговує досвід держав Балтії, насамперед Естонії та Литви. Так, в Естонії закони «Про надзвичайні ситуації» [190] та «Про кібербезпеку» [191] створюють правову основу для централізованого управління інформаційними системами в кризових умовах. Наприклад § 1 та § 12 Закону Естонії «Про кібербезпеку» передбачають загальні вимоги стосовно забезпечення кібербезпеки та механізми запобігання і реагування на кіберінциденти [191]. Зокрема, законодавчо встановлюються обов’язки державних органів та приватних операторів щодо забезпечення кібербезпеки, включаючи моніторинг загроз, аналіз ризиків та обмін інформацією про кібератаки для захисту важливих інформаційних систем.

В Литві у законі «Про надзвичайний стан» прямо передбачається можливість тимчасового обмеження діяльності ЗМІ та онлайн-платформ з метою протидії

інформаційним загрозам [192]. Цей закон дозволяє тимчасово обмежувати діяльність засобів масової інформації та онлайн-ресурсів у разі, коли це необхідно для протидії інформаційним загрозам, що можуть підірвати національну безпеку або загальний порядок.

Порівняльний аналіз забезпечення інформаційної безпеки в умовах воєнного конфлікту в США, Ізраїлі та згаданих країнах-членах ЄС засвідчує, що ключовим елементом забезпечення інформаційної безпеки в умовах війни є *спеціальні правові режими.* Спеціальним правовим режимом прийнято називати воєнний або надзвичайний стан. Їх спільною рисою є тимчасове розширення дискреційних повноважень виконавчої влади у сфері контролю за інформаційним простором. Відмінності між національними моделями правового регулювання суспільних відносин при спеціальних правових режимах полягають у ступені формалізації таких повноважень, наявності судового або парламентського контролю та рівні деталізації допустимих обмежень.

Дискусійним залишається питання меж допустимого втручання у свободу вираження поглядів при запровадженні спеціальних правових режимів. Чи потрібно у таких випадках більше звертати увагу на обґрунтування пріоритету безпеки в умовах екзистенційної загрози, або ж наполягати на збереженні ядра фундаментальних прав навіть у період війни? Зарубіжна практика свідчить про поступове формування компромісної моделі, за якої інформаційні обмеження визнаються легітимними лише за умови їх тимчасовості, пропорційності та підконтрольності. Вважаємо, що саме на таку модель слід орієнтуватися при формування в Україні механізмів забезпечення інформаційної безпеки в умовах воєнного конфлікту.

Дійсно, в умовах воєнного конфлікту при забезпеченні інформаційної безпеки можуть змінюватися підходи до правового регулювання інформаційної сфери. Однак держава має не тільки реагувати на загрози, а й у своїх діях залишатися у межах конституційних та міжнародно-правових зобов’язань у сфері прав людини. Саме тому порівняльно-правовий аналіз нормативних механізмів різних держав дозволяє

виявити усталені моделі правового балансу між інтересами національної безпеки та свободою вираження поглядів.

У більшості демократичних держав свобода вираження поглядів визнається фундаментальною цінністю, однак не має абсолютного характеру. Зазвичай, конституції допускають можливість її обмеження з метою захисту важливих державницьких засад, особливо в умовах надзвичайного або воєнного стану. Незважаючи на надзвичайні обставини та наявність загроз, такі обмеження підлягають суворій перевірці на відповідність принципам законності, легітимної мети та необхідності в демократичному суспільстві.

Європейський суд з прав людини застосовує послідовний підхід до оцінки допустимості втручання держави в інформаційну сферу навіть за умов воєнного конфлікту чи загроз національній безпеці. Так, у справі «Гендісайд проти Сполученого Королівства» Суд сформулював базовий підхід, відповідно до якого свобода вираження охоплює не лише інформацію або ідеї, що сприймаються прихильно, але й ті положення, що можуть ображати, шокувати чи турбувати державу або частину суспільства [193]. Цей підхід не втрачає актуальності й у контексті воєнного часу.

Разом із тим, у справах, що безпосередньо стосуються питань безпеки, Суд визнає за державами певний «простір розсуду». Показовою є справа «Леандер проти Швеції», у якій ЄСПЛ погодився з тим, що захист національної безпеки може виправдовувати обмежений доступ до інформації, якщо відповідні заходи мають достатні гарантії від зловживань [194]. Аналогічний підхід простежується й у справі «Сенер проти Туреччини», де Суд наголосив, що обмеження свободи слова, навіть у контексті боротьби з тероризмом, не повинні виходити за межі необхідного [195].

Забезпечення інформаційної безпеки в умовах воєнного конфлікту та захист основних прав людини правовими засобами є важливим перетином у законодавчому регулювання цих сфер. У зв’язку із цим, ми можемо виділити *особливості правового регулювання відносин щодо забезпечення інформаційної безпеки в умовах воєнного конфлікту* відповідно до практики США, Ізраїлю та деяких європейських країн, які

входять до ЄС, з метою вивчення можливості застосування цього досвіду в Україні (табл.).

Таблиця

Особливості нормативно-правового регулювання забезпечення інформаційної безпеки в умовах воєнного конфлікту

Держава	Ключові нормативно-правові акти	Основні механізми регулювання	Модель балансу між безпекою та правами людини
США	USA PATRIOT Act; National Defense Authorization Act; Cybersecurity Information Sharing Act	Розширені повноваження спецслужб; контроль інформаційних потоків; кіберзахист критичної інфраструктури	Змішана модель із судовим контролем та парламентським наглядом
Велика Британія	Civil Contingencies Act 2004; Official Secrets Act; Online Safety Act 2023	Тимчасові обмеження свободи слова; протидія дезінформації; регулювання цифрових платформ	Пропорційна модель з акцентом на права людини
Ізраїль	Emergency Regulations; Defence Regulations; Military Censorship Orders	Військова цензура; попередній контроль публікацій; захист військової таємниці	Пріоритетно-безпекова модель
Франція	Code de la sécurité intérieure; Loi sur l'état d'urgence; Loi contre la manipulation de l'information	Адміністративні обмеження медіа; блокування шкідливого контенту; судовий контроль	Пропорційна модель у межах стандартів ЄСПЛ
Німеччина	Grundgesetz; Gesetz über das Bundesamt für Sicherheit in der Informationstechnik	Захист конституційного ладу; кібербезпека; обмеження з жорсткими правовими гарантіями	Модель суворої пропорційності
Литва, Латвія, Естонія	National Security Acts; Media Laws; Emergency Powers Regulations	Протидія інформаційним операціям; обмеження трансляції ворожих медіа	Превентивна безпекова модель з європейськими гарантіями

Джерело: сформовано автором

Порівняльний аналіз правового регулювання зарубіжними країнами забезпечення інформаційної безпеки в умовах воєнного конфлікту дозволяє виокремити щонайменше кілька моделей. Перша з них може бути охарактеризована як пріоритетно-безпекова, за якої держава надає розширені повноваження органам влади щодо контролю інформаційних потоків, цензурування або тимчасового призупинення діяльності медіа. Така модель притаманна державам, що перебувають у тривалих або інтенсивних воєнних конфліктах, однак вона несе підвищені ризики для свободи слова та плюралізму.

Друга модель ґрунтується на принципі пропорційності та процесуальних гарантіях. У межах цього підходу обмеження свободи вираження допускаються лише на підставі закону, мають тимчасовий характер і супроводжуються ефективним судовим контролем. Ця модель відповідає стандартами ЄСПЛ і переважає у правопорядках держав-членів Ради Європи.

Окремої уваги заслуговує й змішана модель, за якої елементи жорсткого регулювання поєднуються з розвинутими механізмами парламентського та судового нагляду. Її застосування свідчить про прагнення держав мінімізувати негативний вплив воєнних обмежень на інформаційні права, не нівелюючи водночас ефективність заходів безпеки. Вважаємо, що для України є прийнятною саме *змішана модель правового регулювання забезпечення інформаційної безпеки* в умовах довго триваючого воєнного конфлікту. Для цього існують усі передумови, зокрема необхідність жорсткого регулювання інформаційної сфери, зважаючи на масштаб агресії, та дотримання євроінтеграційного курсу, що вимагає повагу до основних прав людини.

В умовах воєнного конфлікту протидія інформаційним загрозам набуває інституційно оформленого характеру та виходить за межі традиційного сектору безпеки, охоплюючи сферу стратегічних комунікацій, кібероборони, регулювання медіапростору й взаємодії з приватними цифровими платформами. Відповідно, у державах, що мають досвід воєнного протистояння або тривалого перебування в умовах гібридних загроз, сформувалися специфічні *організаційні підходи* до забезпечення цілісності інформаційного простору та зниження вразливості суспільства до деструктивного інформаційного впливу.

Важливою характеристикою таких організаційних підходів є діяльність спеціалізованих органів, передусім кіберкомандувань та структур інформаційної безпеки у складі сектору оборони. В США, Ізраїлі, Великій Британії кіберкомандування функціонують як окремі військові або міжвидові структури, наділені повноваженнями щодо захисту критичної інформаційної інфраструктури, ведення кібероперацій оборонного характеру та координації дій з цивільними органами. Наприклад, в США Кіберкомандування синхронізує, об’єднує, координує

та здійснює необхідні дії щодо керування функціонування і захистом інформаційних мереж Міністерства оборони [173, с. 176].

У низці держав сформовано центри стратегічних комунікацій або аналогічні координаційні платформи, завданням яких є узгодження публічних наративів, забезпечення культури кібербезпеки серед персоналу [163, p. 46], оперативне реагування на дезінформаційні кампанії та забезпечення єдності офіційної позиції органів влади. Наприклад, у ФРН – це Національний центр кіберзахисту, який здійснює співробітництво та координацію між усіма державними установами із захисту інформації [196, с. 32]. Практика держав Балтії та скандинавських країн свідчить, що такі центри ефективні лише за умови чіткого розмежування між інформаційною протидією та цензурою, а також за наявності прозорих процедур взаємодії з медіа й громадянським суспільством.

При забезпеченні інформаційної безпеки в умовах воєнного конфлікту важливою складовою є міжвідомча координація, яка за таких умов розглядається як фактор ефективності державної політики в цій сфері. При аналізі зарубіжного досвіду міжвідомчої координації чітко проглядається відсутність фрагментарного підходу, коли оборонні відомства, спецслужби, медіарегулятори та органи виконавчої влади діють ізольовано. Застосовуються координаційні механізми у формі спільних штабів, міжвідомчих комітетів або постійних робочих груп, до яких залучається також приватний сектор, зокрема оператори зв’язку, ІТ-компанії, соціальні мережі.

Особливу увагу в цьому контексті приділяють співпраці з приватними цифровими платформами, які де-факто виконують квазірегуляторну функцію у сфері поширення інформації. У державах, що перебувають у стані воєнного конфлікту, така взаємодія, як правило, ґрунтується не на примусовому контролі, а на договірних і процедурних механізмах обміну інформацією, спільних протоколах реагування та добровільному дотриманні стандартів. Разом із тим, ми не можемо погодитися на повне перенесення цього зарубіжного досвіду в Україну без урахування національних правових особливостей і рівня інституційної довіри, оскільки надмірна залежність від приватних акторів може створювати додаткові ризики для суверенітету інформаційної політики держави. У науковій літературі постійною проблемою,

характерною для нашої держави, відмічається навмисне створення штучно маніпульованого інформаційного середовища в суспільстві, яке суттєво впливає на суспільну свідомість та сприяє ворожим настроям щодо держави та її основних ознак [166, p. 3].

Співпраця державних органів із глобальними цифровими платформами, такими як Facebook (Meta), X (Twitter) або Google, є сьогодні однією з тенденцій у сучасному забезпеченні інформаційної безпеки. У державах, що перебувають у стані воєнного конфлікту така взаємодія зазвичай вибудовується у форматі спеціалізованих контактних центрів або міжвідомчих координаційних груп, уповноважених ініціювати блокування контенту, обмеження доступу до облікових записів або маркування інформації як потенційно недостовірної.

Водночас слід зауважити, що зазначені механізми не мають універсального правового оформлення. Вони ґрунтуються на поєднанні національного законодавства про воєнний або надзвичайний стан, внутрішніх правил платформ та неформалізованих домовленостей. Це породжує дискусію щодо меж допустимого державного впливу на інформаційні потоки, зокрема з огляду на стандарти свободи вираження поглядів, вироблені практикою ЄСПЛ. У цьому контексті характерною є тенденція до зміщення акценту з попередньої цензури на післяфактну реакцію та підвищення прозорості процедур видалення або обмеження контенту.

Окрему роль у таких моделях відіграють національні та міжнародні засоби масової інформації. Держави, залучені до воєнного протистояння, дедалі частіше застосовують інструменти стратегічних комунікацій, спрямовані не лише на внутрішню аудиторію, а й на міжнародну спільноту. Це зумовлює необхідність чіткого розмежування між інформаційною політикою як елементом національної безпеки та пропагандою у вузькому значенні, що також залишається предметом наукових дискусій.

Забезпечення інформаційної безпеки в умовах воєнного конфлікту задля ефективності цього процесу має передбачати участь громадянського суспільства у виявленні і протидії дезінформації. Н. Ржевська зауважує на системному характері державної діяльності щодо налагодження зв’язків із громадськістю у питаннях

формування основ інформаційної політики в умовах воєнного стану [172, с. 79]. Практика воєнних конфліктів останнього десятиліття засвідчує, що волонтерські ініціативи, незалежні аналітичні центри та спільноти фактчекерів здатні швидко виявляти інформаційні атаки, здійснювати перевірку повідомлень та поширювати спростування. Їхня ефективність значною мірою обумовлена гнучкістю організаційних форм та високим рівнем довіри з боку суспільства.

Разом із тим, інтеграція таких ініціатив у загальну систему забезпечення інформаційної безпеки потребує обережного підходу. Надмірна формалізація або підпорядкування державним структурам може знизити їхню автономність і, відповідно, суспільну легітимність. У зв'язку із цим, у зарубіжній практиці поширюється модель партнерської взаємодії, за якої держава створює правові та організаційні умови для діяльності громадянських акторів, утримуючись від прямого контролю за їхнім контентом.

Звернення до зарубіжного досвіду забезпечення інформаційної безпеки в умовах воєнного конфлікту є закономірним етапом наукового аналізу, зумовленим як транснаціональним характером сучасних інформаційних загроз, так і потребою пошуку ефективних правових та інституційних рішень для національної правової системи. Оцінка релевантності зарубіжного досвіду для України передбачає, передусім, розмежування універсальних і контекстуально зумовлених елементів системи інформаційної безпеки. До універсальних та таких, що заслуговують увагу щодо можливості рецепції зарубіжного досвіду, відносяться ті елементи, які ґрунтуються на визнанні інформаційного простору складовою національної безпеки, пріоритеті захисту критичної інформаційної інфраструктури, а також необхідності міжвідомчої координації та стратегічних комунікацій. Актуальним питанням залишається боротьба з кіберзагрозами, де міжнародна співпраця набуває надзвичайно важливого значення [167]. Такі положення визначені у правових актах і стратегічних документах держав-членів НАТО та ЄС і можуть бути адаптовані до українських реалій без істотних наслідків. Натомість моделі, що передбачають надмірну концентрацію повноважень у виконавчої влади або суттєве звуження свободи вираження поглядів під приводом воєнної необхідності, потребують

зваженої оцінки з огляду на конституційні засади України та її міжнародно-правові зобов'язання.

Окремої уваги заслуговує питання *меж правової імплементації* в національну практику правовідносин іноземних моделей забезпечення інформаційної безпеки в умовах воєнного конфлікту. Правова рецепція іноземного досвіду є ефективною лише за умови функціональної сумісності запозичуваних норм із національною правовою системою. У сфері інформаційної безпеки це означає необхідність узгодження нових регулятивних механізмів із чинним законодавством з питань захисту інформаційних прав, а також із практикою Конституційного Суду України та Європейського суду з прав людини. Ігнорування цих аспектів створює ризик формування формально жорстких, але фактично неефективних або навіть деструктивних правових конструкцій.

Разом із тим, не можна ігнорувати позитивний потенціал зарубіжного досвіду для розвитку національної моделі інформаційної безпеки. Зокрема, перспективним видається запозичення підходів до нормативного закріплення стратегічних комунікацій, протидії дезінформації в цифровому середовищі, а також використання гнучких регуляторних інструментів у взаємодії з приватними цифровими платформами. Важливо, однак, щоб такі підходи адаптувалися з урахуванням принципу пропорційності та тимчасовості обмежень, характерних для режиму воєнного стану.

Аналіз досвіду Німеччини, Франції, країн Балтії, США, Ізраїлю щодо забезпечення інформаційної безпеки в умовах воєнного конфлікту засвідчує, що його адаптація до національного правопорядку не може зводитися до механічного запозичення окремих нормативних чи інституційних рішень. Вирішальне значення має врахування специфіки конституційного ладу, правової культури, рівня інституційної спроможності держави, а також характеру та інтенсивності актуальних інформаційних загроз. У цьому контексті імплементація зарубіжних моделей повинна розглядатися як складний процес правової та організаційної трансформації, спрямований на підвищення стійкості національного інформаційного простору за умов триваючого воєнного протистояння.

Насамперед потребує уваги удосконалення законодавства України у сфері інформаційної безпеки. Досвід держав-членів ЄС, а також США та Ізраїлю свідчить про доцільність формування системного, а не фрагментарного нормативного регулювання, яке поєднує норми безпекового, інформаційного та адміністративного права. Актуальним питанням залишається адаптація міжнародних стандартів з інформаційної безпеки, таких, наприклад, як ISO/IEC 27001 [178, с. 6]. Окрім цього, для України перспективним видається подальше уточнення правових підстав обмеження окремих інформаційних прав і свобод у період воєнного стану з одночасним закріпленням ефективних гарантій від їх непропорційного звуження. Йдеться не лише про формальне відтворення стандартів Європейської конвенції з прав людини, а про вироблення чітких процедурних механізмів контролю за втручанням держави в інформаційну сферу, включно з роллю судової влади та незалежних регуляторних органів.

Зважаючи на досвід обраних нами для аналізу зарубіжних країн щодо забезпечення інформаційної безпеки в умовах воєнного конфлікту, ми можемо говорити про можливість внесення змін до Закону України «Про правовий режим воєнного стану». Згаданий закон, хоча і не є єдиним законодавчим актом, який регулює правовідносини у сфері забезпечення інформаційної безпеки в умовах потенційного або реального воєнного конфлікту, має системоутворююче значення для запровадження й реалізації відповідних обмежувальних та безпекових заходів. Саме цей нормативний акт виконує інтеграційну та режимну функцію, оскільки визначає допустимі межі втручання держави в інформаційну сферу, забезпечує правову легітимацію спеціальних заходів інформаційної безпеки, а також слугує нормативною основою для застосування інших законів в умовах воєнного стану.

Так, у п.п. 11 та 12 ст. 8 Закону передбачені деякі повноваження органів влади, що стосуються регулювання діяльності постачальників електронних мереж та вилучення комунікаційного обладнання [196]. Для конкретизації уже наявних повноважень у сфері інформаційної безпеки без розширення їх обсягу поза межами конституційних норм пропонуємо п. 11 доповнити наступними положенням: *«запроваджувати спеціальні заходи щодо моніторингу, аналізу та протидії*

інформаційним операціям, у тому числі іноземного походження, та вимоги до операторів електронних комунікацій щодо обміну інформацією про кіберінциденти з уповноваженими державними органами». Аналогічні положення містяться у законодавстві США та Великої Британії щодо обов'язку постачальників даних співпрацювати з державою у ситуаціях загрози національній безпеці. Це узгоджується з практикою розширеного доступу до комунікацій за допомогою судових санкцій.

Окрім цього, необхідно п. 12 ст. 8 Закону доповнити положенням про можливість *«запровадження тимчасових технічних обмежень доступу до онлайн-контенту, що становить безпосередню загрозу національній безпеці, після прийняття відповідного рішення уповноваженим державним органом у сфері інформаційної безпеки»*. Це відповідає практикам Франції, де в умовах надзвичайного стану держава отримує повноваження щодо блокування контенту, що загрожує безпеці. Забезпечення такої норми в національному законодавстві дозволить врегулювати належним чином механізми реагування на інформаційні загрози.

Законом України «Про правовий режим воєнного стану» достатньо детально визначаються повноваження військових адміністрацій як одних із головних, за думкою законодавця, суб'єктів забезпечення правового режиму воєнного стану. Очевидно, що ВА виступають за цих умов і гарантами основних прав людини. Відповідно до принципів прозорості, що часто застосовуються у правових системах ЄС та Великої Британії, гарантії прав громадян потребують балансу між безпекою та доступом до інформації. В Законі України «Про правовий режим воєнного стану» було б доцільно визначити чіткі межі оприлюднення та підзвітності з боку ВА, у зв'язку із чим ст. 15 слід доповнити положеннями наступного змісту: *«Військові адміністрації зобов'язані забезпечувати оприлюднення узагальненої інформації про застосовані заходи та їх правову підставу, крім випадків, коли таке оприлюднення може завдати шкоди національній безпеці»*.

Окрім цього, можна розглянути правову конструкцію, за якою у Законі України «Про правовий режим воєнного стану» буде прямо передбачено відповідальність за порушення вимог інформаційної безпеки в умовах воєнного стану, що завдало шкоди функціонуванню критичної інформаційної інфраструктури або забезпеченню захисту

населення від дезінформації. Інтеграція відповідальності за інформаційні правопорушення на рівні воєнного стану відповідає практикам, де функціональні гарантії інформаційної безпеки супроводжуються відповідними санкціями (наприклад, санкції за перешкоджання розслідуванню кіберзагроз у Великій Британії та США).

Окремий блок проблем пов'язаний із розвитком системи стратегічних комунікацій. Зарубіжна практика демонструє, що ефективна протидія інформаційним операціям противника ґрунтується не стільки на репресивних заходах, скільки на здатності держави формувати узгоджену, послідовну та довірчу комунікацію з власним населенням і міжнародними партнерами. Це зумовлює потребу інституціоналізації стратегічних комунікацій із чітким розмежуванням повноважень між органами сектору безпеки і оборони, органами виконавчої влади та публічними мовниками. При цьому запозичення моделей, розроблених у межах НАТО або ЄС, потребує корекції з огляду на високу динаміку воєнних подій та значний вплив неформальних цифрових платформ на формування суспільної думки.

Не менш важливим є підвищення стійкості інформаційної інфраструктури, що в зарубіжних державах розглядається як складова національної безпеки. Досвід країн, які зазнавали масштабних кібератак у період воєнних чи гібридних конфліктів, підтверджує доцільність поєднання правових, технічних та організаційних заходів захисту. У зв'язку із цим виникає необхідність подальшого розвитку нормативної бази у сфері кіберзахисту, зокрема щодо обов'язків операторів важливих інформаційних систем, а також поглиблення державно-приватного партнерства у сфері кібербезпеки. При цьому ідея перенесення моделей жорсткого державного контролю, характерних для країн із явно вираженим недемократичним устроєм, не вважається нами конструктивною, оскільки такі підходи можуть вступати в суперечність із євроінтеграційними зобов'язаннями України.

Таким чином, адаптація зарубіжного досвіду забезпечення інформаційної безпеки в умовах воєнного конфлікту має здійснюватися на засадах пропорційності як ключового правового орієнтиру. Застосування принципу пропорційності дозволяє відокремити правові механізми, спрямовані на легітимний захист національної

безпеки від практик, які не відповідають європейським стандартам захисту прав людини та зобов'язанням України в межах євроінтеграційного процесу. Це створює підґрунтя для обґрунтованої імплементації іноземних моделей правового регулювання забезпечення інформаційної безпеки в умовах воєнного конфлікту без порушення засад конституційного ладу.

Забезпечення інформаційної безпеки в умовах воєнного конфлікту не може розглядатися ізольовано від системи гарантій інформаційних прав людини. У результаті аналізу зарубіжної практики нами сформовано підхід, відповідно до якого обмеження таких прав мають характер тимчасового правового режиму, допустимого лише за наявності чітких процедурних підстав, ефективного судового контролю та можливості подальшого перегляду. Незважаючи на зовнішню агресію, Україні слід намагатися забезпечити баланс між безпековими потребами держави та вимогами правової визначеності й захисту прав особи.

Правове регулювання інформаційної безпеки в умовах воєнного конфлікту доцільно здійснювати відповідно до системної нормативно-правової моделі, що поєднує норми інформаційного, безпекового та адміністративного права. Такий підхід є характерним, зокрема, для Німеччини, Франції, Естонії та Іспанії, де правове регулювання інформаційної та кібербезпеки вибудовується на основі узгодження загальних актів безпекового характеру, спеціального інформаційного законодавства та адміністративних механізмів публічного управління. Це сприяє узгодженості правового регулювання в умовах кризових і воєнних загроз, підвищує ефективність реалізації безпекових рішень і водночас зменшує ризики правових колізій та непропорційного втручання держави в інформаційну сферу.

Зважаючи на аналіз зарубіжного досвіду, стратегічні комунікації слід розглядати не лише як елемент інформаційної політики, а як окрему функцію сектору безпеки і оборони. Ефективність стратегічних комунікацій безпосередньо залежить від чіткого інституційного закріплення, розмежування повноважень між суб'єктами публічної влади та налагодженої міжвідомчої координації, що має особливе значення в умовах активного інформаційного протиборства.

Інформаційна інфраструктура в умовах воєнного конфлікту набуває ознак об’єкта підвищеної правової охорони та має розглядатися як складова критичної інфраструктури держави. Зарубіжний досвід свідчить про ефективність поєднання публічно-правових інструментів із механізмами державно-приватного партнерства у сфері кібербезпеки, що дозволяє підвищити стійкість інформаційних систем без надмірного розширення державного контролю.

Інформаційну безпеку слід розглядати як складову національної безпеки з урахуванням її трансформації в умовах гібридних та інформаційних воєн. Нами надається аргументація, відповідно до якої зростання ролі цифрових платформ і недержавних акторів істотно змінює традиційні підходи до правового регулювання інформаційної сфери та потребує переосмислення інструментів державного впливу.

Існує необхідність післявоєнного перегляду правових режимів, запроваджених у сфері інформаційної безпеки. Зарубіжний досвід забезпечення інформаційної безпеки в умовах воєнного конфлікту демонструє можливість існування ризику збереження надзвичайних обмежень поза межами їх фактичної необхідності, що зумовлює потребу забезпечення балансу між безпековими обмеженнями та гарантіями інформаційних прав.

Євроінтеграційний характер забезпечення інформаційної безпеки в умовах воєнного конфлікту передбачає гармонізацію національного законодавства з правом ЄС не лише шляхом формального наближення норм, а й через змістовне врахування європейських підходів у сферах цифрових послуг, протидії дезінформації та захисту інформаційних прав. Це створює основу для формування стійкої моделі інформаційної безпеки України у воєнний та післявоєнний періоди.

Висновки до розділу 1

1. Методологія дослідження інформаційної безпеки України визначена як цілісна концептуальна основа, що забезпечує логіку наукового аналізу та формує системне бачення інформаційної безпеки як складової національної безпеки. Її багатовимірність розкривається через поєднання загальнонаукових і спеціально-юридичних методів із системним, синергетичним, герменевтичним, антропологічним і кібернетичним підходами, що дозволяє інтегрувати проблематику кібербезпеки, інформаційного суверенітету та захисту прав людини в єдину наукову конструкцію. Сучасні методологічні підходи, засновані на міждисциплінарності, ризик-орієнтованості та концепції кіберстійкості, розширюють можливості юридичної науки та створюють теоретико-методологічне підґрунтя для розвитку правових засад інформаційної безпеки в умовах воєнного стану.

2. Незважаючи на значний обсяг наукових досліджень, проблематика інформаційної безпеки не набула належної теоретико-правової систематизації, що зумовлено відсутністю її цілісної концепції як складової національної безпеки. Водночас воєнні та гібридні виклики актуалізували її розуміння як самостійного функціонального елемента системи національної безпеки, тісно пов’язаного з кібербезпекою, інформаційною політикою та стратегічними комунікаціями. Сформувався переважно міждисциплінарний підхід до її дослідження, що відображає багатовимірний характер цієї категорії та її значення як стратегічного ресурсу держави. Розширення методологічних підходів через інтеграцію концепцій кіберстійкості, управління ризиками та протидії дезінформації сприяє формуванню сучасної моделі інформаційної безпеки, адаптованої до цифрових і воєнних викликів.

3. Інформаційна безпека є складовою національної безпеки, що забезпечує захист життєво важливих інтересів людини, суспільства і держави в інформаційній сфері від внутрішніх і зовнішніх загроз. Вона характеризується складною багаторівневою структурою, поєднанням статичних і динамічних властивостей, нормативною регламентацією та тісним зв’язком із суверенітетом держави. Її структура охоплює об’єкти захисту, систему забезпечення та сукупність загроз. В

умовах воєнного стану ключовими є як внутрішні загрози (низька медіаграмотність, недосконаліть регулювання, слабкість інфраструктури), так і зовнішні (інформаційна агресія, кіберзагрози, дезінформація, втручання у внутрішні процеси). Це зумовлює необхідність комплексного підходу до її правового та організаційного забезпечення.

4. Забезпечення інформаційної безпеки в умовах воєнного конфлікту потребує застосування принципу пропорційності як критерію відмежування легітимних заходів захисту від надмірного втручання у права людини. Ефективною є системна модель правового регулювання, що поєднує норми інформаційного, безпекового та адміністративного права та відповідає європейським підходам. Стратегічні комунікації доцільно розглядати як окрему функцію сектору безпеки і оборони, що потребує інституційного закріплення та міжвідомчої координації. У цілому актуалізується потреба післявоєнного перегляду правових режимів інформаційної безпеки для забезпечення балансу між безпековими обмеженнями та гарантіями інформаційних прав.

РОЗДІЛ 2. ЮРИДИЧНА ПРИРОДА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ ТА ПЕРСПЕКТИВИ УДОСКОНАЛЕННЯ

2.1. Нормативно-правове забезпечення інформаційної безпеки України в умовах воєнного стану: проблеми та перспективи

В умовах сучасних глобальних викликів інформаційна безпека стала ключовим елементом національної безпеки держави. Особливо це стосується України, яка з 2014 р. протидіє безпрецедентній гібридній агресії з боку рф. Ця агресія включає не лише військові дії, але й потужні інформаційні атаки, спрямовані на дестабілізацію суспільства, підрив довіри до державних інституцій та маніпулювання громадською думкою. Використання дезінформації, кібератак, пропаганди та інших засобів інформаційного впливу стало невід'ємною складовою сучасних конфліктів, що підкреслює необхідність формування ефективної системи нормативно-правового забезпечення інформаційної безпеки.

Недостатня правова регламентація та відсутність чітких механізмів протидії інформаційним загрозам можуть призвести до посилення соціальної напруги, розколу у суспільстві та підриву інформаційного суверенітету. Тому, дослідження та вдосконалення нормативно-правових основ інформаційної безпеки України є надзвичайно важливим завданням для забезпечення стійкості та стабільності безпеки держави.

Правові основи національної безпеки і оборони досліджували М. Баймуратов, В. Богданович, В. Горовенко, С. Грищак, А. Георгіца, В. Денисов, О. Запорожець, М. Карпенко, В. Колесник, В. Куницький, В. Ліпкан, О. Литвиненко, Ю. Максименко, Л. Наливайко, В. Оборотов, Н. Пархоменко, В. Погорілко, О. Семенченко, В. Ткаченко, О. Чорноусенко та ін. Проблематика законодавчого регулювання інформаційної безпеки стала предметом уваги багатьох вітчизняних науковців. Серед дослідників, які зробили значний внесок у вивчення цієї тематики, можна відзначити: В. Антонова, І. Арістову, П. Біленчука, С. Білька, Л. Борисову, М. Гаврильців, С. Гнатюка, М. Григорчука, О. Дзьобаня, О. Довганя, І. Дороніна,

О. Золотаря, Б. Кормича, О. Косілову, С. Кудіна, В. Ліпкана, О. Логінова, О. Малашко, Н. Ментух, А. Нашинець-Наумову, І. Неклонського, Н. Новицьку, О. Олійника, В. Собину, Д. Сулацького, Т. Перун, І. Проць, Е. Рижкова, Т. Ткачука, В. Цимбалюка, А. Шевченка, О. Ярему та ін. Підзаконне регулювання інформаційної безпеки розкривалось у працях С. Гордієнка, В. Онищенка, Ю. Самохвалова, Н. Тарасенка, А. Турчака, О. Цвігуненко та ін. Їхні праці присвячені різним аспектам правового забезпечення інформаційної безпеки, включно з організаційно-правовими основами, політикою інформаційної безпеки, захистом інформаційних ресурсів та іншими ключовими питаннями.

Незважаючи на значний внесок цих дослідників, питання нормативно-правового забезпечення інформаційної безпеки України потребує подальшого комплексного аналізу з урахуванням сучасних викликів та загроз. Це зумовлює необхідність детального вивчення та вдосконалення правових механізмів, спрямованих на захист національного інформаційного простору

Правове регулювання в інформаційній сфері достатньо ускладнене, оскільки вона активно, швидко і всебічно розвивається. Ця сфера сповнена креативними й інноваційними поступками, які важко окреслити і спрямувати за допомогою юридичних правил. Низка інформаційних явищ фактично і практично взагалі не піддаються будь-якому унормуванню.

О. Золотар дійшов висновку, що початок історії захисту інформації пов’язаний з появою можливості фіксації інформаційних повідомлень на твердих носіях, тобто з винаходом писемності, а першим видом інформації, що підлягала захисту, вважають державну таємницю [199, с. 140]. Сучасний же інформаційний простір складно ефективно контролювати, він багатогранний.

Інформаційний простір – це форма співіснування сукупності матеріальних та нематеріальних об’єктів і процесів, спрямованих на задоволення інформаційних потреб всіх живих істот на Землі. Інформаційний зв’язок та інформаційні відносини відбуваються між суб’єктами «живої» і «неживої» природи. Об’єктами інформаційного простору є суб’єкти природного середовища, природні та штучні інформаційні відносини між ними та їх формування і використання, матеріальні та

нематеріальні об’єкти і процеси, спрямовані на задоволення інформаційних потреб для забезпечення збереження життя та життєдіяльності живої істоти, угрупування живих істот; суб’єктами інформаційного простору є живі істоти та їх угруповання, які спроможні сприймати, запам’ятовувати та переробляти інформацію, а також обмінюватися нею [134]. Правове врегулювання процесів, що відбуваються в інформаційному просторі здійснюється «post factum».

І. Валюшко справедливо підкреслює, що побудова законодавства у такій важливій сфері як інформаційна безпека відбувається за принципом надолуження згаяного. Натомість потрібно навчитися стратегічно планувати, прогнозувати дії у даному напрямі. Важливого значення набуває й контроль держави щодо виконання вже прийнятих юридичних норм, повне фінансове й кадрове забезпечення структур, пов’язаних із системою інформаційної безпеки, активізація інституційних реформ, які відповідають нагальним потребам у зазначеній сфері [198, с. 98]. Інформаційна безпека це відкрита динамічна система суспільних відносин. Відкритість цієї системи обумовлена тим, що інформаційна безпека не може мати постійний, незмінний характер. Структура інформаційної безпеки як об’єкта правової охорони не може бути визначена лінійно. Нелінійна класифікація структури інформаційної безпеки обумовлена складністю самої інформаційної сфери [92]. Отож, право визначає динаміку інформаційної сфери дуже опосередковано, що загалом є негативним фактором впливу на інформаційну безпеку.

При цьому, інформаційна сфера – це системоутворюючий чинник життя суспільства та держави, вона активно впливає на політичну, економічну, воєнну та інші складові національної безпеки країни, а у багатьох країнах і «вбирає» їх [91, с. 26]. Під національним інформаційним простором розуміють усю сукупність інформаційних потоків як національного походження, так і іноземних, що доступні на території держави [113, с. 71]. Отож, належне, ефективне правове забезпечення процесів, що відбуваються в інформаційній сфері, має ключове значення як для інформаційної безпеки, так і для національної безпеки загалом.

Механізм правового регулювання встановлює структуру для запобігання, виявлення, реагування на інциденти безпеки та відновлення після них, гарантує

вжиття відповідних заходів для захисту конфіденційної інформації. Правові норми сприяють підвищенню підзвітності, встановлюють керівні принципи для звітності про інциденти та розкриття інформації, полегшують співпрацю між різними установами та заохочують впровадження передової практики у сфері інформаційної безпеки. Правова база діє як захисний механізм, створюючи правову основу для забезпечення безпеки інформації та надаючи засоби правового захисту окремим особам чи організаціям, які постраждали від порушень безпеки [200; 383]. Правова основа забезпечення інформаційної безпеки в теоретичному сенсі є сукупністю різних за юридичною силою права норм, що відносяться до різних галузей і відображають сутність процесів, що відбуваються в сфері забезпечення інформаційної безпеки, складаючи єдину систему, що сприяє вдосконаленню механізму правового забезпечення інформаційної безпеки, направленого на підтримання балансу інтересів особи, суспільства та держави в інформаційній сфері завдяки вдосконаленню законодавчих засад [102, с. 200-201]. Нормативно-правове регулювання інформаційної безпеки в Україні базується на системному підході, який охоплює як стратегічне бачення національної безпеки в цілому, так і конкретні правові інструменти, спрямовані на запобігання інформаційним загрозам, що загострилися в умовах гібридної агресії рф.

Отже, нормативно-правова основа інформаційної безпеки України представлена нормами, що закріплені в Конституції України та законах України; підзаконних нормативно-правових актах; міжнародні актах, згоду на обов’язковість яких надано Верховною Радою України.

Важливою базою правового забезпечення інформаційної безпеки є Конституція України, яка проголошує свободу думки і слова, вільний доступ до інформації (ст. 34), а також закріплює обов’язок держави захищати національні інтереси, включно з безпековими аспектами (ст. 17) [201]. Конституція утворює основу правового забезпечення інформаційної безпеки, підпорядковуючи своїм положенням і систему законодавства у сфері безпеки та оборони, і систему інформаційного законодавства.

Закони в галузі національної безпеки і оборони за своїм політико-правовим змістом посідають після Конституції особливе місце, органічно розвивають її основні положення. Цим законам відводиться важлива роль у процесі захисту національних інтересів і гарантування в Україні безпеки особи, суспільства і держави від зовнішніх та внутрішніх загроз [202, с. 70]. Забезпечення інформаційної безпеки як складової національної безпеки здійснюється на рівні таких законів у сфері національної безпеки і оборони, як: Закони України «Про національну безпеку України» від 21.06.2018 р., «Про оборону України» від 06.12.1991 р., «Про правовий режим воєнного стану» від 12.05.2015 р., «Про контррозвідувальну діяльність» від 26.12.2002 р., «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р., «Про боротьбу з тероризмом» від 20.03.2003 р., Кодекс цивільного захисту України від 02.10.2012 р. та ін.

Законодавчим підґрунтям нормативного регулювання виступає Закон України «Про національну безпеку України» від 21.06.2018 р., який визначає інформаційну безпеку як складову національної безпеки та передбачає необхідність її забезпечення у сферах інформаційних ресурсів, кібербезпеки, інформаційного простору, протидії пропаганді та маніпулятивному впливу [94]. Відповідно до ст. 3 Закону України «Про оборону України» від 06.12.1991 р., підготовка держави до оборони в мирний час включає, зокрема, захист інформаційного простору України та її входження у світовий інформаційний простір, створення розвинутої інфраструктури в інформаційній сфері. Відповідно до ст. 4 Закону у разі збройної агресії проти України або загрози нападу на Україну Збройні Сили України разом з іншими військовими формуваннями розпочинають воєнні дії, у тому числі проведення спеціальних операцій (розвідувальних, інформаційно-психологічних тощо) у кіберпросторі [203]. Вказані норми визначають хоч і рамкові, проте досить конкретні гарантії забезпечення інформаційної безпеки, що повинні реалізуватись на постійні основі.

Окремо слід зупинитись на положеннях Закону України «Про правовий режим воєнного стану» від 12.05.2015 р., що у ст. 8 визначає заходи правового режиму воєнного стану. Серед них і ті, що спрямовані на забезпечення інформаційної безпеки, зокрема можливості: встановлювати (посилювати) охорону об’єктів критичної

інфраструктури та об’єктів, що забезпечують життєдіяльність населення, і вводити особливий режим їх роботи; порушувати питання про заборону діяльності політичних партій, громадських об’єднань, якщо вона спрямована на … пропаганду війни, насильства, на розпалювання міжетнічної, расової, релігійної ворожнечі, посягання на стійкість критичної інфраструктури, права і свободи людини, здоров’я населення; регулювати у порядку, визначеному Кабінетом Міністрів України, роботу постачальників електронних комунікаційних мереж та/або послуг, поліграфічних підприємств, видавництв, телерадіоорганізацій, телерадіоцентрів та інших підприємств, установ, організацій і закладів культури та медіа, а також використовувати місцеві радіостанції, телевізійні центри та друкарні для військових потреб і проведення роз’яснювальної роботи серед військ і населення; забороняти роботу приймально-передавальних радіостанцій особистого і колективного користування та передачу інформації через комп’ютерні мережі; у разі порушення вимог або невиконання заходів правового режиму воєнного стану вилучати у підприємств, установ і організацій усіх форм власності, окремих громадян електронне комунікаційне обладнання, телевізійну, відео- і аудіоапаратуру, комп’ютери, а також у разі потреби інші технічні засоби зв’язку; вживати додаткових заходів щодо посилення охорони державної таємниці [197]. Реалізація вказаних заходів в умовах воєнного стану супроводжується вжиттям окремих заходів щодо захисту інформації різного типу.

Нормативно-правове регулювання інформаційної безпеки є відносно самостійним напрямом правового регулювання в рамках комплексного механізму забезпечення національної безпеки України. Воно ґрунтується, перш за все, на нормах інформаційного права.

До ключових законів у цій сфері належать: Закони України «Про інформацію» від 02 жовтня 1992 р., «Про доступ до публічної інформації» від 13 січня 2011 р., «Про державну таємницю» від 21 січня 1994 р., «Про захист інформації в інформаційно-комунікаційних системах» від 05 липня 1994 р., «Про захист персональних даних» від 01 червня 2010 р., «Про Національну програму інформатизації» від 01 грудня 2022 р., «Про електронні комунікації» від 16 грудня 2020 р., «Про публічні електронні

реєстри» від 18 листопада 2021 р., «Про медіа» від 13 грудня 2022 р., «Про суспільні медіа України» від 17 квітня 2014 р., «Про хмарні послуги» від 17 лютого 2022 р., «Про цифровий контент та цифрові послуги» від 10 серпня 2023 р., «Про Національну систему конфіденційного зв'язку» від 10 січня 2002 р., «Про електронні документи та електронний документообіг» від 22 травня 2003 р.; «Про електронну ідентифікацію та електронні довірчі послуги» від 05 жовтня 2017 р. та багато ін.

Правове регулювання інформаційної безпеки здійснюється за допомогою спеціальних законів, серед яких важливе місце займає Закон України «Про інформацію», який визначає правові основи доступу до інформації, її захисту та класифікації, а також регулює обіг інформації у суспільстві [204]. Значну роль у забезпеченні кібербезпеки, як складової інформаційної безпеки, відіграє Закон України «Про основні засади забезпечення кібербезпеки України», який закріплює принципи кіберзахисту, визначає суб'єктів у сфері кібербезпеки та встановлює їхні повноваження [205]. У сфері діяльності медіа та захисту інформаційного простору працюють положення Закону України «Про медіа». Інформаційна сфера багатогранна, тому забезпечується широким колом нормативно-правових актів, які включають гарантії та засоби захисту інформації, регулюють безпеку її обробки та контролюють безпеку поширення і використання.

При цьому, саме правове забезпечення інформаційної безпеки на рівні інформаційного законодавства не позбавлене проблем.

Важливість розвитку законодавства у сфері інформації та інформаційної безпеки, становлення інформаційного суспільства визначається тією обставиною, що норми законів цієї сфери суттєво впливають на законодавче регулювання відносин суб'єктів у всіх сферах життя держави [114]. Концептуальні початкові напрацювання у вітчизняній законодавчій базі інформаційної політики та безпеки були, але вони мали досить фрагментарний та декларативний характер. Окрім того, багато колізій виникало у самому категоріальному апараті, що було перешкодою у гармонізації законодавства у цій сфері. Схвалені документи не забезпечили системного підходу до питання інформаційної безпеки, не було й забезпечено механізмів для їх реалізації. [198, с. 86]. В умовах гібридної війни, ці недоліки стають критичними для

національної інформаційної безпеки, демонструючи недієвість окремих норм. Тому, необхідною є систематизація, узгодження і гармонізація інформаційного законодавства загалом, що передбачатиме чітке визначення термінів, розробку ефективних механізмів реалізації правових норм та інтеграцію європейських стандартів.

В окрему групу варто виділити закони, що визначають правовий статус суб'єктів забезпечення інформаційної безпеки, оскільки вони закріплюють їх завдання і повноваження у цій сфері, а також напрями управління інформаційною безпекою.

Суб'єкти забезпечення інформаційної безпеки мають адміністративно-правовий статус, у зв'язку з чим норми адміністративного права визначають порядок взаємовідносин з органами державної влади та управління, регламентують контрольно-наглядову, дозвільну і юрисдикційну діяльність в цій сфері. Ціль правового регулювання інформаційної безпеки залежить від правової політики держави в інформаційній сфері. Вона визначається суб'єктами, що здійснюють нормативно-правове регулювання інформаційної безпеки з урахуванням свободи розсуду та розвитку приватної ініціативи юридичних і фізичних осіб, власників інформаційних систем і інформаційних ресурсів. Перспективою інформаційно-правової політики є формування відповідного інституційно-правового порядку, що сприяє досягненню державою бажаного результату, пов'язаного з національними інтересами в інформаційній сфері [102, с. 200-201]. Ефективне нормативно-правове забезпечення інституційної системи має ґрунтуватися на реалізації національних інтересів в інформаційній сфері та адаптації до викликів воєнного стану.

До нормативно-правових актів, що визначають правовий статус суб'єктів, залучених до забезпечення інформаційної безпеки належать: Закони України «Про Збройні Сили України» від 06 грудня 1991 р., «Про Національну гвардію України» від 13 березня 2014 р., «Про Раду національної безпеки і оборони України» від 05 березня 1998 р., «Про Службу безпеки України» від 25 березня 1992 р., «Про прокуратуру» від 14 жовтня 2014 р., «Про Національну поліцію» від 02 липня 2015 р., «Про Службу зовнішньої розвідки України» від 01 грудня 2005 р., «Про Кабінет

Міністрів України» від 27 лютого 2014 р., «Про центральні органи виконавчої влади» від 17 березня 2011 р., «Про військово-цивільні адміністрації» від 03 лютого 2015 р., «Про розвідку» від 17 вересня 2020 р., Указ Президента України «Про утворення військових адміністрацій» від 24 лютого 2022 р. № 68/2022, Постанова Кабінету Міністрів України «Питання Міністерства цифрової трансформації» від 18 вересня 2019 р. № 856, Постанова Кабінету Міністрів України «Про затвердження Положення про Міністерство оборони України» від 26 листопада 2014 р. № 671, Указ Президента України «Питання Центру протидії дезінформації» від 7 травня 2021 р. № 187/2021 та ін.

Розгалужена структура нормативно-правових актів у сфері інформаційної безпеки доповнюється численними актами Президента України, рішеннями РНБО, постановами Кабінету Міністрів України, які регламентують порядок реалізації окремих повноважень, особливо у період воєнного стану. У цьому контексті особливе значення має практика застосування рішень РНБО, введених у дію указами Президента щодо санкцій, блокування інформаційних ресурсів, протидії деструктивному інформаційному впливу тощо.

Програмними документами, що визначають загрози, виклики, стратегічні цілі та бажані результати у сфері інформаційної безпеки є вже згадані вище: Стратегія національної безпеки України, затверджена Указом Президента України від 14 вересня 2020 р. № 392; Стратегія інформаційної безпеки, затверджена Указом Президента України від 28 грудня 2021 р. № 685/2021; Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 р. № 447/2021; Концепція розвитку штучного інтелекту в Україні, схвалена розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. №1556-р та ін.

Одним із ключових документів, який визначає стратегічні орієнтири у цій сфері, є Стратегія інформаційної безпеки України, затверджена Указом Президента України від 14 травня 2021 р. № 187/2021. У Стратегії наголошено на необхідності посилення протидії дезінформації, розвитку медіаграмотності, забезпеченні кіберзахисту, охороні критичної інформаційної інфраструктури, захисті журналістів та свободи слова, а також створенні ефективної системи реагування на загрози в інформаційній

сфері [206]. Однак, реалізація зазначеної стратегії розрахована до 2025 р. Хоча низка її положень не втратили актуальності, все ж вона потребує концептуального оновлення.

Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 р. № 447/2021 визначає забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України. Стратегія кібербезпеки України враховує попередній досвід і проблеми, стан кібербезпекового середовища на національному та міжнародному рівні, а також положення Стратегії кібербезпеки ЄС на цифрове десятиліття, стратегій кібербезпеки окремих держав-членів ЄС та держав-членів НАТО [207]. Увалена стратегія є прикладом ефективного довгострокового планування. При цьому, як і Стратегія інформаційної безпеки України, вона потребує оновлення з урахуванням реалій воєнного стану.

З моменту оголошення воєнного стану, приймаються зміни до нормативно правових актів з врахуванням реалій війни. Вони стосуються врегулювання деяких аспектів інформаційних правовідносин щодо заборони поширювати певну інформацію, враховуючи її суспільнонебезпечний характер; врегулювання важливих моментів щодо технічного фіксування інформації в умовах воєнного стану; встановлення чи посилення відповідальності за поширення певної інформації; врегулювання процесуальних дій щодо вилучення інформаційних даних [139, с. 147; 375]. Україна співпрацює з міжнародними організаціями для обміну досвідом та технічної підтримки у сфері кібербезпеки.

Серед міжнародних організацій, що займались виробленням міжнародних та регіональних стандартів забезпечення інформаційної безпеки слід виділити ООН, Раду Європи, Європейський Союз, а також а також НАТО.

Як глобальна міжнародна організація, саме ООН має вплив на інформаційну безпеку як на міжнародному, так і на національному рівні.

Відповідно з п. 4 Статуту ООН всі Члени ООН утримуються в їхніх міжнародних відносинах від загрози силою або її застосування як проти територіальної недоторканності або політичної незалежності будь-якої держави, так і яким-небудь іншим чином, несумісним з цілями Об’єднаних Націй [208]. Діяльність

ООН спрямована на запобігання конфліктам у кіберпросторі, протидію дезінформації, регулювання технологій подвійного призначення та підтримку прав людини в цифровому середовищі.

Генеральна Асамблея ООН ухвалила ряд резолюцій у сфері забезпечення різних аспектів інформаційної безпеки, зокрема: Резолюції ГА ООН № 55/63 від 4 грудня 2000 р. та № 56/121 бід 19 грудня 2001 р. «Боротьба із злочинним використанням інформаційних технологій»; Резолюція ГА ООН 56/27 від 2003 р. «Заходи з ліквідації міжнародного тероризму»; Резолюція ГА ООН № 62/17 від 5 грудня 2007 р. «Про сприяння розгляду на багатосторонньому рівні існуючих та потенційних загроз у сфері інформаційної безпеки»; Серія Резолюцій ГА ООН «Роль науки та техніки в контексті міжнародної безпеки, роззброєння та інших, пов'язаних з цим сфер» (№ 43/77 від 07 грудня 1988 р., № 51/40 від 10 грудня 1996 р., № 54/50 від 1 грудня 1999 р.; № 60/51 від 2005 р.; № 60/51 від 06 січня 2006 р.; № 65/251 96 від 15 жовтня 2010 р.; № 74/367 від 18 листопада 2019 р.; № 78/22 від 04 грудня 2023 р. та ін.); Резолюція ГА ООН № 70/1 від 25 вересня 2015 р. «Перетворення нашого світу: Порядок денний у сфері сталого розвитку до 2030 року»; Резолюція ГА ООН № 73/218 від 20 грудня 2018 р. «Використання інформаційно-комунікаційних технологій з метою сталого розвитку» та багато ін.

Окремо слід виділити серію Резолюцій Генеральної Асамблеї ООН «Досягнення у сфері інформації та телекомунікацій у контексті міжнародної безпеки» (36/103 від 9 грудня 1981 р., 43/78 Н від 7 грудня 1988 р., 53/70 від 4 грудня 1998 р., 54/49 від 1 грудня 1999 р., 55/28 від 20 листопада 2000 р., 56/19 від 29 листопада 2001 р., 57/53 від 22 листопада 2002 р., 58/32 від 8 грудня 2003 р., 59/61 від 3 грудня 2004 р., 60/45 від 8 грудня 2005 р., 61/54 від 6 грудня 2006 р., 62/17 від 5 грудня 2007 р., 63/37 від 2 грудня 2008 р., 64/25 від 2 грудня 2009 р., 65/41 від 8 грудня 2010 р., 66/24 від 2 грудня 2011 р., 67/27 від 3 грудня 2012 р., 68/243 від 27 грудня 2013 р., 69/28 від 2 грудня 2014 р., 70/237 від 23 грудня 2015 р., 71/28 від 5 грудня 2016 р., 73/27 від 5 грудня 2018 р., 74/29 від 12 грудня 2019 р., 75/240 від 31 грудня 2020 р., 76/19 від 6 грудня 2021 р., 77/36 від 7 грудня 2022 р., 78/237 від 22 грудня 2023 р., 79/251 від 14 листопада 2024 р.), в яких наголошено на використанні інформаційних

та комунікаційних технологій у мирних цілях з метою формування спільноти спільного майбутнього для людства заради миру, безпеки та стабільності в інформаційному просторі.

Окремо увага Генеральної Асамблеї ООН була зосереджена навколо гарантування кібербезпеки. Цьому компоненту глобальної інформаційної безпеки були присвячені: Резолюція ГА ООН № 57/239 від 20 грудня 2002 р. «Створення глобальної культури кібербезпеки»; Резолюція ГА ООН № 58/199 від 23 грудня 2003 р. «Створення глобальної культури кібербезпеки і захист найважливіших інформаційних структур»; Резолюція ГА ООН № 64/211 від 21 грудня 2009 р. «Створення глобальної культури кібербезпеки і оцінка національних зусиль із захисту найважливіших інформаційних інфраструктур».

Отож, ООН виступає гарантом інформаційної безпеки в глобальному масштабі, просуваючи стандарти мирного міжнародного співробітництва в інформаційній сфері.

На регіональному рівні Рада Європи впливає на регулювання процесів в інформаційній сфері, формуючи правові стандарти для забезпечення інформаційної безпеки, захисту прав людини у цифровому середовищі та протидії кіберзлочинності. Особливу увагу Рада Європи приділяє захисту персональних даних, свободі медіа, боротьбі з дезінформацією та безпеці журналістів.

Рада Європи ухвалила Конвенція про захист осіб у зв’язку з автоматизованою обробкою персональних даних від 28 січня 1981 р. та Додатковий протокол до неї від 28 січня 2003 р., Конвенцію про транскордонне телебачення від 05 травня 1989 р., Конвенцію про кіберзлочинність від 22 листопада 2001 р., Конвенцію про доступ до офіційних документів від 18.06.2009 р., Декларацію Комітету Міністрів Ради Європи «Про свободу висловлювань та інформації від 29 квітня 1982 р. та ін.

Парламентською Асамблеєю Ради Європи та Комітетом Міністрів Ради Європи видано низку рекомендацій, що стосуються інформаційної сфери та загроз інформаційній безпеці людини, суспільства і держави. Серед них: Рекомендації Парламентської Асамблеї Ради Європи № 1506 (2001) «Свобода слова та інформації в засобах масової інформації в Європі», Рекомендації КМ РЄ № R (99) 1 «Про заходи

щодо сприяння плюралізму в ЗМІ», Рекомендації КМ РЄ № R (97) 21 «ЗМІ та сприяння культурі терпимості», Рекомендації КМ РЄ № R (97) 19 «Про показ насильства електронними ЗМІ», Рекомендації КМ РЄ № R (96) 4 «Про захист журналістів за умов конфліктів і тиску», Рекомендації КМ РЄ Rec (2002) 2 «Про доступ до офіційних документів», Рекомендації КМ РЄ № R (81) 19 «Про доступ до інформації, що знаходиться в розпорядженні державних органів», Рекомендації КМ РЄ № R (2000) 13 «Про європейську політику щодо доступу до архівів», Рекомендації КМ РЄ № R (91) 10 «Про передачу третім особам персональних даних, що знаходяться в розпорядженні державних органів», Рекомендації КМ РЄ № R (97) 18 «Про захист персональних даних, що збираються і обробляються в статистичних цілях», Рекомендації КМ РЄ № R (87) 15 «Про використання особистих даних у поліцейській галузі», Рекомендації КМ РЄ № R (95) 4 «Про захист особистих даних у сфері телекомунікаційних послуг», Рекомендація КМ РЄ № (2020) 1 «Щодо впливу алгоритмічних процесів на права людини та інші документи», Рекомендації КМ РЄ № (2018) 7 «Про принципи дотримання, захисту та реалізації прав дитини в цифровому середовищі», Рекомендація КМ РЄ № (2018) 2 «Про роль та відповідальність інтернетпосередників», Рекомендації КМ РЄ № R (89) 9 «Про злочини, пов'язані з комп'ютерами», Рекомендації КМ РЄ № R (95) 13 «Про проблеми кримінально-процесуального права, пов'язані з інформаційними технологіями» та багато ін.

Не зважаючи на рекомендаційних характер вказаних актів, їх реалізація та впровадження має вплив на гарантування інформаційної безпеки в Україні та в Європі. Україна активно імплементує вказані вище стандарти у законодавство про кібербезпеку, захист персональних даних і протидію інформаційним загрозам. Співпраця у рамках проєктів Ради Європи дозволяє Україні отримувати експертну підтримку, брати участь у спільних програмах і реформах.

Окремо слід виділити Плану дій Ради Європи для України «Стійкість, відновлення та відбудова» на 2023-2026 рр., що серед іншого підтримує необхідність надавати підтримку в частині зміцнення та подальшого погодження правової бази й практичних інструментів для цілей розслідування, судового переслідування та

міжнародного співробітництва в галузі кіберзлочинності та електронних доказів, особливо з урахуванням впровадження Другого Додаткового протоколу до Будапештської Конвенції про кіберзлочинність, що стосується розширення співробітництва та розкриття електронних доказів; надавати підтримку в частині повного здійснення процесуальних повноважень відповідно до Будапештської Конвенції про кіберзлочинність для сприяння розслідуванню та збору електронних доказів у випадках грубих порушень прав людини, включно з воєнними злочинами [209]. План дій Ради Європи для України є важливим документом, який демонструє стратегічну підтримку України з боку європейської спільноти. Особливе значення має поглиблення співпраці у боротьбі з кіберзлочинністю, зокрема у справах, пов'язаних із воєнними злочинами та порушеннями прав людини.

Узагальнюючи питання міжнародних стандартів у сфері інформаційної безпеки, слід відзначити, що їх вплив є факультативним, оскільки це питання стосується інформаційного суверенітету держави. Держави самостійно вирішують, у якому обсязі та якими незабороненими засобами досягати своїх національних інтересів в інформаційній сфері, з урахуванням наявних технічних можливостей та характеру загроз. Водночас міжнародні стандарти слугують орієнтиром для побудови ефективної системи інформаційної безпеки в умовах війни, а також сприяють уніфікації підходів на міжнародному рівні.

Засади нормативно-правового регулювання інформаційної безпеки в Україні становлять комплексну систему правових норм, що функціонують у межах загальнонаціональної стратегії безпеки. Вони забезпечують юридичне підґрунтя для реалізації державної політики у сфері захисту інформаційного простору, особливо в умовах гібридної агресії з боку російської федерації, яка потребує оперативного та ефективного реагування [67; 377, с. 5]. Водночас ця система потребує подальшого вдосконалення, зокрема в аспектах кодифікації, чіткого розподілу компетенції між суб'єктами, а також імплементації міжнародних стандартів інформаційної безпеки.

Вплив гібридної агресії на правове регулювання інформаційної безпеки в Україні є визначальним чинником трансформації нормативно-правової системи, що охоплює як зміст, так і динаміку правотворчих процесів. Починаючи з 2014 р., після

незаконної анексії Автономної Республіки Крим та частини територій Донецької і Луганської областей, російська федерація послідовно застосовує широкий арсенал засобів інформаційного впливу проти України. З початком повномасштабного вторгнення у 2022 р. ці процеси набули ще більшого масштабування. Це, у свою чергу, зумовило необхідність термінового перегляду підходів до правового регулювання сфери інформаційної безпеки.

Одним із найбільш показових проявів впливу гібридної агресії стало значне посилення правових механізмів державного реагування на загрози в інформаційному середовищі. Зокрема, в умовах воєнного стану було активовано практику прийняття рішень Ради національної безпеки і оборони України, які набувають юридичної сили після введення їх у дію Указами Президента. У цих рішеннях часто містяться заходи з блокування інформаційних ресурсів, пов'язаних з державою-агресором, або таких, що поширюють проросійську дезінформацію, розпалюють ворожнечу чи підривають обороноздатність держави [210]. Також було посилено кримінально-правові механізми, зокрема, введено додаткову відповідальність за колабораціонізм, поширення недостовірної інформації в умовах війни, публічне виправдовування збройної агресії проти України, передачу ворогові інформації про розташування Збройних Сил України тощо. Ці положення були закріплені у змінах до Кримінального кодексу України, ухвалених після 24 лютого 2022 р. [211]. У відповідь на масштабну дезінформаційну кампанію було створено Центр протидії дезінформації, що діє при РНБО України, основним завданням якого є виявлення фейків, інформаційних маніпуляцій і координація заходів протидії інформаційним загрозам. Діяльність цього органу не лише потребувала нормативного оформлення, а й стала стимулом для розробки додаткових підзаконних актів, методичних рекомендацій і протоколів взаємодії між суб'єктами безпеки.

В умовах гібридної війни держава була змушена балансувати між забезпеченням свободи слова та реалізацією функції самозахисту. З цією метою Національна рада України з питань телебачення і радіомовлення отримала розширені повноваження щодо тимчасового або постійного припинення мовлення телеканалів, діяльність яких створює загрозу національній безпеці, а також вживає заходів щодо

недопущення в ефір проросійських наративів або прихованої пропаганди [212]. Водночас важливою зміною, викликаною гібридною агресією, стало посилення ролі громадянського суспільства у забезпеченні інформаційної безпеки. Були запущені освітні й просвітницькі кампанії, спрямовані на підвищення рівня медіаграмотності, зокрема з ініціативи Міністерства культури та інформаційної політики, а також завдяки участі громадських організацій. Така активність отримала підтримку і на нормативному рівні – положення про формування критичного мислення і протидію фейкам дедалі частіше включаються до національних стратегій і державних програм.

Гібридна агресія російської федерації мала суттєвий вплив на зміст і структуру нормативно-правового регулювання інформаційної безпеки в Україні. Відбулося оперативне оновлення законодавства, розширення повноважень відповідних органів, активізація співпраці між державою та суспільством. Водночас залишається актуальним завданням удосконалення правових механізмів в аспекті дотримання стандартів прав людини, демократичного врядування та забезпечення належного контролю за реалізацією повноважень у сфері інформаційної безпеки.

У сучасних умовах, коли інформаційна сфера перетворилася на простір жорсткої боротьби за вплив на свідомість громадян, нормативно-правове забезпечення інформаційної безпеки постає одним із головних інструментів захисту суверенітету та демократичного розвитку України.

Проведений аналіз дає підстави зробити висновок, що вітчизняна правова система продемонструвала здатність до адаптації до нових викликів, які зумовлені гібридною агресією російської федерації. Законодавча база зазнала значного розширення, було створено нові інститути, запроваджено спеціальні процедури реагування на інформаційні загрози. Водночас, на тлі надзвичайного режиму воєнного стану, виникають і нові виклики, пов’язані із дотриманням балансу між безпековими цілями та захистом прав людини, свободою слова, прозорістю діяльності органів публічної влади.

Нормативно-правове забезпечення державної інформаційної політики необхідно привести у відповідність до вимог сучасності. У Конституції України прямо не вказується на обов’язок держави управляти процесами інформаційного

простору з метою захисту та реалізації прав та життєво важливих інтересів громадян, суспільства і держави; коло суб'єктів інформаційних відносин обмежується системою «громадянин-суспільство-держава», при цьому не враховані такі впливові суб'єкти управління процесами інформаційного простору, як іноземні держави, наддержавні об'єднання, транснаціональні корпорації та інші неурядові організації тощо. Це створює передумови для неспроможності законів та підзаконних актів гарантувати реальний інформаційний суверенітет України [213; 372]. О. Троянський зауважує, що є потреба в законодавчому закріплені таких понять, як інформаційна безпека держави, інформаційна безпека суспільства, інформаційна безпека організації (юридичної особи), інформаційна безпека людини (фізичної особи). Цілком логічним було б дати визначення даних термінів у базовому Законі України «Про інформацію» або Законі України «Про основні засади забезпечення кібербезпеки України». Адже відсутність однозначного розуміння вказаних формулювань може призвести до їх довільного тлумачення і, таким чином. створити умови для можливих зловживань під час застосування Стратегії на практиці, запровадження цензури та обмеження діяльності ЗМІ, Інтернету, соціальних мереж та створити інші посягання на свободу слова, що вже викликає занепокоєння громадськості [214, с. 189-190; 386]. Е. Рижков підкреслює, що законодавче забезпечення інформаційної безпеки в умовах воєнного стану потребує комплексного підходу, який враховує потреби безпеки, посилення ролі збройних сил, прозорості та міжнародного співробітництва. Вчений підтримує прийняття закону «Про кібервійська України» та їх створення повинно розглядатись як один із законотворчих пріоритетів держави наприкінці 10 років військового протистояння з російським агресором [215]. Отже, інституційна й нормативно-правова модернізація інформаційної політики є стратегічною потребою в умовах воєнного стану, без якої неможливе забезпечення інформаційного суверенітету України.

У контексті перспектив подальшого вдосконалення законодавства вбачається доцільним звернути увагу на кілька ключових напрямів. По-перше, необхідна систематизація правових норм у сфері інформаційної безпеки, з урахуванням того, що вони сьогодні розпорошені у великій кількості актів різної юридичної сили. Це

ускладнює їх застосування та ефективне правозастосування. Виходом може бути розробка та прийняття єдиного кодифікованого акта – наприклад, Інформаційного кодексу України.

По-друге, варто переглянути підходи до визначення повноважень суб'єктів забезпечення інформаційної безпеки, зокрема у частині чіткої регламентації механізмів взаємодії між державними органами та суб'єктами громадянського суспільства. Необхідно також удосконалити законодавчі положення, що стосуються оперативного інформування населення в умовах надзвичайних ситуацій, алгоритмів спростування дезінформації та правової відповідальності за її поширення. У цьому контексті доцільно враховувати міжнародний досвід, зокрема директиви Європейського Союзу, як-от Директива (ЄС) 2018/1808 щодо аудіовізуальних медіапослуг, яка посилює вимоги до прозорості медіа та відповідальності онлайн-платформ [216].

По-третє, потрібно підвищити якість правового регулювання у сфері медіаграмотності, оскільки критичне мислення громадян є не менш важливим елементом інформаційної безпеки, ніж технічні засоби захисту. Варто передбачити в освітньому законодавстві України обов'язкове включення тематики медіаграмотності до навчальних програм різного рівня – від загальної середньої освіти до вищої.

По-четверте, необхідно удосконалити інструменти судового захисту в разі порушення прав осіб у сфері інформаційних відносин. Показовими є приклади судової практики Європейського суду з прав людини, зокрема рішення у справах «Шмідт проти Австрії» (Schmid v. Austria) або «Сатакуннан Маркетінтімі і Сатамедіа Ой проти Фінляндії» (Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland), які підкреслюють важливість дотримання балансу між свободою вираження поглядів і захистом прав інших осіб на приватність [217].

У підсумку можна констатувати, що правове забезпечення інформаційної безпеки України значною мірою відповідає сучасним викликам, однак потребує подальшої глибокої модернізації – не тільки у відповідь на зовнішні загрози, але й для зміцнення засад демократичної правової держави. Зміцнення нормативної бази, підвищення правової обізнаності громадян, координація між державними та

громадськими суб'єктами інформаційної безпеки – це ключові орієнтири для подальшого руху України у цьому напрямі.

Аналіз чинної нормативно-правової бази України у сфері інформаційної безпеки дозволив зробити наступні висновки:

1. Нормативно-правова основа інформаційної безпеки України представлена нормами, що закріплені в Конституції України та законах України; підзаконних нормативно-правових актах; міжнародні актах, згоду на обов'язковість яких надано Верховною Радою України. Забезпечення інформаційної безпеки як складової національної безпеки здійснюється на трьох рівнях нормативно-правових актів: у сфері національної безпеки і оборони; у сфері інформаційних відносин та інформаційної безпеки; у сфері забезпечення правового статусу суб'єктів забезпечення інформаційної безпеки. Розгалужена структура нормативно-правових актів у сфері інформаційної безпеки доповнюється численними актами Президента України, рішеннями РНБО, постановами Кабінету Міністрів України, які регламентують порядок реалізації окремих повноважень, особливо у період воєнного стану. У цьому контексті особливе значення має практика застосування рішень РНБО, введених у дію указами Президента щодо санкцій, блокування інформаційних ресурсів, протидії деструктивному інформаційному впливу тощо.

2. Вплив міжнародних стандартів у сфері інформаційної безпеки, слід визнати факультативним, оскільки це питання стосується інформаційного суверенітету держави. Держави самостійно вирішують, у якому обсязі та якими незабороненими засобами досягати своїх національних інтересів в інформаційній сфері, з урахуванням наявних технічних можливостей та характеру загроз. Водночас міжнародні стандарти слугують орієнтиром для побудови ефективної системи інформаційної безпеки, а також сприяють уніфікації підходів на міжнародному рівні.

3. Норми у сфері інформаційної безпеки розпорошені у великій кількості актів різної юридичної сили, що ускладнює їх застосування. Необхідною є систематизація, узгодження і гармонізація інформаційного законодавства загалом, що передбачатиме чітке визначення термінів, розробку ефективних механізмів реалізації правових норм та інтеграцію європейських стандартів. Пропонується розробка та прийняття єдиного

кодифікованого акта – Інформаційного кодексу України. Потребують перегляду підходи до визначення повноважень суб'єктів забезпечення інформаційної безпеки, зокрема у частині чіткої регламентації механізмів взаємодії між державними органами та суб'єктами громадянського суспільства. Потребує посилення правове забезпечення медіаграмотності населення, оскільки критичне мислення громадян є не менш важливим елементом інформаційної безпеки, ніж технічні засоби захисту. Варто передбачити в освітньому законодавстві України обов'язкове включення тематики медіаграмотності до освітніх програм різного рівня – від загальної середньої освіти до вищої.

2.2. Інституційне забезпечення інформаційної безпеки України та напрями його удосконалення

В умовах інформаційного суспільства, швидкого розвитку інформаційних та кібертехнологій, стрімкого поширення інформації, з'являються численні можливості розвитку механізмів забезпечення інформаційної безпеки. Водночас, зростають безпекові загрози та ризики. Саме тому, набувають особливої актуальності та значущості наукові розвідки, спрямовані на виявлення правових та інституційних прогалин щодо регулювання інформаційної сфери.

Тематика інституційного забезпечення інформаційної безпеки в Україні не втрачає своєї актуальності з початку російської агресії. Низка дослідників звертали свою увагу на різні аспекти забезпечення, гарантування, регулювання, поновлення інформаційної безпеки, але розвиток цієї сфери є інтенсивним, тому він потребує подальшого наукового розкриття. Дослідження інституційного забезпечення інформаційної безпеки дозволяє віднайти оптимальні підходи для удосконалення всього механізму забезпечення інформаційної безпеки, оскільки саме від інституцій залежить якість такої діяльності.

Серед вітчизняних науковців, які досліджували інституційне забезпечення інформаційної безпеки: В. Авер'янов, І. Арістова, О. Баранов, І. Березовська, Н. Бортник, К. Бондаренко, В. Брижко, В. Гаращук, Т. Гаврилюк, І. Давидова,

Л. Євдоченко, Р. Калюжний, Л. Коваленко, В. Конах, Б. Кормич, А. Кузьменко, В. Ліпкан, Г. Линник, О. Логінов, Ю. Максименко, О. Олійник, Т. Субіна, В. Супрун, О. Тихомиров, О. Харитонова, В. Цимбалюк, В. Шамрай, М. Шевченко, Ю. Шемшученко та ін. Постійна наукова увага до інституційного забезпечення інформаційної безпеки пояснюється тим, що цей процес передбачає динамічну діяльність розгалуженої системи уповноважених суб'єктів. Але залишаються нерозкритими сучасні проблеми інституційного забезпечення інформаційної безпеки в Україні в умовах воєнного стану.

Відповідно до ст. 17 Конституції України [201] забезпечення інформаційної безпеки віднесене до найважливіших функцій держави, нарівні із захистом українського суверенітету та територіальної цілісності.

Досягнення стабільного стану інформаційної безпеки можливе за досягнення низки умов. Серед них, зокрема: розвиненість державної інформаційної політики; якість нормативно-правової основи; використання сучасних, інноваційних технологій і підходів в інформаційній сфері держави. Впровадження сучасних технологій і систем для захисту інформаційної безпеки вимагає нового бачення і відповідального підходу. Особливе значення має реальна, якісна і цілеспрямована робота державних і недержавних суб'єктів.

Отже, осмислення тематики інституційного забезпечення інформаційної безпеки України та визначення напрямів його удосконалення першочергово потребує з'ясування таких питань: що означає категорія «забезпечення інформаційної безпеки»; що входить до змісту поняття її «інституційного забезпечення»; які саме суб'єкти реалізують відповідну діяльність.

Категорія «забезпечення» активно застосовується в правничих дослідженнях. Етимологічно воно означає задовольняти когось, що-небудь у якихось потребах; створювати надійні умови для здійснення чого-небудь; гарантувати щось [218, с. 18]. До змісту категорії «забезпечення» в юриспруденції відносять такі складники, як: врегулювання, правове закріплення, визнання, гарантування, сприяння, реалізація, охорона, захист, поновлення та ін. [219-228]. Широка категорія «забезпечення» у поєднанні зі словосполученням «інформаційна безпека» позначає специфічний вид

діяльності, безперервний процес досягнення стану захищеності національних інтересів та інших життєво важливих інтересів людини, суспільства і держави в інформаційній сфері України. Для розкриття сутності інституційного забезпечення інформаційної безпеки, важливо з'ясувати що означає категорія «забезпечення інформаційної безпеки» та визначити з яких елементів складається цей процес.

Забезпечення інформаційної безпеки є складним і багатокомпонентним процесом. Цілком виправдано, що розкриття такого явища неодмінно потребує застосування *системного підходу.*

Так, О. Олійник під системою забезпечення інформаційної безпеки розуміє сукупність державних органів і органів місцевого самоврядування, підприємств, установ і організацій незалежно від форм власності, громадських об'єднань, їх посадових осіб та громадян, що здійснюють діяльність, спрямовану на вирішення завдань реалізації державної політики інформаційної безпеки відповідно до їх адміністративно-правового статусу, визначеного законодавством [229, с. 350]. Т. Ткачук до системи забезпечення національної безпеки включає сили та засоби забезпечення національної безпеки. Під силами пропонує розуміти суб'єктний склад системи забезпечення національної безпеки, тоді як під засобами – технології, а також технічні, програмні, лінгвістичні, правові, організаційні засоби, включаючи телекомунікаційні канали, що використовуються з метою збирання, формування, оброблення, передачі або приймання інформації щодо стану національної безпеки та щодо заходів, спрямованих на її зміцнення. Так само система забезпечення інформаційної безпеки (як складова частина системи забезпечення національної безпеки) включає в себе відповідні сили й засоби [230]. В залежності від завдань системи забезпечення національної безпеки Л. Радовецька виділяє: її формальну частину (органи державної влади, сили і засоби забезпечення безпеки тощо), а також неформальну (ІГС, громадяни, ЗМІ тощо). Суб'єктами, що утворюють цю систему є посадові особи, органи державного управління, ОМС, державні інститути, діяльність яких прямо чи опосередковано пов'язана із забезпеченням національної безпеки [231; 376, с. 39]. Отже, забезпечення інформаційної безпеки організоване на принципах системності, комплексності і цілісності. Низка науковців розкриває забезпечення

інформаційної безпеки як систему, що цілком виправдано, з огляду на те, що вона дійсно має специфічну багатоелементну структуру, внутрішні зв'язки, єдину мету та завдання.

Системний підхід дозволяє поглянути на її інституційну (суб'єктну) складову як на важливу, але не єдину складову. Інституційна складова забезпечення інформаційної безпеки діє на основі нормативної складової та послуговується засобами, ресурсами, технологіями, які умовно можна об'єднати під назвою інструментальної складової.

У науковій літературі також поширений погляд на забезпечення інформаційної безпеки як на вид діяльності уповноважених суб'єктів.

Забезпечення інформаційної безпеки О. Тихомиров розкриває як цілеспрямовану діяльність, домінуючим, але не єдиним елементом, об'єктно-суб'єктного складу якої є держава. Така інтерпретація, на думку вченого, враховує синергетичні тенденції розвитку сучасного суспільства та субсидіарні особливості його взаємодії з державою і у повну міру відповідає положенням теорії держави і права, згідно з якими функції держави розуміються як напрями, сторони або види державної діяльності [232]. О. Довгань та Т. Ткачук зауважують, що забезпечення інформаційної безпеки – діяльність щодо недопущення шкоди властивостям об'єкта безпеки, зумовленої інформацією та інформаційною інфраструктурою, а також засобів і суб'єктів цієї діяльності. Структура цього поняття охоплює: предмет та об'єкт безпеки, загрози об'єкту безпеки, діяльність із захисту об'єкта безпеки від загроз, засоби і суб'єкти забезпечення безпеки [233, с. 80]. Враховуючи, що забезпечення інформаційної безпеки дійсно є складним, врегульованим і цілеспрямованим процесом, застосування *діяльнісного підходу* щодо його розкриття дійсно сприяє отриманню об'єктивного наукового результату. Водночас, виправданим є те, що застосування діяльнісного та функціонального підходу в єдності для розкриття державно-правових явищ і процесів завжди пов'язане з особливою увагою до їх суб'єктивного складу.

Функціональний підхід у вивченні забезпечення інформаційної безпеки зосереджує увагу на функціях, завданнях, повноваженнях, компетенції конкретних суб'єктів.

В. Маслій зауважує, що невід'ємною ознакою будь-якої інституційної системи є організаційна єдність її складових, що виражається в чіткому розмежуванні завдань та функцій окремих суб'єктів, їх одночасна взаємозалежність і взаємообумовленість та відповідальність за остаточні результати діяльності [234, с. 50]. Ю. Шемшученко та І. Чиж вважають, що політика інформаційної безпеки має реалізовуватися як системою інститутів публічної влади, так і інститутами громадянського суспільства, до компетенції яких належить вирішення питань створення безпечних умов функціонування і розвитку інформаційної сфери [235, с. 79]. С. Білько акцентує, що сукупність державних і недержавних інституцій забезпечують створення нормативно-правових, організаційних та економічних умов, необхідних для формування та реалізації ефективної державної політики у сфері інформаційної безпеки [236, с. 38]. Б. Кормич підкреслює, що суб'єктам забезпечення інформаційної безпеки належить функція розробки і реалізації політики інформаційної безпеки [237, с. 157]. Отже, застосування функціонального підходу дозволяє зробити висновки про значення, роль та потенціал конкретних суб'єктів у забезпеченні інформаційної безпеки, розподіл їх функцій тощо. Він важливий, передусім, для досягнення комплексного та узгодженого розуміння функціонування інституційної складової в цілому.

Підсумовуючи, слід акцентувати, що наукова увага до інституційного компоненту забезпечення інформаційної безпеки зосереджується на визначенні місця і ролі суб'єктів, окресленні їх кола, а також на спробах встановити характер їх взаємодії, гармонізувати розподіл повноважень між ними тощо.

Прослідковується тенденція поєднання системного, діяльнісного, функціонального та інституційного підходів до осмислення проблематики забезпечення інформаційної безпеки. Однак, застосовуючи кожен із зазначених підходів, вчені зосереджують особливу увагу саме на суб'єктах.

Отже, забезпечення інформаційної безпеки – це комплексний, системний, організований і нормативно врегульований процес та вид діяльності уповноважених суб'єктів, спрямований на досягнення і підтримку стану захищеності життєво важливих інтересів людини, суспільства і держави в інформаційній сфері.

Детальної уваги заслуговує інституційний компонент цього процесу, а саме сутність «інституційного забезпечення інформаційної безпеки» та система відповідних суб'єктів.

Загалом, категорія «інституційний» походить від поняття «інститут» (від лат. institutio) і в довідниковій літературі визначається як офіційно встановлений, закріплений у своєму суспільному статусі [238]. Інститут – це сформоване системне високоорганізоване утворення, яке об'єднує діяльність людей для досягнення певної суспільної мети (суб'єктний підхід). В вузькому сенсі, інститут – це сукупність ідей, правил, норм, механізмів, які формують та розвивають певну організацію (об'єктний підхід) [238]. Слід підкреслити, що поняття «інститут» та «інституція» не є тотожними. Інституція як рушійна сила відповідної цілеспрямованої діяльності є основною категорією інституційної теорії. Інститут є поняттям більш складним, який розглядають як функціональну організацію, функціонування якої сприяє реалізації відповідної системи подібних інституцій [240, с. 53]. З метою розкриття предмету цього дослідження нами використано саме суб'єктний підхід до розуміння поняття «інституційний».

Інституційне забезпечення в правничих дослідженнях часто ототожнюють з цілеспрямованою, врегульованою діяльністю конкретних суб'єктів [241; 242; 243; 236, с. 38]. Інституційне забезпечення інформаційної безпеки є особливою структурною складовою державного механізму, що забезпечує створення норм і правил, що регулюють взаємодію різних суб'єктів в інформаційній сфері щодо запобігання загроз інформаційної безпеки [244]. Інституційна складова забезпечення інформаційної безпеки є не просто сукупністю суб'єктів, а представляє собою цілісну організовану систему – включає розподіл повноважень, компетенцій, функцій і завдань, меж відповідальності тощо.

Принагідно зауважимо, що у правничій літературі часто використовується категорія «інституційний механізм інформаційної безпеки». Її сутність обґрунтовує низка авторитетних дослідників.

Б. Кормич зауважує, що інституційний механізм інформаційної безпеки України – це сукупність державних інституцій, задіяних у процесі формування та впровадження політики інформаційної безпеки [130, с. 149]. О. Стоєцький вважає, що вузькому значенні інституційний механізм інформаційної безпеки охоплює виключно державні інституції, задіяні в процесі формування та впровадження політики інформаційної безпеки. У широкому значенні, крім інститутів публічної влади, до його складу входять також ІГС [245, с. 162]. На думку А. Новицького, цей термін позначає особливу структурну складову частину державного механізму, що забезпечує створення норм і правил, які регулюють взаємодію різних суб'єктів в інформаційній сфері щодо запобігання загроз інформаційній безпеці [246] В. Пашковський зауважує, що чітко діючий інституційний механізм має потенціал перетворення на вагомий політичний, силовий, гуманітарний інструмент щодо протидії антидержавним інформаційній впливам і стримування агресора в умовах гібридної війни [247]. Отож, з певною відмінністю, автори розкривають інституційний механізм інформаційної безпеки як сукупність суб'єктів, що взаємодіють для досягнення єдиної мети.

Однак, з позиції саме теоретико-правового дослідження важливо уточнити наступне. Як система елементів, що взаємопов'язані між собою, правовий механізм має єдину загальну мету, внутрішньо організовану структуру, елементи якої знаходяться у взаємозв'язку та підпорядкуванні [248, с. 131]. Забезпечення інформаційної безпеки є складним і багатоелементним явищем, яке утворює собою цілісний і комплексний механізм. Механізм забезпечення інформаційної безпеки включає правові, політичні, організаційні, інституційні, інструментальні та інші аспекти. Його інституційний компонент є важливим, системним і функціональним елементом. Але ціле не може бути складовою цілого, тому вважаємо недоцільним виділять в структурі цілісного механізму забезпечення інформаційної безпеки самостійного інституційного механізму.

Отож, розуміємо інституційну складову забезпечення інформаційної безпеки як організовану систему уповноважених суб'єктів, діяльність яких нормативно врегульована та спрямована на формування і реалізацію державної політики у сфері інформаційної безпеки, а також на забезпечення належного рівня захищеності життєво важливих інтересів особи, суспільства і держави в інформаційній сфері.

Перелік суб'єктів, які у різний спосіб забезпечують інформаційну безпеку держави, суспільства чи людини практично невичерпний. Чи не кожна інституція на своєму рівні в публічно-правових та приватно-правових інтересах здійснює заходи щодо захисту інформації, якою оперує. Отож, визначити чіткий перелік суб'єктів забезпечення інформаційної безпеки теоретично можливо, але не доцільно з практичної точки зору. Проте, важливо і цілком реально визначити та деталізувати їх систему.

В чинному законодавстві визначено суб'єктів інформаційної безпеки шляхом наділення їх окремими повноваженнями у цій сфері.

Так, відповідно до ст. 12 Закону України «Про національну безпеку України» від 21 червня 2018 р. до складу сектору безпеки і оборони входять: Міністерство оборони України, Збройні Сили України, Державна спеціальна служба транспорту, Міністерство внутрішніх справ України, Національна гвардія України, Національна поліція України, Державна прикордонна служба України, Державна міграційна служба України, Державна служба України з надзвичайних ситуацій, Служба безпеки України, Антитерористичний центр при Службі безпеки України, Служба судової охорони, Управління державної охорони України, Державна служба спеціального зв'язку та захисту інформації України, Апарат Ради національної безпеки і оборони України, розвідувальні органи України, центральний орган виконавчої влади, що забезпечує формування та реалізує державну військово-промислову політику [94]. Передусім сектору безпеки та оборони належить здійснювати контроль за інформаційною безпекою та реагувати на потенційні та реальні загрози.

У Стратегії інформаційної безпеки, затвердженій Указом Президента України від 28 грудня 2021 року № 685/2021 вказані наступні суб'єкти забезпечення інформаційної безпеки: 1) Рада національної безпеки і оборони України; 2) Кабінет

Міністрів України (забезпечує формування та реалізацію інформаційної політики держави, забезпечує інформаційний суверенітет, фінансування програм, пов'язаних з інформаційною безпекою, спрямовує і координує роботу міністерств, інших органів виконавчої влади у цій сфері); 3) органи державної влади у взаємодії з органами місцевого самоврядування, Центром протидії дезінформації та інститутами громадянського суспільства забезпечують реалізацію Стратегії; 4) центральний орган виконавчої влади, що забезпечує формування та реалізацію державної політики в інформаційній сфері – Міністерство цифрової трансформації України; 5) Міністерство закордонних справ України; 6) Міністерство оборони України; 7) Служба безпеки України; 8) Розвідувальні органи України; 9) Національна рада України з питань телебачення і радіомовлення [94]. Але і такий перелік фактично є не повним.

У Стратегії кібербезпеки України, затвердженій Указом Президента України від 26 серпня 2021 року № 447/2021, зауважено про утворення центрів (підрозділів) забезпечення кібербезпеки або кіберзахисту в Державній службі спеціального зв'язку та захисту інформації України, Службі безпеки України, Національному банку України, Міністерстві інфраструктури України, Міністерстві оборони України, Збройних Силах України. Розбудовується Національна телекомунікаційна мережа, утворюється Національний центр резервування державних інформаційних ресурсів, забезпечується функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, діє урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA. З метою покращення координації діяльності суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, утворено робочий орган Ради національної безпеки і оборони України – Національний координаційний центр кібербезпеки, рішення якого сприяють вирішенню найбільш складних проблем у цій сфері [207]. Протягом останніх років Україна значно зміцнила свої інституційні механізми у сфері інформаційної безпеки, і цей процес продовжує розвиватися.

Отже, аналіз нормативно-правового забезпечення інформаційної безпеки дозволяє відстежити ключових його суб'єктів, однак нормативний перелік не дає можливості простежити їх реальну цілісну систему.

Цікавим є науковий підхід до визначення системи суб'єктів забезпечення інформаційної безпеки України. Традиційно таких суб'єктів поділяють на державні та недержавні.

О. Стоєцький пропонує класифікувати суб'єктів забезпечення інформаційної безпеки України на: державні інституції (Президент України; органи виконавчої влади; інші державні органи й організації); недержавні інституції (ОМС; об'єднання громадян; інші недержавні інституції; громадяни України) [245, с. 162]. Схожу позицію підтримують В. Лук'янова та А. Лаутар, які до суб'єктів інформаційної безпеки відносять: державу, що здійснює свої функції через відповідні органи; громадян; суспільні або інші організації і об'єднання, що володіють повноваженнями по забезпеченню інформаційної безпеки у відповідності до законодавства [85]. Також, Р. Калюжний та В. Шамрай до суб'єктів інформаційної безпеки відносять: державу, що здійснює свої функції через відповідні органи державної влади шляхом створення системи забезпечення інформаційної безпеки, а також громадян, суспільні або інші організації і об'єднання, що володіють повноваженнями із забезпечення інформаційної безпеки відповідно до законодавства [249, с. 98]. Підтримуючи такий підхід вчених, зауважимо на його об'єктивності.

Наявні спроби і більш широко поглянути на характер та організаційну форму суб'єктів забезпечення інформаційної безпеки України.

На думку М. Барана, до суб'єктів забезпечення інформаційної безпеки належать: державні органи, державні установи, юридичні особи та фізичні особи-підприємці, яким належать інформаційні системи, інформаційно-комунікаційні мережі, автоматизовані системи управління, юридичні особи та фізичні особи-підприємці, які забезпечують взаємодію зазначених систем чи мереж [250, с. 222]. Т. Перун зауважує, що до суб'єктів забезпечення інформаційної безпеки на різних рівнях відносяться організації, інститути, служби, окремі особи (оперативні працівники, співробітники служб безпеки, інженерно-технічні працівники служб

захисту інформації тощо), які забезпечують інформаційну безпеку об'єкта на основі практичних дій, при введенні в дію механізму забезпечення інформаційної безпеки і організації практичних дій [102, с. 142]. Такий підхід, також, має наукову вагу, оскільки вказує на функціональне призначення суб'єктів забезпечення інформаційної безпеки, сприяє більш повному розумінню їх реальної структури.

Наявні й наукові підходи, що зосереджені на деталізації переліку таких суб'єктів. Їх емпіричний потенціал є значимим, однак з огляду на стрімкий розвиток інформаційної сфери та часті зміни у системі уповноважених суб'єктів забезпечення інформаційної безпеки, вони не рідко втрачають свою актуальність.

Зокрема, А. Крупнова відносить до системи суб'єктів адміністративно-правового забезпечення інформаційної безпеки в Україні наступних суб'єктів: Президент України; ВРУ; КМУ; РНБО України; Міністерство культури та інформаційної політики України; Міністерство з питань реінтеграції ТОТ України; Національна поліція України; СБУ; Служба зовнішньої розвідки України, Державна прикордонна служба України; Державна спеціальна служба транспорту; Державна служба України з надзвичайних ситуацій; Державна служба спеціального зв'язку та захисту інформації України; Збройні Сили України та інші органи виконавчої влади та військові формування, які входять до сектору інформаційної безпеки; ОМС; судові органи; комерційні компанії; недержавні організації та громадяни [251, с. 279]. С. Білко вважає органами державної влади, на які покладено функції формування та реалізації державної політики у сфері інформаційної безпеки: Президента України, Верховну Раду України, Кабінет Міністрів України, Міністерство оборони України, Міністерство культури та інформаційної політики України, Міністерство цифрової трансформації, Державну службу спеціального зв'язку та захисту інформації, Державний комітет телебачення і радіомовлення України, Раду національної безпеки і оборони України, Департамент кіберполіції Національної поліції України, інші центральні органи виконавчої влади та органи сектору безпеки і оборони України, місцеві органи виконавчої влади та ОМС [236, с. 38]. Погоджуючись із запропонованими підходами, зауважимо, що до забезпечення інформаційної безпеки

в тій чи іншій мірі залучено кожен орган державної влади та місцевого самоврядування.

Т. Перун узагальнює, що для забезпечення інформаційної безпеки характерна багаторівнева система суб'єктів, заснована на принципі єдності та диференціації [102, с. 149]. Це складна багаторівнева система, яка, з одного боку, об'єднується особливою загальною функціональною спрямованістю, а з іншого – розділяється специфічними особливостями, пов'язаними з рівнем компетенції і характером відповідних цілей [252, с. 149]. Інституційна система забезпечення інформаційної безпеки в Україні є цілісною, але водночас диференційованою. Для неї характерна така риса як спільна функціональна спрямованість великої кількості автономних суб'єктів, хоча їх компетенції, повноваження та завдання розмежовані. Така багаторівневість дозволяє забезпечити комплексний вплив на стан інформаційної безпеки, але вона призводить і до негативних наслідків, таких як брак якісної координації, неузгодженість дій різних суб'єктів, відсутність чіткого розподілу функцій між цими суб'єктами та їх дублювання тощо.

К. Захаренко справедливо зауважує, що суб'єкт-об'єктні характеристики інформаційної безпеки мають багатоплановий й різнорівневий характер. Системоутворюючим суб'єктом інформаційної безпеки є держава, але її діяльність у демократичних країнах не може повною мірою забезпечити багатоаспектні інтереси й потреби об'єктів у цій сфері. Саме тому виникає необхідність залучення до забезпечення інформаційної безпеки країни недержавних суб'єктів [253, с. 42]. Дійсно, держава не має фактичного монопольного впливу на інформаційну безпеку, оскільки сучасний інформаційний простір формується та функціонує за участю широкого кола недержавних суб'єктів.

Тому в науковому співтоваристві [253-256] підтримуються ідеї посилення консолідації та взаємодії державних і недержавних суб'єктів забезпечення інформаційної безпеки.

Держава в першу чергу, має бути зацікавленою у побудові міцних і стабільних зв'язків з недержавним сектором у інформаційній сфері, заснованих на принципах взаємоповаги, взаємної відповідальності та партнерства. Водночас держава зберігає

ключову роль у формуванні нормативно-правової основи інформаційної безпеки, визначенні стратегічних напрямів і стандартів її забезпечення, отож має безпосередній потенціал впливати на консолідацію всієї системи.

Особливості здійснення державою функцій забезпечення інформаційної безпеки полягають у тому, що діяльність кожного державного органу здійснюється шляхом використання інформаційної інфраструктури суспільства, формування та споживання ресурсів інформаційного характеру, встановлення відносин із громадянами [257, с. 214]. Відповідно, органи державної влади як розпорядники відповідної інфраструктури повинні реалізувати комплекс заходів, спрямованих на забезпечення збереження ресурсів і безпеки роботи систем інформації, телекомунікації, управління та зв'язку.

Державні органи в системі інституційного забезпечення інформаційної безпеки України слід поділяти відповідно до їх компетентності на загальні та спеціальні.

Загалом, в Україні система забезпечення інформаційної безпеки на рівні держави формується та реалізується центральними та регіональними органами, спеціалізованими організаціями та підприємствами. Сьогодні сформувалася ієрархічна система суб'єктів, пов'язаних із забезпеченням безпеки в інформаційній сфері, яку очолює Президент України (відповідно до п. 17 статті 106 Конституції України). Ряд функцій щодо інформаційної безпеки покладено на Раду національної безпеки і оборони України, як конституційного дорадчого органу, закріплено у Законі України «Про Раду національної безпеки і оборони України» [258]. Ця система охоплює, також, інших суб'єктів, зокрема Верховну Раду України, яка відповідає за законодавчу діяльність, органи судової влади, органи виконавчої влади центрального рівня, суб'єкти контролю за виконанням законодавства іншими органами виконавчої влади, державні та міжвідомчі комісії, місцеві представницькі та виконавчі органи, громадян та громадські об'єднання, що залучені до забезпечення інформаційної безпеки.

Варто зазначити, що такі центральні органи виконавчої влади, як Міністерство економіки України та Міністерство цифрової трансформації України, які відповідають за розвиток електронних комунікацій, цифровізації та цифрової

економіки, є особливо важливими суб'єктами системи, які забезпечує інформаційну безпеку [259, с. 497]. До того ж, Державна служба України спеціального зв'язку та захисту інформації та підпорядковані регіональні органи мають повноваження у галузі технічного захисту інформації, здійснюють планові та позапланові перевірки об'єктів критичної інформаційної інфраструктури, організацію спеціального зв'язку та захисту інформації в органах публічної влади.

Однак, питання утворення єдиної інституції з питань забезпечення інформаційної безпеки постійно обговорюється.

Т. Ткачук зауважує, що залишається відкритим питання щодо необхідності створення спеціально уповноваженого органу державної влади з питань забезпечення інформаційної безпеки. Водночас не виключено, що така «надструктура» не зможе монополізувати й ефективно виконувати функції щодо забезпечення інформаційної безпеки внаслідок специфічного інтегруючого характеру останньої та її здатності «проникати» до інших сфер життєдіяльності суспільства внаслідок їх інформаційного обслуговування. [230]. В Україні, на сьогодні, не існує єдиного спеціально уповноваженого державного органу, який би відповідав за забезпечення інформаційної безпеки. Натомість діє система суб'єктів, у межах якої різні функції розподілені між різними інституціями. Однак, така ситуація пояснюється саме природою інформаційної безпеки як міжгалузевого, інтегративного явища.

М. Зайцев стверджує, що кількість елементів системи забезпечення інформаційної безпеки не повинна бути надмірною, оскільки їх збільшення буде призводити до ускладнення функціонування і, як наслідок, зменшення її ефективності [260]. Ми підтримуємо ідею про те, що замість створення нової інституції в умовах воєнного стану, пріоритетним є вдосконалення вже існуючої системи суб'єктів забезпечення інформаційної безпеки шляхом підвищення їх інституційної спроможності та посилення механізмів координації.

Дослідники зосереджують увагу на державному секторі в інституційному забезпеченні інформаційної безпеки, але підкреслюють роль громадянського суспільства та окремих фізичних осіб.

Громадянські інституції є повноцінними учасниками процесу забезпечення інформаційної безпеки держави. Як показує суспільно-політична практика, зусиль державних органів, як правило, не вистачає для ефективної протидії інформаційним загрозам, що обумовлює потребу побудови діалогу з соціумом. Базовими елементами механізму взаємодії між владою і суспільством у даній сфері є інституційна, нормативно-правова та практична складові. Від повноцінного використання всіх можливостей і ресурсів, наявних у суспільстві залежить ефективність функціонування всієї системи інформаційної безпеки держави [122]. Інститути громадянського суспільства є невід'ємною частиною забезпечення інформаційної безпеки України. Вони не лише реагують на виклики, але й беруть участь у формуванні стратегії інформаційної безпеки держави.

Перелік недержавних суб'єктів забезпечення інформаційної безпеки достатньо широкий, але їх участь у цьому процесі є добровільною. До таких суб'єктів відносять засоби масової інформації, громадські організації, наукові установи, недержавні підприємства та інші структури, які беруть участь у захисті інформаційного простору.

Окрему категорію специфічних недержавних суб'єктів забезпечення інформаційної безпеки представляють зацікавлені фізичні особи.

Це особи, які беруть участь у формуванні безпечного інформаційного середовища шляхом реалізації своїх прав, свобод, законних інтересів та юридичних обов'язків. До них належать, зокрема: користувачі інформаційних ресурсів, осінтери, блогери, науковці, експерти у сфері інформаційних технологій та кібербезпеки та багато ін. Крім того, це також громадяни України, які здійснюють громадський контроль в інформаційній сфері.

Наприклад, як зауважує О. Любиченко, сучасні лідери громадської думки, або інфлюенсери, мають значний вплив на формування суспільних настроїв в Україні, що зумовлено доступністю сучасних технологій, які дозволяють їм здійснювати цей вплив фактично безперешкодно. Часто їхні дії створюють потужний резонанс у суспільстві, який може мати як конструктивний, так і деструктивний вплив. Вплив блогерів на їхні аудиторії настільки значний, що довіра до них часто перевищує довіру до державних інституцій. Це створює ризик того, що через недостатню

освіченість інфлюенсери можуть поширювати в своїх соціальних мережах меседжі, які сприймаються аудиторією як істина, що призводить до дестабілізації суспільних відносин [254; 374]. Отож, зацікавлені фізичні особи виступають впливовими суб'єктами забезпечення інформаційної безпеки, оскільки саме на індивідуальному рівні формується стійкість суспільства до інформаційних впливів і загроз.

Важливими суб'єктами забезпечення інформаційної безпеки є комерційні та некомерційні підприємства, установи та організації різних форм власності. Їх мережа є широкою, а діяльність часто пов'язана з виробництвом, розпорядженням, зберіганням та поширенням інформації. Особливо це стосується комерційних суб'єктів.

Існує постійна небезпека несанкціонованого втручання у інформаційні ресурси комерційних суб'єктів з боку інших держав, іноземних комерційних структур (промисловий та комерційний шпіонаж, знищення баз даних задля перемоги у конкурентній боротьбі тощо). Саме тому від якісного захисту власних інформаційних ресурсів суб'єктами комерційної діяльності залежить і загальносуспільна та загальнодержавна інформаційна безпека, перш за все, у сфері економічної діяльності. Вищеозначені суб'єкти повинні дбати про власну інформаційну безпеку, прогнозуючи та нівелюючи можливі загрози, оскільки захист комерційної інформації є важливим чинником безпеки суспільства та держави в цілому та інформаційної зокрема [253, с. 39; 381].

Особливе значення мають суб'єкти господарювання у сфері інформаційно-комунікаційних технологій, медіа та критичної інформаційної інфраструктури, оскільки їх діяльність безпосередньо впливає на стан інформаційної безпеки держави, суспільства та особи.

Отже, до системи суб'єктів забезпечення інформаційної безпеки України пропонується віднести: 1) інституції державного сектору – Верховну Раду України, відповідні парламентські комітети; Президента України, Раду національної безпеки та оборони; Кабінет Міністрів України, міністерства та інші центральні та місцеві органи виконавчої влади; органи сектору безпеки і оборони; 2) недержавні інституції – ОМС; недержавні підприємства, установи та організації; ІГС; фізичні особи.

Формування і модернізація інституційної складової забезпечення інформаційної безпеки є безперервним процесом, який вимагає постійного вдосконалення, оптимізації, гармонізації та адаптації до нових загроз і викликів.

Враховуючи проведений аналіз, слід зауважити, що інституційне забезпечення інформаційної безпеки в Україні потребує переосмислення та посилення. Низка проблем інституційного забезпечення інформаційної безпеки залишаються невирішеними в умовах воєнного стану та суттєво впливають на обороноздатність України в цілому.

Як вже було зауважено, воєнний стан в Україні зумовлює потребу критично оцінити ефективність координації суб'єктів забезпечення інформаційної безпеки. Брак координації та взаємодії між державними та недержавними суб'єктами призводить до того, що рф успішно реалізує інформаційні атаки, а протидія їм здійснюється постфактум. Системне і оперативне реагування на інформаційні загрози ускладнене через недоліки комунікації, брак гнучких підходів щодо взаємодії уповноважених суб'єктів.

В умовах воєнного стану в Україні, надзвичайно важливо забезпечити комунікаційну взаємодію не тільки між органами державної влади та органами місцевого самоврядування, а й з інституціями громадянського суспільства. Стратегічні комунікації як процес взаємодії між органами публічної влади в Україні щодо забезпечення інформаційної безпеки – це система внутрішніх і зовнішніх комунікацій, а зв'язки з інститутами громадянського суспільства – це один зі складників стратегічних комунікацій, які надають можливість реалізувати державну політику у сфері забезпечення інформаційної безпеки комплексно та цілісно.

Для забезпечення інформаційної безпеки, уповноваженим суб'єктам необхідно забезпечити пріоритет захисту прав громадян на доступ до інформації. Це передбачає спільний моніторинг різноманітних форм прояву інформаційних загроз і ризиків та впровадження необхідних заходів для протидії їм [261].

В умовах війни органи публічної влади демонструють високий рівень інформаційної взаємодії із суспільством. Міністерства та відомства систематично доводять до суспільства актуальну інформацію. А виступи Президента України, голів

обласних військових адміністрацій, присвячені аналізу поточної ситуації, звіту про свою роботу, стали для громадян звичними та підвищують рівень довіри суспільства до органів влади, незважаючи на інформаційну політику держави-терориста, спрямовану на дестабілізацію політичної, економічної та соціальної систем українського суспільства.

Проблеми забезпечення інформаційної безпеки пов'язані з фрагментарністю власне самої інституційної системи загалом. Розподіл функцій із забезпечення інформаційної безпеки між широким колом суб'єктів ускладнює узгодженість їх спільної діяльності. Проблемою є не скільки дублювання повноважень між різними рівнями інституційного забезпечення інформаційної безпеки, скільки нечіткість розмежування сфер та меж їх відповідальності.

Протидія загрозам у сфері інформаційної безпеки вмагає посилення інституційної спроможності окремих суб'єктів. Проблемами, які важливо вирішити є брак кадрових, матеріально-фінансових та інноваційних технічних ресурсів.

Отже, можна виділити ключові проблеми інституційного забезпечення інформаційної безпеки в Україні: фрагментарність інституційної системи забезпечення інформаційної безпеки; недостатня координація між її суб'єктами; брак чітко визначених меж відповідальності суб'єктів забезпечення інформаційної безпеки; недостатній рівень інституційної спроможності окремих суб'єктів; слабка інтеграція недержавних суб'єктів до системи забезпечення інформаційної безпеки; низький рівень інформаційної культури та медіаграмотності населення.

Перспективи удосконалення інституційного забезпечення інформаційної безпеки в умовах воєнного стану обумовлені реальними практичними і правовими проблемами, що наразі існують в інформаційній сфері держави.

Забезпечення організаційної взаємодії органів публічної влади у сфері забезпечення інформаційної безпеки неможливе без актуалізації наступних аспектів: досягнення балансу між владою та суспільством, що сприяє соціальному та суверенному розвитку України; використання всіх наявних засобів для протидії інформаційній агресії російської федерації; підтримання автентичності та

ідентичності українського народу в контексті глобалізації, а також визнання ролі України як повноправного учасника процесу європейської інтеграції.

Ефективне функціонування інституційного забезпечення інформаційної безпеки потребує: оновлення законодавства, а саме внесення змін до законів і положень, які регламентують діяльність суб'єктів забезпечення інформаційної безпеки, взаємоузгодження завдань і функцій по забезпеченню інформаційної безпеки; встановлення механізму керівництва, контролю та нагляду у сфері забезпечення інформаційної безпеки з чітким розподілом ролей і повноважень; введення інституту відповідальності за неналежний рівень організації дотримання вимог внутрішньої інформаційної безпеки; запровадження системи загальної підготовки суб'єктів забезпечення інформаційної безпеки до виконання покладених на них завдань; активація взаємодії та інформаційного обміну між суб'єктами забезпечення інформаційної безпеки як ефективного інструменту вирішення покладених на них завдань [144; 262]. Ключовою умовою ефективного забезпечення інформаційної безпеки є посилення медіаграмотності населення та досягнення довіри громадян до об'єктивної і прозорої інформації, яку надають органи публічної влади.

До напрямів удосконалення інституційного забезпечення інформаційної безпеки в Україні в умовах воєнного стану пропонується віднести: 1) систематизація правових основ діяльності суб'єктів забезпечення інформаційної безпеки та закріплення їх в окремому розділі єдиного кодифікованого акту – Інформаційного кодексу України; 2) гармонізація підходів щодо розподілу функцій, повноважень і меж відповідальності ключових суб'єктів забезпечення інформаційної безпеки; 3) розвиток публічно-приватного партнерства, посилення координації та комунікації між державними та недержавними суб'єктами забезпечення інформаційної безпеки, створення гнучких і ефективних механізмів їх взаємодії; 4) посилення інституційної спроможності суб'єктів забезпечення інформаційної безпеки через розвиток кадрового потенціалу, наукового, фінансового, правового, технічного забезпечення; 5) розвиток стратегічних комунікацій уповноважених суб'єктів забезпечення інформаційної безпеки з населенням та забезпечення комплексного підвищення рівня інформаційної грамотності громадян.

Отже, дослідження інституційного забезпечення інформаційної безпеки України та напрямів його удосконалення дозволяє запропонувати наступні висновки та узагальнення:

1. Забезпечення інформаційної безпеки – це комплексний, системний, організований і нормативно врегульований процес та вид діяльності уповноважених суб'єктів, спрямований на досягнення і підтримку стану захищеності життєво важливих інтересів людини, суспільства і держави в інформаційній сфері. Забезпечення інформаційної безпеки включає правові, політичні, організаційні, інституційні, інструментальні та інші елементи. Застосування системного, діяльнісного, функціонального та інституційного підходів до осмислення проблематики забезпечення інформаційної безпеки демонструє провідне значення системи суб'єктів, як елементу цього процесу.

2. Інституційну складову забезпечення інформаційної безпеки запропоновано розуміти як організовану систему уповноважених суб'єктів, діяльність яких нормативно врегульована та спрямована на формування і реалізацію державної політики у сфері інформаційної безпеки, а також на забезпечення належного рівня захищеності життєво важливих інтересів особи, суспільства і держави в інформаційній сфері. Інституційна складова забезпечення інформаційної безпеки в Україні є цілісною, але водночас диференційованою. Для неї характерна така риса як спільна функціональна спрямованість великої кількості автономних суб'єктів, хоча їх компетенції, повноваження та завдання розмежовані. Така багаторівневість дозволяє забезпечити комплексний вплив на стан інформаційної безпеки, але вона призводить і до негативних наслідків.

3. До системи суб'єктів забезпечення інформаційної безпеки України пропонується віднести: 1) інституції державного сектору – Верховну Раду України, відповідні парламентські комітети; Президента України, Раду національної безпеки та оборони; Кабінет Міністрів України, міністерства та інші центральні та місцеві органи виконавчої влади; органи сектору безпеки і оборони; 2) недержавні інституції – органи місцевого самоврядування; недержавні підприємства, установи та організації; інститути громадянського суспільства; фізичні особи. В Україні не існує

єдиного спеціально уповноваженого державного органу, який би відповідав за забезпечення інформаційної безпеки. Однак, замість створення нової державної інституції в умовах воєнного стану, пріоритетним є вдосконалення вже існуючої системи суб'єктів забезпечення інформаційної безпеки шляхом підвищення їх інституційної спроможності та посилення механізмів координації.

4. Ключовими проблемами інституційного забезпечення інформаційної безпеки в Україні: фрагментарність інституційної системи забезпечення інформаційної безпеки; недостатня координація між її суб'єктами; брак чітко визначених меж відповідальності суб'єктів забезпечення інформаційної безпеки; недостатній рівень інституційної спроможності окремих суб'єктів; слабка інтеграція недержавних суб'єктів до системи забезпечення інформаційної безпеки; низький рівень інформаційної культури та медіаграмотності населення. До напрямів удосконалення інституційного забезпечення інформаційної безпеки в Україні в умовах воєнного стану пропонується віднести: 1) систематизація правових основ діяльності суб'єктів забезпечення інформаційної безпеки та закріплення їх в окремому розділі єдиного кодифікованого акту – Інформаційного кодексу України; 2) гармонізація підходів щодо розподілу функцій, повноважень і меж відповідальності ключових суб'єктів забезпечення інформаційної безпеки; 3) розвиток публічно-приватного партнерства, посилення координації та комунікації між державними та недержавними суб'єктами забезпечення інформаційної безпеки, створення гнучких і ефективних механізмів їх взаємодії; 4) посилення інституційної спроможності суб'єктів забезпечення інформаційної безпеки через розвиток кадрового потенціалу, наукового, фінансового, правового, технічного забезпечення; 5) розвиток стратегічних комунікацій уповноважених суб'єктів забезпечення інформаційної безпеки з населенням та забезпечення комплексного підвищення рівня інформаційної грамотності громадян.

2.3. Кібербезпека як елемент інформаційної безпеки в умовах воєнного стану

У контексті трансформації сучасного безпекового середовища, зумовленої цифровізацією суспільного життя та ескалацією гібридних загроз, кібербезпека набуває статусу одного з ключових напрямів національної безпеки, а в умовах воєнного стану – стає критичним елементом інформаційної безпеки держави. Війна нового покоління відбувається не лише у фізичному просторі, а й у віртуальному середовищі – кіберпросторі, що перетворився на повноцінну площину ведення бойових дій.

З урахуванням цього постає об'єктивна потреба в глибокому теоретико-правовому осмисленні категорії «кібербезпека», її сутності, структури, правової природи та місця у системі інформаційної безпеки. Зокрема, актуальним є визначення особливостей кіберзагроз в умовах збройного конфлікту, правових механізмів їх попередження і нейтралізації, а також встановлення меж і форм відповідальності за дії у кіберпросторі.

Незважаючи на наявність окремих теоретичних та прикладних досліджень у сфері кібербезпеки, зокрема, на рівні доктрини національної безпеки, кримінального права, адміністративного регулювання, в українській юридичній науці відсутнє комплексне бачення кібербезпеки саме як структурного елементу інформаційної безпеки в умовах воєнного стану. Це значно ускладнює нормативне регулювання, міжвідомчу координацію, а також формування цілісної державної політики в цій сфері.

З огляду на викладене, виникає необхідність не лише в концептуалізації категоріального апарату, а й у системному аналізі чинного законодавства України та міжнародно-правових підходів до забезпечення кібербезпеки під час збройних конфліктів. Особливої уваги потребує правовий статус кіберпростору, легітимність кібератак у межах воєнного стану, а також узгодження національного підходу з нормами міжнародного гуманітарного права.

Питання правового забезпечення кібербезпеки, зокрема в умовах збройного конфлікту, стали предметом наукового аналізу як українських, так і зарубіжних дослідників. Серед українських учених варто відзначити праці О. Бакалінської, О. Баранової, М. Дмитренко, В. Лисиченка, С. Карвацької, Н. Кучминди, С. Мазепи, М. Сироватченко, М. Пашкова, О. Петришина, І. Валюшко, О. Передерій, В. Поліщука, О. Юрченка, які розглядали кібербезпеку крізь призму національної безпеки, адміністративно-правового та інформаційного регулювання, а також у контексті міжнародно-правових зобов'язань України. Серед зарубіжних науковців, важливий внесок у розвиток теорії кібербезпеки зробили: M. E. O'Connell, яка досліджує кібератаки з позицій міжнародного гуманітарного права; J. Healey – автор робіт із кіберстратегії та державної кібероборони; N. Tsagourias, який аналізував правовий статус кіберпростору та відповідальність у кіберсфері; а також T. Stevens і D. Betz, що розробляли концептуальні підходи до «кіберсили» та кіберконфліктів у межах воєнної доктрини. Утім, незважаючи на наявність зазначених наукових розвідок, питання кібербезпеки як складової інформаційної безпеки держави в умовах воєнного стану, її правової природи, системного місця в безпековому механізмі та узгодженості з міжнародно-правовими нормами, продовжує залишатися недостатньо дослідженим. Це зумовлює потребу у подальшому науковому осмисленні й обґрунтуванні відповідних правових підходів, що і є предметом цього дослідження.

Отже, аналіз кібербезпеки як структурного елементу інформаційної безпеки в умовах воєнного стану є не лише актуальним, а й необхідним для формування ефективної моделі захисту державного суверенітету в цифровому вимірі. Саме цій проблематиці присвячено цей підрозділ дисертаційного дослідження.

Зазначимо, що у XXI ст. спостерігається безпрецедентна трансформація характеру воєнних конфліктів, зумовлена стрімким розвитком інформаційно-комунікаційних технологій. Інформаційний простір, що охоплює сферу виробництва, зберігання, обробки, передачі та поширення інформації, перетворився на стратегічний ресурс і самостійний театр бойових дій. Війна у сучасному світі вже не обмежується лише фізичними зіткненнями на полі бою – її фронти проходять через сервери, інформаційні платформи, цифрову інфраструктуру та свідомість громадян.

Воєнні дії, що супроводжуються масованими інформаційними, кібертехнічними й психологічними атаками, характеризують нову епоху гібридних конфліктів, у межах яких знищується чіткий поділ між цивільною та військовою сферами. У цьому контексті інформаційна безпека стає не лише елементом національної безпеки, а й невід'ємною частиною стратегії оборони держави.

Варто наголосити, що в умовах повномасштабної збройної агресії проти України інформаційний компонент бойових дій набув надзвичайної ваги. Масштабне поширення дезінформації, фальсифікацій, психологічних операцій та кібератак на критичну інфраструктуру з боку держави-агресора засвідчило, що контроль над інформаційним простором є визначальним для досягнення воєнно-політичних цілей. Тому інформаційна війна – це не абстрактне поняття, а конкретний інструмент воєнної агресії.

Поняття «кібербезпека» сформувалося як відповідь на потребу правового та інституційного реагування на зростання загроз у кіберпросторі. З розвитком глобальної цифрової інфраструктури, вразливості інформаційних систем, інтенсифікації злочинності в кіберсфері та зростання кібершпигунства постала необхідність створення системи захисту не лише технічного, а й юридичного рівня.

Спочатку термін «кібербезпека» використовувався переважно в технічному контексті, однак із часом він набув правового і політичного значення. У сучасному розумінні кібербезпека є комплексом організаційно-правових, технічних, інформаційних, комунікаційних та інших заходів, спрямованих на запобігання, виявлення, нейтралізацію та ліквідацію загроз у кіберпросторі.

Закон України «Про основні засади забезпечення кібербезпеки України» (2017) визначає кібербезпеку як «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі» [205]. Таке визначення чітко інтегрує категорію кібербезпеки до системи національної безпеки, що підтверджується також положеннями Стратегії національної безпеки

України (2020) [263], Стратегії кібербезпеки (2021) та іншими актами стратегічного характеру [264].

Важливо, що особливого значення кібербезпека набуває у періоди збройного конфлікту, коли держава повинна одночасно захищати інформаційні системи критичної інфраструктури, запобігати втручанню у державні реєстри, оборонятися від кібератак на військові об'єкти, і водночас вести активну боротьбу на інформаційному фронті.

У межах сучасної правової науки інформаційна безпека розглядається як інтегральна категорія, що охоплює захист інформації, інформаційної інфраструктури, інформаційного простору та суб'єктів, котрі в ньому функціонують. Кібербезпека є, з одного боку, складовою інформаційної безпеки, а з іншого – відносно самостійним елементом системи національної безпеки.

Теоретико-правовий взаємозв'язок між цими двома категоріями полягає в тому, що: по-перше, інформаційна безпека має ширший зміст, охоплюючи всі види інформаційних впливів, включаючи психологічні, пропагандистські, соціально-комунікаційні, інформаційно-правові; по-друге, кібербезпека фокусується на цифровій складовій – захисті комп'ютерних мереж, інформаційно-комунікаційних систем, програмного забезпечення, апаратного забезпечення, каналів передачі інформації, у тому числі в умовах використання новітніх технологій (штучного інтелекту, Internet of Things, Big Data тощо).

Так, кібербезпека не охоплює всі аспекти інформаційної безпеки, однак є її критичним елементом, без якого неможливе повноцінне функціонування інформаційного простору держави, особливо в умовах гібридних загроз і збройного конфлікту.

У період воєнного стану межа між інформаційною та кібербезпекою дедалі більше стирається, адже кібератаки стають не лише засобом виведення з ладу систем, але й платформою для інформаційного впливу на громадську думку, зниження морального духу населення та дискредитації державних інституцій. У зв'язку з цим виникає об'єктивна потреба у перегляді традиційних доктринальних підходів до цих

понять, а також у розробці комплексного правового механізму, здатного адекватно реагувати на виклики цифрової епохи.

У науковій та прикладній площині поняття «кібербезпека» розглядається як багатоаспектна категорія, що поєднує елементи технічного, інформаційного, правового та організаційного характеру. В юридичній доктрині відсутнє єдине усталене визначення цього поняття, що зумовлено динамічністю розвитку кіберпростору та гібридністю загроз, що виникають у ньому.

Загальнотеоретичні підходи трактують кібербезпеку як стан захищеності національного кіберпростору, суб'єктів кібердіяльності та критичної інфраструктури від зовнішніх і внутрішніх загроз, спрямованих на порушення конфіденційності, цілісності, доступності та достовірності інформації.

У роботах провідних дослідників, зокрема, О. Белова, І. Костюка, М. Каркача, С. Глазьєва, кібербезпека розглядається як невід'ємний елемент інформаційної безпеки, орієнтований на забезпечення стабільного функціонування цифрових систем у межах національного інформаційного простору. Низка зарубіжних авторів, зокрема, L. Ablon та M. Libicki наголошують на стратегічному характері кібербезпеки як чинника, що безпосередньо впливає на стійкість державного управління, економіки, військової сфери та демократичних інститутів.

Окремі підходи поділяють кібербезпеку на: індивідуальну (персональну) – захист персональних даних і цифрової ідентичності; організаційну – захист IT-інфраструктури підприємств та установ; державну – охоплює захист критичної інфраструктури, систем урядового зв'язку, воєнної сфери, банківської системи тощо.

Таким чином, доктринальний підхід до розуміння кібербезпеки свідчить про її системний та багатокомпонентний характер, що вимагає чіткої регламентації на рівні національного та міжнародного права.

Згідно з положеннями Закону України «Про національну безпеку України» (2018), кібербезпека є складовою національної безпеки, що тісно пов'язана із забезпеченням інформаційної безпеки [94]. У цій площині вона постає як окрема підсистема, що функціонує у взаємодії з іншими складовими: воєнною, економічною, екологічною, техногенною тощо.

Водночас Закон України «Про основні засади забезпечення кібербезпеки України» (2017) закріплює інституційну модель забезпечення кібербезпеки, визначаючи її об’єкти (державні інформаційні ресурси, об’єкти критичної інфраструктури, інформаційно-телекомунікаційні системи тощо) та суб’єкти (органи державної влади, Служба безпеки України, Збройні Сили України, Національний банк України, Державна служба спеціального зв’язку та захисту інформації України, приватні оператори тощо) [205].

Таким чином, у системі інформаційної безпеки кібербезпека виконує функцію захисту технологічного сегмента інформаційного простору, охоплюючи: інформаційно-комунікаційні системи, бази даних та сервіси, канали передачі даних, апаратно-програмне забезпечення, електронну інфраструктуру державного управління.

На рівні практики, особливо в умовах воєнного стану, межа між інформаційною безпекою (у широкому розумінні) та кібербезпекою (у технічному й правовому вимірі) часто є умовною, оскільки кібератаки поєднують технічні, психологічні та пропагандистські компоненти.

До числа основних суб’єктів системи кібербезпеки України належать: 1) Рада національної безпеки і оборони України – координує реалізацію державної політики у сфері кібербезпеки на стратегічному рівні; 2) Служба безпеки України – головний орган із протидії кібертероризму та кібершпигунству, здійснює кіберконтррозвідку; 3) Державна служба спеціального зв’язку та захисту інформації України – відповідальна за урядовий зв’язок, криптографічний та технічний захист інформації; 4) Міністерство оборони України / Збройні Сили України – створюють підрозділи кібероперацій у складі сил оборони; 5) Національний банк України – здійснює заходи з кіберзахисту банківської системи; 6) Кібервійська / ІТ-армія України – хоч і мають волонтерське або напівофіційне походження, але активно беруть участь у кібервійні; 7) Приватний сектор (оператори критичної інфраструктури, телеком-компанії, хостинги) – згідно з законом, зобов’язані дотримуватися вимог кіберзахисту.

Важливо, що координація між цими суб'єктами в умовах воєнного стану набула нових форм через інтеграцію воєнної та кіберскладової у стратегії національної безпеки.

Щодо нормативно-правового закріплення кібербезпеки на міжнародному та національному рівнях, слід зазначити, що національне законодавство України, що регулює сферу кібербезпеки, включає: Закон України «Про основні засади забезпечення кібербезпеки України» (2017) – основоположний документ, що встановлює принципи, цілі, суб'єкти й механізми забезпечення кібербезпеки [205]; Закон України «Про національну безпеку України» [92], Закон України «Про інформацію» [204], Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [265]; профільні укази Президента України, зокрема, Стратегія кібербезпеки України (2021) [264] та укази про створення кібервійськ; постанови Кабінету Міністрів України, що регламентують діяльність центрів реагування на інциденти (Урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA) та захист критичної інфраструктури.

Серед нормативної регламентації на міжнародному рівні, слід виокремити: Талліннський мануал 2.0 – авторитетне джерело щодо застосування міжнародного гуманітарного права до кібероперацій [266]; Резолюції ООН (Група урядових експертів, Відкрита робоча група з інформаційно-комунікаційних технологій) щодо відповідального поводження держав у кіберпросторі [267]; документи НАТО, зокрема Cyber Defence Pledge – визнають кібератаки як потенційні підстави для застосування ст. 5 Вашингтонського договору [268]; право ЄС – Директива NIS2 (Directive on Security of Network and Information Systems 2) [269], Загальний регламент про захист даних (General Data Protection Regulation) [270], а також політика Європейського агентства з кібербезпеки (European Union Agency for Cybersecurity) [271; 387].

Варто зазначити, що в умовах війни Україна вимушена адаптувати свій нормативно-правовий механізм кібербезпеки в режимі реального часу, реагуючи на нові виклики, зокрема через імплементацію західного досвіду, оперативне оновлення процедур кіберзахисту та легалізацію нових форм взаємодії з приватним сектором.

Так, можна стверджувати про складність і поліфункціональність інституту кібербезпеки в умовах воєнного стану. Українське законодавство демонструє тенденцію до поступового наближення до стандартів НАТО/ЄС, але ще потребує подальшої систематизації, імплементації норм міжнародного гуманітарного та кримінального права щодо кібервійн, а також удосконалення інституційної взаємодії. Усі ці фактори мають бути враховані у правозастосовній і нормотворчій практиці найближчих років.

Стосовно кіберзагроз як інструменту ведення гібридної війни, важливо зазначити, що сучасна війна набуває гібридного характеру, де межа між військовими та цивільними цілями, між миром і війною, суттєво розмита. У цій парадигмі кіберпростір стає однією з ключових арен збройного протистояння, а кіберзагрози – дієвим інструментом агресії проти держави, суспільства та особи.

У міжнародному праві досі триває дискусія щодо правового статусу кібератак: чи можуть вони кваліфікуватися як «застосування сили» в розумінні ст. 2(4) Статуту ООН або як «збройний напад» відповідно до положень міжнародного гуманітарного права [272]. Проте вже зараз зрозуміло, що кібератаки можуть мати ефект, еквівалентний збройному нападу, особливо коли вони спрямовані на об’єкти критичної інфраструктури або порушують функціонування органів державної влади.

У випадку з Україною кіберагресія рф почалася задовго до відкритої фази повномасштабного вторгнення у 2022 р., що підтверджує стратегічний характер кібервійни як підготовчого, паралізуючого та дестабілізаційного інструменту.

У цьому контексті важливо надати характеристику основних кіберзагроз.

Кібератаки на критичну інфраструктуру є однією з найнебезпечніших форм кіберзагроз, оскільки спрямовані на об’єкти, від котрих залежить життєздатність держави: енергетика, транспорт, зв’язок, водопостачання, охорона здоров’я, банківська система. Зокрема, міжнародна практика (і Талліннський мануал) розглядає атаки на критичну інфраструктуру як можливий casus belli, тобто підставу для застосування збройної сили у відповідь.

Серед прикладів, зокрема, можна навести 2015 та 2016 рр. – кібератаки на енергосистему України (приписані групі Sandworm), в результаті яких відбувалося

відключення електроенергії у Києві та на заході України; 2022 р. – масштабні спроби дестабілізувати роботу «Укренерго», атомних електростанцій, водоканалів та інших об’єктів критичної інфраструктури [273].

Окрему увагу слід приділити кібершпигунству, що є цілеспрямованою діяльністю з проникнення до інформаційних систем органів державної влади, оборонних підприємств, аналітичних центрів з метою викрадення конфіденційної або державної таємниці. Цей тип загроз класифікується як порушення державного суверенітету та може кваліфікуватися відповідно до національного кримінального законодавства як державна зрада або шпигунство (ст.ст. 111 та 114 Кримінального кодексу України [211]).

Серед прикладів, зокрема, можна навести атаки з боку груп APT28, APT29, що здійснювали фішингові кампанії проти Міністерства закордонних справ, Збройних Сил України, Уряду України [274].

Масовані DDoS-атаки (Distributed Denial of Service), розподілені на відмову в обслуговуванні, унеможливлюють доступ до офіційних сайтів органів влади, блокують державні сервіси, створюють інформаційний хаос [275]. У контексті воєнного стану – це загроза не лише технічна, а й політична, оскільки може паралізувати мобілізаційні процеси, електронне управління, повідомлення населення про евакуацію тощо.

Щодо прикладів, зокрема, можна зазначити про масовані атаки на «Дію», сайти Кабінету Міністрів України, Верховної Ради України, Міністерства оборони України у лютому-березні 2022 р.

Інформаційно-психологічні операції -- це найскладніша для ідентифікації форма кіберзагроз, адже полягає не лише в технічному зламі, а й в маніпуляції свідомістю громадян через фейки, дезінформацію, бот-атаки, провокації в соціальних мережах [276].

Такі операції активно поєднуються з воєнними подіями (наприклад, перед наступом чи під час окупації територій) і мають на меті: посіяти паніку; дискредитувати командування Збройних сил України або керівництво держави; створити внутрішньополітичну дестабілізацію.

У цьому контексті слід зазначити про типові ознаки таких операцій, зокрема: поширення фейкових інтерв'ю, згенерованих штучним інтелектом; спроби кібератак на платформи телеканалів для трансляції дезінформації; спроби формування масового відчаю та навмисного поділу українців на «своїх» та «чужих»; створення оманливого ефекту про надзвичайну могутність ворога; розвідку даних, що можуть бути корисними для ворога; звернення до особистості як переконливого аргументу; знецінення офіційних джерел інформації та залучення псевдоекспертів; дискредитація України на міжнародній арені. Важливо зауважити, що синхронність публікацій, а також фактичні, логічні, мовні помилки та нереальність так званих авторів таких матеріалів також є маркерами подібних інформаційно-психологічних операцій [277].

Щодо практичних кейсів з досвіду України після 2014 р. та з початку повномасштабного вторгнення 2022 р., то починаючи з 2014 р., Україна стала полігоном для тестування нових форм кіберагресії, про що свідчить низка масштабних атак.

BlackEnergy (2015) – атака на енергетичну інфраструктуру, що вперше в історії спричинила фізичне відключення електроенергії через кіберінструменти [278]. NotPetya (2017) – руйнівна кібератака на урядові й приватні системи, визнана в США та Великій Британії актом кібервійни з боку рф [279]. WhisperGate та HermeticWiper (2022) – віруси-шкідники, що мали на меті знищення інформації в урядових системах у переддень вторгнення [280]. У період 2023-2024 рр. зафіксовано нові форми кіберагресії проти України, зокрема: спроби несанкціонованого доступу до систем управління безпілотними апаратами, а також кібератаки на підприємства, пов'язані з логістикою й виробництвом дронів [281-282]. Відкриті джерела Державної служби спеціального зв'язку та захисту інформації України також повідомляють про злами акаунтів, пов'язаних з державними установами та посадовими особами [283].

Наведені кейси підтверджують, що кібератаки в умовах війни мають не лише підтримуючий, а стратегічний характер, і можуть виконувати функції артилерійської підготовки, дезорієнтації, маскування або знищення критично важливих інформаційних вузлів.

Також важливо зазначити, про унікальність взаємодії державних і недержавних суб'єктів у протидії кіберзагрозам в Україні полягає в тому, що у відповідь на масштаб кіберзагроз склалася гібридна система захисту, що включає як офіційні державні органи, так і громадські ініціативи, волонтерські хакерські об'єднання, експертне середовище.

У цьому контексті до державних суб'єктів доцільно віднести: Службу безпеки України, що реагує на кібератаки проти державних органів, координує зусилля в кіберконтррозвідці; Державну службу спеціального зв'язку та захисту інформації України, що забезпечує криптографічний та технічний захист державних ІТ-систем; Збройні сили України та Міноборони, що створюють підрозділи кіберзахисту та кібероперацій; Міністерство цифрової трансформації, що координує державну політику у сфері цифрової безпеки.

До недержавних суб'єктів доцільно віднести: ІТ-армію України, що є волонтерським угрупування, котре виконує активні дії у відповідь, атакуючи російські сайти, інфраструктуру, банківські системи [284]; Кіберальянс, «Рух Опору Капітуляції», «Кіберпартизан» – групи, що здійснюють як оборонні, так і наступальні операції [285]; Приватний ІТ-сектор, що надає сервери, фахівців, ресурси для захисту [286].

Слід зазначити, що така синергія є новим феноменом у міжнародному праві, що викликає численні питання: про легітимність приватних кібератак, відповідальність суб'єктів, міжнародно-правовий статус кіберопору, котрі мають бути врегульовані у майбутньому.

Україна наразі перебуває у центрі глобального процесу еволюції концепції кібербезпеки в умовах війни. Загрози набули багатовекторного характеру: від технічного знищення інфраструктури – до маніпуляції суспільною свідомістю. Така ситуація вимагає нової якості правового регулювання, чіткої відповідальності суб'єктів і інституційного посилення як на національному, так і міжнародному рівні.

Правове регулювання кібербезпеки в Україні в умовах воєнного стану ґрунтується на низці законів, указів, рішень, що адаптують мирні правові норми до надзвичайних умов. Воєнний стан як особливий правовий режим вводиться за

Законом України «Про правовий режим воєнного стану» [197] і відповідними указами Президента України [287], котрі відповідно до положень Конституції України підлягають затвердженню Верховною Радою України [201]. Зазначене створює законодавчу підставу для тимчасового розширення повноважень державних органів, обмеження прав і свобод, необхідних для захисту держави.

Аналіз режиму воєнного стану свідчить, що такі норми як право на таємницю листування чи телефонних переговорів, на інформаційну приватність, право формувати інформацію тощо можуть бути обмежені або регульовані особливим порядком, коли це необхідно для кібербезпеки. Обмеження мають бути законними, пропорційними, здійсненими у межах компетенції визначених органів. Зокрема, Закон України «Про правовий режим воєнного стану» [197] і Указ Президента України «Про введення воєнного стану в Україні» [287] дають правове підґрунтя для втручання держави у інформаційні комунікації, але законодавець встановлює, що це може здійснюватись тільки в межах, передбачених законом, та з урахуванням прав людини.

Повноваження органів державної влади у сфері кіберзахисту в умовах воєнного стану чітко розмежовані, хоча існують випадки, коли межі між повноваженнями органів перекриваються, що створює ризики для юридичної визначеності. Основні суб’єкти – Служба безпеки України, Державна служба спеціального зв’язку та захисту інформації, Міністерство цифрової трансформації, Міністерство оборони, Генеральний штаб, Урядова команда реагування на комп’ютерні надзвичайні події України CERT-UA та інші уповноважені підрозділи. Служба безпеки України має право вести кіберконтррозвідку, розслідувати кібершпигунство, кібератаки проти державних об’єктів; Державна служба спеціального зв’язку та захисту інформації відповідає за технічний захист, криптографію, безпечний зв’язок державних органів, об’єкти критичної інфраструктури. Міністерство оборони і Збройні сили України забезпечують захист систем оборонного призначення, кібероперацій у сфері оборони. При цьому законодавство України, зокрема Закон «Про основні засади забезпечення кібербезпеки України» [205], закріплює ці повноваження і дає нормативну базу для взаємодії між суб’єктами.

Особливою складністю є застосування міжнародного гуманітарного права до кібервійн. На міжнародному рівні спеціального універсального договору щодо кіберзбройних конфліктів наразі немає, але Україна користується вже наявними нормами міжнародного гуманітарного права, зокрема принципами розрізнення, пропорційності, гуманності, захисту цивільного населення [288].

Водночас практика застосування цих принципів у кіберпросторі ставить перед державами безпрецедентні виклики правозастосування. Так, традиційно положення міжнародного гуманітарного права базуються на матеріальній площині збройного конфлікту, що має фізичний вимір. Кібервійна ж, на відміну від кінетичних дій, відбувається у сфері, де межа між цивільними і військовими об'єктами часто розмита. Багато цифрових платформ, що мають критичне значення для безпеки держави, водночас є комерційними або належать приватному сектору. Тому розрізнення між правомірною ціллю та об'єктом, що перебуває під цивільним захистом, у кіберпросторі часто є неможливим без розробки нових нормативних критеріїв. Це ставить завдання подальшої доктринальної розробки jus in bello у контексті цифрових конфліктів, а також вимагає більшого залучення держав до формування загальновизнаних правил поведінки у кіберсфері під час війни.

Практика Талліннського мануалу 2.0, доктринальні позиції міжнародних експертів визнають, що кібератаки, котрі спричиняють руйнування фізичної інфраструктури, жертви серед цивільного населення або значні порушення життєдіяльності населення, можуть кваліфікуватись як атаки, що підпадають під норму jus in bello [371]. Водночас питання атрибуції, відповідальності держави, а також нормативного закріплення статусу кібероперацій як складової воєнних дій є предметом дискусій у науковій і правозастосовній практиці [289].

Щодо національних норм, ключовим нормативним актом є Закон України «Про основні засади забезпечення кібербезпеки України» (2017). Він визначає об'єкти кібербезпеки, суб'єкти, принципи, загальні засади, обов'язки органів державної влади та інших учасників, систему реагування на кіберінциденти. Крім того, значущим є Закон України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану»

(2022), що розширює кримінально-правові засоби реагування на кібератаки й інші злочини в кіберпросторі [290]. Також Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» (1994) встановлює вимоги до інформаційних систем, їх безпеки, стандартів [265].

Постанови уряду, рішення Рада національної безпеки і оборони України, укази Президента України доповнюють законодавчу базу. Наприклад, Указ Президента «Про Стратегію кібербезпеки України» регламентує у стратегічному аспекті інституційні, технічні, організаційні заходи з кіберзахисту [264]. Окремі постанови передбачають обов'язок операторів критичної інфраструктури провадити відповідну сертифікацію, звітування про кіберінциденти, дотримуватися підвищених вимог щодо захисту зв'язку і інформаційних систем.

Утім, важливо зазначити, що не зважаючи на наявність цих нормативних підстав, правове регулювання у цій сфері має суттєві недоліки. По-перше, багато норм ухвалені до початку повномасштабного вторгнення і не враховують сучасного масштабу кіберзагроз та агресії. По-друге, залишається відкрите питання відповідальності за кібератаки, що здійснюються з території держави-агресора або через проксі-структури: законодавство не завжди визначає, яким чином ці злочини кваліфікуються – як злочини проти нацбезпеки, воєнні злочини, тероризм чи інші категорії. По-третє, існують проблеми з координацією між суб'єктами та з обов'язковими аспектами приватного сектору; деякі об'єкти критичної інфраструктури не мають достатніх правових стимулів чи санкцій у разі невиконання нормативів. По-четверте, законодавство часто не забезпечує достатньої прозорості чи доступності процедур реагування на кіберінциденти, зокрема в частині залучення наукових та експертних спільнот.

Зазначимо, що правове регулювання кібербезпеки в умовах воєнного стану в Україні має значну законодавчу основу, включно з ключовими законами, стратегічними документами та спеціальними змінами (наприклад, у Кримінальному кодексі України). Однак існує потреба у цілеспрямованій модернізації, зокрема в кодифікації норм, адаптації до умов електронної та кібер-війни, встановленні чітких

процедур визначення ступеня відповідальності за кібератаки, і забезпеченні балансу між безпекою та правами людини.

Окрему увагу слід приділити проблемам та викликам у сфері забезпечення кібербезпеки під час воєнного стану. Так, з початку широкомасштабної агресії проти України кіберпростір перетворився на повноцінний фронт, що вимагає відповідної нормативної, інституційної та оперативної реакції держави. Втім, аналіз чинного законодавства та правозастосовної практики свідчить про наявність серйозних викликів і проблемних вузлів у сфері забезпечення кібербезпеки в умовах воєнного стану. Йдеться не лише про окремі тактичні труднощі, але про системні вади, що підривають здатність держави ефективно протидіяти кіберагресії та забезпечувати належний рівень кіберзахисту критичних об’єктів, державного управління й інформаційного суверенітету загалом.

Одна з ключових проблем – це нормативна фрагментарність і колізійність у законодавчому полі. Закон України «Про основні засади забезпечення кібербезпеки України» (2017) формально визначає засади кібербезпеки, однак навіть після кількох оновлень у 2022-2024 рр. він не враховує комплексно специфіку умов воєнного стану. Зокрема, у законі відсутні чіткі норми щодо: особливого режиму функціонування суб’єктів забезпечення кібербезпеки в умовах війни; правового статусу добровольчих кібервійськ, котрі де-факто беруть участь у бойових операціях в кіберпросторі; режиму правового реагування на масштабні кібератаки, що є складовою воєнної агресії відповідно до ст. 51 Статуту ООН [275; 378].

Існують й міжгалузеві колізії, зокрема Кримінальний кодекс України у ст.ст. 361–363-1 описує окремі кіберзлочини [211], проте не охоплює всіх типів шкідливої кібердіяльності, що використовується під час гібридної війни – таких як інформаційно-психологічні атаки, масове розповсюдження deepfake, порушення інформаційної цілісності баз даних органів влади. Законодавство також не містить ефективного механізму швидкої юридичної кваліфікації кібератаки як акту збройної агресії чи міжнародного злочину.

Також особливої актуальності набуває проблема правової кваліфікації деструктивного цифрового впливу на громадську думку, політичні процеси та

психічне здоров'я населення. У сучасному міжнародному праві відсутні чіткі категорії для інформаційно-психологічних кібероперацій, що призводять до стратегічної дестабілізації без прямої фізичної шкоди. Застосування аналогій із категоріями «пропаганди війни» чи «розпалювання ворожнечі» є недостатнім. В умовах воєнного стану необхідно ініціювати кодифікацію понять, що відображають цифрові методи дестабілізації: «когнітивна атака», «психоцифрова зброя», «інформаційне насильство» тощо. Їх правове визначення дозволить формувати доктрину інформаційної безпеки на рівні, що відповідає характеру гібридних загроз XXI століття.

Окрему проблему становить відсутність кодифікованого підходу до класифікації кіберінцидентів за рівнем загрози національній безпеці. Це призводить до невизначеності у діях суб'єктів, неузгодженості між цивільним і військовим сегментами системи реагування.

Важливо зазначити про наявність низки інституційних проблем. Попри те, що чинне законодавство (зокрема Закон № 4336-IX від 27.03.2025 [291] та Постанова Кабінету Міністрів України № 299 від 04.04.2023 [292]) визначає повноваження основних суб'єктів національної системи кібербезпеки (Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації України, Міністерства цифрової трансформації України, Збройних Сил України, CERT-UA тощо), а також встановлює порядок реагування на кіберінциденти, обміну інформацією та координації їх дій, на практиці зберігається ризик дублювання функцій, нечіткості процедур взаємодії або недостатньої координації в умовах кризових ситуацій, зокрема під час воєнного стану. Крім того, відсутнє належне правове регулювання участі недержавних суб'єктів, зокрема волонтерських IT-формувань і приватного сектору, у спільних заходах кіберзахисту, що створює потенційні прогалини у відповідальності, контролі та підзвітності.

Це зумовлює потребу в подальшій кодифікації процедур передачі повноважень, узгодженні функцій суб'єктів та формалізації механізмів державно-приватної взаємодії у сфері кібербезпеки, особливо в умовах воєнного стану.

До прикладу, Державна служба спеціального зв'язку та захисту інформації України здійснює функції технічного захисту інформації, однак під час воєнних дій значна частина відповідальності переходить до військових формувань, не завжди узгоджених із цивільним сегментом [293].

Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, котра номінально є координаційним центром реагування на кіберінциденти, обмежена у спроможності координувати дії за участю військових структур та добровольчих ІТ-груп [294]. Отже, існує потреба ефективного усунення ризиків суперечностей повноважень, невизначеності в умовах воєнного стану і потенційного «вакууму» для недержавних ІТ-формувань.

В умовах збройного конфлікту особливо гостро виявляються системні проблеми у сфері кібербезпеки, зокрема – обмеженість матеріально-технічної бази державного сектору. Значна частина державних установ не має належно розвиненої інфраструктури резервного зберігання даних (дата-центрів), комплексних систем виявлення та реагування на кіберінциденти (IDS/IR), а також технологій криптографічного захисту, адаптованих до умов воєнного часу [295].

Слід зауважити, що проблема технічної спроможності держави у сфері кіберзахисту нерозривно пов'язана із рівнем технологічного суверенітету. Залежність від закордонних платформ, відсутність вітчизняних рішень у сфері зберігання, шифрування, аналізу даних – це не лише питання інфраструктури, а й національної безпеки. В умовах воєнного стану технічна автономність кіберпростору держави має розглядатись як стратегічний актив. Формування «національного цифрового щита» потребує докорінного переосмислення підходів до державно-приватного партнерства, належного фінансування у сфері цифрових технологій оборонного призначення, а також впровадження системи інституційних преференцій для компаній, що працюють у сфері «цифрової оборонної промисловості».

Окремою проблемою залишається кадровий дефіцит у сферах кіберзахисту критичної інфраструктури, цифрової розвідки та інженерної кібероборони. Масова релокація та міграція фахівців у сфері ІТ після початку повномасштабної агресії рф суттєво послабила кадровий потенціал України у сфері кібербезпеки [296; 389].

У 2023 р. в Україні започатковано процес формування кіберсил у складі Збройних Сил України як окремого структурного елементу сектору безпеки та оборони. Йдеться про розробку нормативно-правової бази, концепції їхнього функціонування та механізмів легітимізації кібероперацій, що здійснюються в інтересах оборони держави [297].

Ще одним гострим питанням є недостатня ефективність системи притягнення до відповідальності за кіберзлочини, особливо ті, що здійснюються під час воєнного стану та мають воєнно-політичну природу. Відсутність міжнародно визнаного механізму атрибуції кібернападів ускладнює правову ідентифікацію суб'єктів злочину [291; 298]. Зокрема, коли атаки проводяться через проксі-сервери, ботнети, підставні компанії, або «приватні» хакерські групи під контролем держави-агресора.

Кримінальний процесуальний кодекс України не має окремого порядку збору цифрових доказів під час війни, що ускладнює документування та судове переслідування кібератак [299-300]. Так, умови воєнного часу потребують спеціального статусу доказів, здобутих у бойовій обстановці, у тому числі – у співпраці з іноземними структурами (The NATO Cooperative Cyber Defence Centre of Excellence, EUROPOL та іншими CERT).

Окрім того, не вирішене питання відповідальності учасників добровольчих кібервійськ, що діють на боці України. Їх правовий статус у національному праві є невизначеним [293]: вони не є військовослужбовцями, але можуть здійснювати втручання у цифрові системи противника. Це створює потенційні ризики як для правової захищеності самих учасників, так і для України як держави – в контексті дотримання міжнародного права.

Щодо міжнародно-правового аспекту та статусу кібератак: на сьогодні немає спеціального (універсального) міжнародного договору, що прямо регулює кібератаки в умовах збройного конфлікту. Україна, котра стала жертвою кіберзбройної агресії, опинилася у ситуації, коли змушена формувати власне правове розуміння застосування норм jus ad bellum та jus in bello до кібероперацій, спираючись на існуючі норми міжнародного права (Статут ООН, міжнародне гуманітарне право) та на висновки юридичних експертів, зокрема у рамках Tallinn Manual 2.0 від

Об’єднаного центру передових технологій з кібероборони НАТО (Cooperative Cyber Defence Centre of Excellence) [301].

Згідно з Талліннським мануалом 2.0, що є найавторитетнішим джерелом з цього питання, кібератака може бути визнана «застосуванням сили» (use of force) або навіть «збройним нападом» (armed attack), якщо вона викликає наслідки, співмірні з фізичним нападом – людські жертви, руйнування критичної інфраструктури, тощо [266]. Відповідно, така атака може дати державі право на самооборону згідно зі ст. 51 Статуту ООН [272].

Однак питання залишається відкритим щодо: критеріїв правової атрибуції кібератаки державі-агресору; стандарту доказування участі державних органів в атаці; статусу відповідальності за кібератаку в системі міжнародної кримінальної юстиції.

Станом на 2025 р., Україна веде активну роботу у цьому напрямі, зокрема через державну політику у сфері кібербезпеки [291], ініціювання проваджень у Міжнародному кримінальному суді, використання доказів кібератак у матеріалах трибуналу щодо воєнних злочинів, а також у співпраці з Європейським центром протидії гібридним загрозам [303].

Слід зазначити, що проблема кібербезпеки в умовах воєнного стану в Україні є комплексною, багатовимірною і глибоко вкоріненою як у правовій, так і в інституційній площинах. Необхідність реформування нормативної бази, посилення координації між суб’єктами, адаптації процедур до умов війни та активної участі в міжнародному правотворенні у сфері кіберправа є актуальними завданнями для української держави в умовах триваючої гібридної агресії.

Стосовно перспектив удосконалення правового механізму кібербезпеки у період воєнного стану, то у контексті сучасної війни проти України, що ведеться зокрема в інформаційному та кіберпросторі, правове забезпечення кібербезпеки потребує глибокої трансформації. Воєнний стан відкрив низку критичних прогалин, котрі за мирного часу не були настільки очевидними. У зв’язку з цим актуалізується завдання не просто оновлення наявного законодавства, а його адаптації до умов

збройного конфлікту з урахуванням міжнародних стандартів, сучасних технологій і специфіки гібридної агресії.

Чинне законодавство у сфері кібербезпеки в Україні залишається орієнтованим на мирний період і не передбачає достатньої деталізації правових режимів у період збройного конфлікту. Насамперед, вимагає перегляду Закон України «Про основні засади забезпечення кібербезпеки України» (2017), зокрема в частині: запровадження спеціального режиму кібербезпеки в умовах воєнного стану; чіткого регулювання повноважень добровольчих ІТ-формувань (так званих кібервійськ); уточнення алгоритмів реагування на масштабні кібератаки в реальному часі; нормативного закріплення категорій «кіберагресія», «кібервійна», «кібертероризм» тощо.

Слід також внести зміни до законодавства про національну безпеку, правовий режим воєнного стану, кримінального та кримінального процесуального законодавства – для забезпечення процесуальної гнучкості в умовах воєнного часу, зокрема щодо збору доказів у кіберпросторі, транснаціональної співпраці в кримінальному провадженні та визнання цифрових доказів, отриманих у межах спільних кібероперацій з міжнародними партнерами.

З огляду на наміри України щодо євроатлантичної інтеграції, одним із пріоритетів є гармонізація національного законодавства з підходами, прийнятими в країнах-членах НАТО та ЄС. Серед найважливіших практик, що потребують запозичення та адаптації: модель «повного циклу кіберзахисту» (prevention–detection–response–recovery), що закріплена в директивах ЄС (зокрема NIS2 Directive 2022/2555); система обов'язкового повідомлення про кіберінциденти, що передбачає відповідальність за недекларування (як у GDPR та NIS2); інституційна модель «єдиного національного кіберкоординатора», що забезпечує міжвідомчу узгодженість; підхід до публічно-приватного партнерства, як механізму інтеграції потенціалу приватного сектору у національну систему кібербезпеки.

Україна має позитивний досвід міжнародної співпраці у сфері кібербезпеки, зокрема як учасник-спостерігач (contributing participant) у Кооперативному центрі кібероборони НАТО (NATO Cooperative Cyber Defence Centre of Excellence) [304]. Окрім того, українські установи беруть участь у проектах програми Horizon Europe,

зокрема в межах кластеру «Цифрові технології, промисловість та космос» [305]. Проте ці зусилля залишаються фрагментованими і потребують нормативного закріплення на національному рівні — зокрема, через необхідність повної гармонізації українського законодавства з Директивою ЄС NIS2 і імплементації положень нової європейської рамкової політики з кіберзахисту (Cyber Resilience Act [306] та інших суміжних актів) для забезпечення одного підходу до безпеки цифрової інфраструктури, критичних інформаційних систем та реагування на кіберінциденти.

Щодо посилення нормативного забезпечення взаємодії між суб'єктами забезпечення кібербезпеки, то інституційна фрагментарність у сфері кібербезпеки, особливо в умовах воєнного стану, є серйозним ризиком. Проблема не стільки в кількості суб'єктів, скільки в недосконалості нормативного механізму взаємодії між ними. Сьогодні взаємодія часто здійснюється в ручному режимі, через міжвідомчі домовленості, а не на підставі стабільних регламентованих процедур.

Потребує оновлення модель управління інцидентами. На рівні підзаконних актів має бути встановлений єдиний протокол реагування на інциденти – із визначенням відповідального координатора, обов'язковим інформуванням Урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA, відповідальністю за неналежне реагування.

Також слід передбачити правову модель взаємодії з недержавними структурами (зокрема, «ІТ-Армією України»), що сьогодні здійснює численні операції, але без чіткого нормативного статусу. У цьому контексті доцільно розробити спеціальний закон про участь цивільних осіб у забезпеченні кібербезпеки в умовах збройного конфлікту.

Окремо слід зазначити про використання штучного інтелекту та новітніх технологій для зміцнення кіберзахисту. Реалії війни довели, що протидія кіберагресії без залучення штучного інтелекту, машинного навчання, хмарних технологій, квантового шифрування стає дедалі менш ефективною. Не зважаючи на певні кроки у цій сфері [307], в українському законодавстві, станом на вересень 2025 р., відсутні правові норми, що регулюють: застосування штучного інтелекту в системах моніторингу кіберзагроз; відповідальність за дії автономних цифрових агентів;

правовий статус технологій, що використовують автоматизовану обробку персональних даних у сфері оборони.

Потребує комплексного правового опрацювання й питання кібербезпеки в умовах використання систем dual-use (тобто тих, що одночасно мають цивільне і військове застосування) [308], адже значна частина рішень, що застосовуються в оборонній сфері, розроблені приватним сектором (наприклад, системи аналітики трафіку, програмне забезпечення на базі штучного інтелекту, інструменти Open Source Intelligence). Водночас, приватний сектор відіграє значну роль у розробці технологій для оборонної сфери, а нормативні рамки для подібних технологій (особливо тих, що мають dual-use характеристики) поки що не комплексно прописані [309].

Важливо, що на практиці саме приватний сектор часто є джерелом найсучасніших цифрових технологій, котрі потім адаптуються для військового застосування. У цьому контексті вкрай необхідне запровадження чітких нормативних правил для технологій подвійного призначення, включно з реєстром таких технологій, механізмами ліцензування, умовами експортного контролю та відповідальності у випадку неналежного використання. Така правова рамка має забезпечити баланс між інноваційною свободою приватного сектору та безпековими інтересами держави. Крім того, це дозволить інтегрувати Україну у транснаціональні ланцюги постачання технологій для кібероборони в рамках євроатлантичних структур.

На перспективу доцільно ухвалити окремий закон «Про національну стратегію застосування штучного інтелекту в сфері безпеки і оборони», в котрому було б передбачено як етичні, так і правові засади його використання.

У контексті удосконалення міжнародного співробітництва, міжнародна правова система кібербезпеки перебуває на етапі становлення. Відтак Україна має не лише адаптувати своє законодавство до стандартів Європейського Союзу та НАТО у процесі євроатлантичної інтеграції, а й активно впливати на формування глобальних нормативних підходів. Зокрема, важливо: ініціювати в рамках ООН питання юридичного визначення терміна «кіберагресія»; брати участь у розробці

міжнародних конвенцій щодо регулювання кібероперацій у збройних конфліктах; укладати дво- та багатосторонні угоди про співробітництво у сфері реагування на кіберзагрози; забезпечити поступову інтеграцію України до системи кібероперацій НАТО, зокрема до NATO Cyber Operations Centre – структурного підрозділу, відповідального за моніторинг, аналіз і реагування на кіберзагрози в межах оперативного командування Альянсу [310]; а також налагодити сталі канали взаємодії з Агентством ЄС з кібербезпеки (European Union Agency for Cybersecurity) – інституцією, що координує політику ЄС у сфері кіберзахисту [311].

Національне законодавство повинно враховувати ці вектори і містити положення щодо міжнародної взаємодії як повноцінної складової системи національної кібербезпеки. Особливо важливо закріпити можливість інтегрованого використання іноземного досвіду, технічних засобів, спільного аналізу цифрових загроз, зокрема у режимі воєнного часу.

Також слід зауважити, що в умовах воєнного стану й активного розвитку цифрових інструментів оборони постає необхідність забезпечення належного громадського контролю та прозорості діяльності держави у сфері кібербезпеки. Попри наявність обмежень, зумовлених специфікою війни, принципи відкритості, підзвітності та участі громадянського суспільства не втрачають своєї актуальності, а навпаки – набувають нового змісту.

Важливо, що навіть в умовах воєнного чи надзвичайного стану принципи демократичного врядування вимагають збереження базових механізмів прозорості та підзвітності у сфері кібербезпеки. Водночас аналіз національного законодавства та практики свідчить про суттєвий дефіцит ефективного громадського контролю за діяльністю органів публічної влади у цифровому середовищі. Така ситуація становить ризик як для правового балансу між безпекою та правами людини, так і для легітимності державної політики у сфері кіберзахисту. З огляду на це, потребує розвитку нормативна модель взаємодії держави з громадянським суспільством у сфері цифрової безпеки, включаючи механізми публічної звітності, експертної оцінки, а також можливості для інституційної участі незалежних фахівців у розробці кіберстратегій.

Як слушно зазначає Л. Наливайко, прозорість є ключовим демократичним стандартом функціонування державної влади, зокрема в контексті доступу до інформації, що не становить державної таємниці, але є суспільно значущою у сфері безпеки [67]. У цьому аспекті, принцип публічності та відкритості в діяльності інституцій, відповідальних за кібербезпеку, має бути збережено навіть за умов обмеженого доступу – через механізми громадського моніторингу, незалежного аудиту та залучення правозахисних організацій.

Важливо, що огляду на дослідження українських правозахисників, недержавні організації відіграють важливу роль у забезпеченні балансу між безпекою і правами людини в цифровому просторі, особливо в контексті зростання державного контролю за комунікаційними каналами [68]. Як підкреслює Л. Наливайко, право на доступ до публічної інформації має розглядатись не лише як інструмент забезпечення прав громадян, але і як механізм демократичного контролю за діяльністю держави, зокрема у сферах, що традиційно вважаються «закритими» [66].

Так, створення ефективного правового режиму кібербезпеки в умовах збройного конфлікту має спиратись не лише на нормативне оновлення, але й на вироблення нової правової філософії, в основі якої – адаптивність, випереджувальне регулювання, системне мислення. Традиційна реактивна модель права, орієнтована на фіксацію вже вчинених правопорушень, у кіберпросторі втрачає ефективність. У цьому контексті, доцільним є перехід до моделі anticipatory regulation, що передбачає здатність нормативної системи передбачати ризики, формувати архітектуру превентивних заходів і встановлювати «правові сигнали» для суспільства та бізнесу щодо меж допустимої поведінки в умовах кіберконфлікту.

Отже, формування правового режиму кібербезпеки у воєнний період повинно відбуватись з урахуванням необхідності збереження основоположних демократичних принципів – прозорості, підзвітності та залучення громадянського суспільства до процесів прийняття рішень, моніторингу ефективності державної політики та контролю за дотриманням прав людини у цифровій сфері.

Проведений аналіз дає підстави зробити такі висновки:

1. Кібербезпека в умовах воєнного стану є системоутворюючою складовою інформаційної безпеки держави, що поєднує правові, організаційні та політичні інструменти захисту. У період збройної агресії вона трансформується зі сфери технічного захисту інформації у сферу стратегічного управління безпекою, стаючи засобом протидії інформаційно-психологічним операціям противника та забезпечення стійкості державного управління.

2. Нормативно-правова та інституційна система кібербезпеки України побудована переважно за моделлю мирного часу і не враховує специфіку воєнного стану. Відсутність правового режиму для діяльності добровольчих кібервійськ, процедур оперативної взаємодії державних і приватних суб'єктів, а також кодифікованих понять як «кіберагресія», «інформаційно-психологічна атака» ускладнює ефективне реагування на загрози. Необхідне нормативне оновлення системи кіберзахисту з урахуванням умов збройної агресії та інтеграція механізмів державно-приватного партнерства.

3. Міжнародно-правовий режим кібероперацій у період війни залишається невизначеним: відсутні універсальні норми, котрі б однозначно встановлювали правову кваліфікацію кібератак як акту агресії чи збройного нападу. Недостатня розробленість питань атрибуції та правового статусу добровольчих кібервійськ зумовлює прогалини у визначенні відповідальності сторін і меж реалізації права на самооборону держави.

4. Кримінально-процесуальні аспекти кібербезпеки у воєнний час не мають спеціального правового режиму збору, фіксації й використання цифрових доказів. Відсутність уніфікованих процедур міжнародного співробітництва перешкоджає легітимному обігу таких доказів між партнерами та обмежує можливості ефективного розслідування кіберзлочинів, пов'язаних з агресією.

5. Технологічна спроможність держави в умовах воєнного стану визначається рівнем її цифрового суверенітету. Залежність від іноземних рішень, нестача вітчизняних криптографічних технологій і кадровий дефіцит у сфері кіберзахисту формують критичні вразливості оборонного потенціалу. Тому

необхідним є нормативне закріплення принципу технологічного суверенітету як складової національної безпеки.

6. Баланс між забезпеченням кібербезпеки та дотриманням прав людини у період воєнного стану має ґрунтуватися на принципах пропорційності, підконтрольності та тимчасовості обмежень. Відсутність ефективного парламентського й громадського контролю за діяльністю органів кібербезпеки створює ризики зловживань. Необхідне правове закріплення механізмів незалежного моніторингу та залучення громадянського суспільства до формування політики кібербезпеки без шкоди для оборонних інтересів.

7. Серед ключових напрямів нормативних та інституційних реформ слід виокремити: 1) розробку та прийняття спеціального закону або розділу в законі про національну безпеку, що визначав би правові режими кібербезпеки під час воєнного стану (повноваження, статус учасників, порядок реагування, відповідальність); 2) кодифікацію й введення у правову систему чітких категорій кіберзагроз (кіберагресія, кібертероризм, когнітивні атаки тощо) із відповідними кваліфікаціями та санкціями; 3) законодавче врегулювання діяльності добровольчих кібервійськ: їх легалізацію, правовий статус, межі діяльності, відповідальність, взаємодію з державними структурами; 4) формування єдиного кіберкоординатора або національного центру кібербезпеки з широкими повноваженнями координації, контролю й оперативного реагування, що має бути законодавчо закріплений; 5) удосконалення процедур реагування у контексті введення єдиного протоколу інцидент-менеджменту (виділення відповідального, етапи реагування, інформування, контроль), обов’язкове повідомлення про інциденти, санкції за неналежне реагування; 6) ефективну інтеграцію міжнародних стандартів і практик (NIS2, GDPR, Талліннський мануал 2.0, стандарти НАТО) у національне законодавство, з урахуванням особливостей воєнного стану; 7) підтримку розвитку національного технологічного суверенітету, зокрема стимулювання державного- приватного партнерства в оборонному ІТ-секторі, створення преференційних умов для розробників кібероборони, системи експортного контролю для технологій подвійного призначення; 8) підсилення кадрового потенціалу, що передбачатиме створення програм із підготовки,

перепідготовки фахівців кіберзахисту, збереження фахівців у державному секторі через адекватні стимули, гранти, систему кар'єрного росту; 9) впровадження спеціального режиму цифрових доказів в умовах воєнного стану, стандартів атрибуції, угод про міжнародне співробітництво у зборі і визнанні кібердоказів, врегулювання використання доказів іноземним партнерам.

2.4. Забезпечення інформаційного суверенітету в умовах воєнного стану: проблеми, тенденції та перспективи

Інформаційна безпека та інформаційний суверенітет є ключовими напрямами державної політики у воєнний і післявоєнний періоди. В умовах збройної агресії рф проти України, забезпечення інформаційного суверенітету і безпеки набуває стратегічного значення.

Інформаційний простір України вражений масштабними інформаційно-психологічними операціями противника, дезінформацією, кібератаками на критичну інформаційну інфраструктуру, посяганнями на персональні дані громадян тощо. Захист національного інформаційного простору від зовнішніх і внутрішніх інформаційних загроз, гарантування інформаційної безпеки та інформаційного суверенітету стають чинниками функціонування України як суверенної та незалежної держави [214, с. 190; 379]. Ефективна інформаційна діяльність може суттєво поліпшити зусилля держави щодо мирного вирішення кризових ситуацій. І навпаки, ігнорування інформаційних чинників, а часто й навмисне змінена інформація здатні спровокувати найрадикальніші настрої, спалахи ворожості та призвести до катастрофічних наслідків. Застосування інформаційних технологій військовими відкрило нові можливості щодо забезпечення оборони держави. Володіння інформаційними ресурсами та його захист у військовій сфері стали таким самим неодмінним атрибутом, як озброєння, боєприпаси, транспорт тощо [312, с. 23]. Крім того, розвиток глобальних цифрових технологій, соціальних мереж і штучного інтелекту, хмарного зберігання даних створює нові ризики для інформаційного

суверенітету. В таких умовах слід визнати, що ймовірність повноцінно забезпечити захист інформаційного суверенітету України є ілюзорною.

Загалом, забезпечення інформаційного суверенітету під час дії воєнного стану є надскладним завданням, що передбачає захист інформаційного простору України [120], гарантування його стійкості та невразливості в умовах відсічі воєнної агресії рф.

Все це обумовлює пошук стратегічних напрямів посилення ефективності забезпечення інформаційного суверенітету в Україні в умовах воєнного стану.

Інформаційний суверенітет держави розглядали у своїх наукових дослідженнях такі вчені, як: О. Баранов, М. Бліхар, І. Боднар, А. Бурбій, В. Гапотій, В. Горовий, О. Довгань, Д. Дубов, К. Ісмайлов, В. Ковтун, Б. Кормич, М. Ожеван, С. Оніщенко, Н. Пархоменко, В. Пилипчук, А. Правдюк, А. Селіванов, О. Скрипнюк, В. Супрун, О. Солодка, В. Тернавська, Т. Ткачук, О. Троянський, О. Федченко, О. Юдін, О. Ярема та ін. Однак, проблематика забезпечення інформаційного суверенітету є динамічною. Швидкі темпи розвитку інформаційних відносин, процесів та технологій обумовлюють нові виклики та загрози для інформаційного суверенітету України в умовах воєнного стану. Отож, науковий пошук напрямів його забезпечення не втрачає актуальності.

Забезпечення інформаційного суверенітету – це комплексне завдання, що має політико-правовий, соціально-економічний, культурний, технологічний, інституційний, організаційний та безпековий виміри. Кожна з цих складових має розвиватись в рамках єдиного цілісного механізму. При цьому, правова основа повинна створювати якісне підґрунтя для формування та реалізації державної політики у кожній зазначеній сфері. Правова рамка інформаційного суверенітету має бути на скільки ефективною, щоб його стабільне гарантування було реальним.

Правнича наука та юридична практика сприймають інформацію як статичний об’єкт, але технічні науки доводять, що її слід розглядати як динамічне явище, як процес. Ця концептуальна розбіжність призводить до того, що правові інструменти іноді не сприяють вирішенню поточних проблем і є малоефективними для забезпечення інформаційного суверенітету в умовах швидкого розвитку цифрових

технологій. Нормативно-правова основа забезпечення інформаційного суверенітету потребує оновлення в контексті реалій воєнного стану та глобальних інформаційних процесів.

Отож, з метою розкриття особливостей забезпечення інформаційного суверенітету в умовах воєнного стану важливо проникнути в його сутність, розкрити його юридичну природу.

Поняття «суверенітет» є родовим відносно поняття «інформаційний суверенітет». Етимологічно «суверенітет» (від нім. souveränität, від франц. souverainete) означає: 1) незалежність і самостійність держави в її зовнішніх і внутрішніх справах [313]; 2) верховенство влади всередині країни та її незалежність від влади будь-якої іншої держави [314, с. 643]; 3) незалежність держави, що полягає в її праві за власним розсудом розв'язувати свої внутрішні й зовнішні справи, без втручання в них будь-якої іншої держави [315]; 4) політична незалежність і самостійність держави у внутрішній та зовнішньополітичній діяльності, що не допускає втручання інших держав [316]. Отже, ключовими є принципи верховенства, незалежності і самостійності держави та її влади для того, щоб визнати наявність у неї суверенітету. Ця теза поширюється і на інформаційну сферу держави і суспільства.

В. Ковтун виділяє два аспекти у змісті суверенітету – формально-юридичний та фактичний. Перший необхідно розглядати як своєрідну політико-правову форму державного суверенітету, як явище, а другий – як його матеріальний зміст [317]. Суверенітет поділяють на державний, народний і національний. Державний суверенітет походить від народного суверенітету. Вони пов'язані з національним суверенітетом, що обумовлений правом нації на самовизначення.

Державний суверенітет визначається в Декларації про державний суверенітет України від 16 липня 1990 р. як верховенство, самостійність, повнота і неподільність влади Української держави в межах її території, що є незалежним і рівноправним суб'єктом міжнародних відносин [318; 390]. Верховенство державної влади полягає в тому, що вона визначає увесь механізм правових відносин у державі, встановлює загальний правопорядок, правоздатність, права й обов'язки державних органів,

суспільних об’єднань, посадових осіб і громадян. [319, с. 8]. Принцип незалежності передбачає політичну самостійність і не підпорядкованість держави іншим суб’єктам у реалізації нею власних функцій і завдань. Самостійність держави проявляється через реальну можливість приймати самостійні рішення з внутрішніх та зовнішніх питань, підкорюючись тільки вимогам національного і міжнародного права.

Фактична наявність суверенітету у держави робить можливою реалізацію життєво важливих інтересів людини, суспільства і держави. Саме її суверенноздатність забезпечує прогресивний демократичний розвиток держави та безпечні умови життєдіяльності і добробуту її громадян [320, с. 85]. Соціальною цінністю суверенітету є юридична самостійність держави, котра виявляється в непідкоренні іншій державі або групі держав тобто незалежність від чужої волі. Однак ця незалежність не означає непідкорення міжнародному праву та не повинна бути теоретичним обґрунтуванням самоізоляції, відокремлення та автаркії [321, с. 40]. Суверенітет має дві сторони – внутрішню і зовнішню, а національний інформаційний простір є частиною глобального [322]. Якщо на внутрішньодержавному рівні слід говорити про суверенітет як ознаку держави, то на міжнародному – про принцип поваги до державного суверенітету. Державний суверенітет залишається базисом міжнародно-правової системи. У межах міжнародного права доцільно розробити більш ефективні механізми для захисту державного суверенітету, враховуючи необхідність його захисту на сучасному етапі від інформаційних проявів міжнародного злочину «агресія», а також «гібридних» війн [323]. Суверенітет не заперечує зобов’язань дотримуватися міжнародного права. А інформаційна сфера безпосередньо пов’язана з глобальною взаємодією, оскільки національний інформаційний простір є невід’ємною частиною глобального. Отож, забезпечення інформаційного суверенітету держави вимагає поєднання національних та міжнародних засобів.

О. Солодка зауважує, що інформаційний суверенітет є відносно відокремленим видом державного суверенітету, оскільки ознаки державного та інформаційного суверенітетів не завжди збігаються. Відтак, інформаційний суверенітет держави, хоча і може розглядатися як видовий відносно суверенітету держави, відрізняється від

останнього юрисдикційними межами, колом уповноважених суб'єктів та ступенем участі недержавних структур у забезпеченні, власними моделями і комбінаціями методів правового регулювання, рівнем міжнародної співпраці тощо [324, с. 84]. У правничій літературі застосовується також поняття «державний суверенітет в інформаційній сфері». Хоча поняття «інформаційний суверенітет» загалом піддається критиці на користь використання поняття «державний суверенітет в інформаційній сфері», вважаємо його таким, що чіткіше підкреслює взаємозв'язок з інформаційною безпекою.

Підтримуємо і позицію про те, що державний суверенітет є цілісним, неподільним, тому інформаційний суверенітет не є окремим, самостійним явищем. Це поняття позначає прояв державного суверенітету в інформаційній сфері.

О. Радутний, зазначає, що виокремлення інформаційного суверенітету та його самостійне дослідження зумовлено складністю інформаційної системи та необхідністю більш детального аналізу її елементів [325, с. 24]. Ми підтримуємо використання поняття «інформаційний суверенітет» в контексті розкриття предмету цієї дисертаційної роботи.

В правничій літературі традиційно представлена низка різних варіацій визначення поняття «інформаційний суверенітет».

Поширеним є підхід до визначення сутності інформаційного суверенітету як складного, багатоелементного явища через перерахування його складових, що варіюються за кількісними і якісними критеріями.

Так, О. Довгань зауважує, що національні інформаційні ресурси є першоосновою інформаційного суверенітету, за їх допомогою держава контролює та регулює інформаційні потоки [326, с. 110]. На думку О. Чайки, інформаційний суверенітет включає в себе контроль над національними інформаційними ресурсами, захист національних інтересів в інформаційній сфері, включно з освітнім простором, й створення механізмів для нейтралізації зовнішніх інформаційних впливів [327]. Є. Єсімов вважає, що інформаційний суверенітет охоплює інформацію, інформаційний простір, що включає інформаційну інфраструктуру і інформаційні технології. [328, с. 42]. О. Талдикін зауважує, що самостійність прийняття рішень

державою стосовно питань комунікації, інформативної сфери, правомірність поширення державного суверенітету на мережевий та віртуальний простір, створення дієвого механізму правової регуляції з урахуванням як норм національного законодавства, так і норм міжнародного права для захисту інформаційного віртуального простору від негативних зовнішніх впливів дає підстави говорити про інформаційний суверенітет [329, с. 133]. Узагальнюючи наведені підходи, можна дійти висновку, що сутність інформаційного суверенітету розкривається через систему взаємопов'язаних складових, зокрема: контрольованості національних інформаційних ресурсів; захищеності національних інтересів в інформаційній сфері; функціонування механізмів нейтралізації зовнішніх інформаційних загроз; забезпеченості безпеки інформаційного простору, включно з інфраструктурою та технологіями; реальної самостійності держави у прийнятті рішень у сфері регулювання інформаційних процесів тощо. Отже, інформаційний суверенітет визначається як комплексне явище, що поєднує низку елементів, спрямованих на збереження та розвиток національного інформаційного простору.

Переважна більшість дослідників співвідносять інформаційний суверенітет з державним суверенітетом та пропонують розуміти його як конкретне право держави, її реальну здатність впливати, визначати та регулювати інформаційну сферу.

Так, О. Олійник, О. Соснін та Л. Шиманський визначають інформаційний суверенітет як виключне право України відповідно до Конституції, законодавства України та норм міжнародного права самостійно і незалежно з додержанням балансу інтересів особи, суспільства і держави визначати й здійснювати внутрішні та геополітичні національні інтереси в інформаційній сфері, державну внутрішню і зовнішню інформаційну політику, розпоряджатися власними інформаційними ресурсами, формувати інфраструктуру національного інформаційного простору, створювати умови для його інтегрування у світовий інформаційний простір та гарантувати інформаційну безпеку держави [330, с. 537]. О. Олійник аргументує, що інформаційний суверенітет – це виключне право України самостійно і незалежно визначати внутрішні і геополітичні інтереси в інформаційній сфері, державну внутрішню і зовнішню інформаційну політику та здійснювати її, формувати і вільно

розпоряджатися власними інформаційними ресурсами, формувати інфраструктуру національного інформаційного простору, створювати умови для його інтегрування у світовий інформаційний простір, забезпечувати інформаційну безпеку відповідно до Конституції і законодавства України та норм міжнародного права з додержанням балансу інтересів особи, суспільства і держави [331, с. 7]. О. Ярема зазначає, що інформаційний суверенітет – це здатність і намір суб'єкта політики виробляти, розподіляти та споживати інформацію залежно від власних інтересів та використовувати інформацію як ресурс політичного впливу в тих масштабах і обсягах, які відповідають за поточний та довгостроковий політичний інтерес [332, с. 192]. О. Радутний розуміє його як верховенство та незалежність держави в інформаційній сфері, її здатність визначати свою внутрішню та зовнішню інформаційну політику, створювати, контролювати і регулювати важливі потоки інформації на своїй території та у міжнародній взаємодії поза її межами, спроможність ефективно протидіяти зовнішнім та внутрішнім інформаційним викликам [325, с. 29]. С. Люлько та С. Сунєгін доводять, що інформаційний суверенітет держави являє собою сталу феноменологічну конструкцію, що включає в себе як здатність держави контролювати власний інформаційний простір в межах міжнародно визнаної юрисдикції, так і захист інтересів внутрішньої інформаційної сфери у контексті попередження дезінформаційних атак з боку інших держав або від засобів масової інформації (ЗМІ), що використовуються такими державами у якості інструмента деструктивного інформаційного впливу на відповідне суспільство [333]. В. Супрун визначає це поняття як стан самостійності формування певних ресурсів, даних, створених у результаті здійснення державою своєї свободи, за рахунок держави або суб'єктів держави, внаслідок реалізації права на інформацію, що забезпечує рівність її у міжнародному інформаційному просторі [334, с. 18]. Отож, на думку вчених, інформаційний суверенітет – це виключне право та реальна здатність держави самостійно й незалежно визначати, формувати та реалізовувати внутрішню й зовнішню інформаційну політику, розпоряджатися національними інформаційними ресурсами та інфраструктурою, а також контролювати й регулювати інформаційні потоки в межах власної юрисдикції.

З точки зору такого підходу важливе: забезпечення балансу інтересів особи, суспільства і держави; інтеграція національного інформаційного простору у глобальний; запобігання та протидія зовнішнім і внутрішнім інформаційним загрозам; гарантування впливовості держави у міжнародному інформаційному просторі.

Інформаційний простір держави не обмежений її територіальними кордонами, адже сучасні інформаційні процеси обумовлюють транснаціональний інформаційний обіг. Звідси підвищена вразливість інформаційного суверенітету до зовнішніх загроз.

Сутність поняття «інформаційний суверенітет» викривлене традиційним розумінням «державного суверенітету» в системі міжнародних відносин і загалом у політико-правовій науці. Але ці дві категорії на скільки темпорально віддалені одна від одної, що сучасна система інформаційних процесів просто не вписується в традиційну доктрину державного суверенітету, що визнана національними та міжнародними документами. Це пов’язано, наприклад, із тим, що відповідно теорії державного суверенітету, від повинен поширюватись і на кіберпростір.

О. Олійник зауважує, що інформаційний суверенітет, так само як і інформаційну безпеку, доцільно розглядати в якості категоричного імперативу сучасності – закономірного результату цивілізаційного розвитку в інформаційну еру. Державний суверенітет – це загальновизнане у світі, суверенне право держави здійснювати через відповідні державні структури функції, спрямовані на формування та реалізацію внутрішньої і зовнішньої політики, а інформаційний суверенітет є важливою складовою забезпечення державного суверенітету [335]. Накладання традиційних уявлень про суверенітет на сучасну інформаційну сферу суспільної діяльності стає дедалі менш адекватним стосовно реальних процесів, пов’язаних з розвитком цієї сфери і, насамперед, інтернет-середовища. Це, зокрема, демонструє не досить переконлива й ефективна практика формування відповідної правової бази, заснованої на традиційних підходах, що є характерною для ряду країн світу [336, с. 89]. Отже, сутність та юридична природа інформаційного суверенітету потребує переосмислення та реконструювання, оскільки його ототожнення з державним суверенітетом не відображає реалій сучасних глобальних інформаційних процесів.

Дослідники у сфері кіберправа Р. Полчакі та Д. Дж. Б. Свантессон підтримують альтернативну концепцію інформаційного компонента державного суверенітету згідно з міжнародним публічним правом – концепцію, яка не обтяжена логічними та технічними суперечностями нещодавно домінуючого територіального розуміння суверенітету та юрисдикції [337]. Інформаційний суверенітет не обмежений, але певним чином пов'язаний з територією держави та реальною географією, оскільки маршрути комунікації, сервери, сховища, перемикачі, з'єднувачі, технічні вузли та доменні зони мають конкретну локалізацію. Крім того, перехрещення потоків інформації від різноманітних навігаційних, мобільних та інших пристроїв утворюють мережу, яку можливо зіставити з певною територією [325, с. 29]. Інформаційний суверенітет держави існує в умовах динамічних інформаційних процесів, тому важливо робити акцент на його адаптивності, гнучкості, здатності швидко реагувати на нові виклики, пов'язані з глобалізацією інформаційного простору.

Інформаційний суверенітет пропонується розуміти як виключне право та реальна здатність України, відповідно до національного і міжнародного законодавства самостійно, незалежно і визначати, формувати та реалізовувати внутрішню й зовнішню інформаційну політику, визначати внутрішні та зовнішні національні інтереси, розпоряджатися національними інформаційними ресурсами та інфраструктурою, контролювати й регулювати інформаційні потоки в межах власної юрисдикції.

Існує взаємозв'язок реалізації державного суверенітету в інформаційному просторі з інформаційною функцією держави та державною інформаційною політикою. Зазначений підхід щодо взаємозв'язку та співвідношення інформаційної функції держави та державної інформаційної політики дозволяє виділяти статичну та динамічну складові в інформаційно-правовому механізмі забезпечення державного суверенітету [332, с. 193]. Уваги заслуговує співвідношення інформаційного суверенітету та інформаційної безпеки в умовах воєнного стану.

Інформаційний суверенітет окремої держави, її інформаційна безпека набувають особливої значущості у державній інформаційній політиці [338]. Інформаційна політика держави має ключову мету – досягнення та підтримка

інформаційного суверенітету. Водночас рівень і стан інформаційної безпеки безпосередньо визначаються змістом та ефективністю реалізації інформаційної політики.

Інформаційна безпека є практичним результатом інформаційної політики, тому якщо вона є неефективною інформаційний суверенітет не забезпечується на належному рівні.

Інформаційний суверенітет та інформаційна безпека взаємопов'язані. Їх взаємозв'язки, на думку О. Олійника, виявляються у тому, що: головною метою забезпечення як інформаційного суверенітету, так як і інформаційної безпеки є захист національних інтересів; реалізація функцій держави у цих сферах має здійснюватися за загальними принципами, визначеними Конституцією України і законами України; забезпечення інформаційної безпеки безпосередньо пов'язано із суверенним правом держави, що випливає із засад інформаційного суверенітету як важливої складової державного суверенітету; державна політика у сфері забезпечення інформаційного суверенітету й інформаційної безпеки мають як загальні напрями діяльності, так і такі, що реалізуються на їм властивих напрямах, котрі доповнюють одне одного та підвищують рівень гарантій щодо досягнення позитивних результатів [335]. Отже, інформаційний суверенітет обумовлює і визначає зміст механізму забезпечення інформаційної безпеки, що включає правові, політичні, організаційні, інституційні, інструментальні аспекти. Реальний інформаційний суверенітет держави можливий за умови забезпеченості інформаційної безпеки. Загрози інформаційній безпеці підривають інформаційний суверенітет, а втрата державою контролю над інформаційним простором унеможливлює інформаційну безпеку.

Поряд із поняттям «інформаційний суверенітет» застосовується термін «цифровий суверенітет». Важливо також обґрунтувати їх співвідношення.

Цифровий суверенітет означає здатність держави контролювати свою цифрову долю, він може охоплювати контроль над усім ланцюжком постачань штучного інтелекту, від даних до апаратного і програмного забезпечення [339]. Суть цифрового суверенітету полягає в необхідності контролю над цифровими технологіями на фізичному рівні (ресурси, інфраструктура, пристрої), на рівні коду (стандарти,

правила, дизайн) та на інформаційному рівні (контент, дані) [340]. Ідея формування можливості та здатності національної держави (об'єднання держав) самостійно приймати рішення, якими регулюються цифрова інфраструктура та використання відповідних технологій в обмеженому суверенітетом просторі є відображенням зміни сталих моделей відносин влади під впливом цифрових трансформацій [341]. Сутність цифрового суверенітету полягає у здатності держави самостійно контролювати та регулювати фізичні, технологічні та інформаційні аспекти цифрової сфери. Цифровий суверенітет стосується не просто технічної автономії, а є нероздільним з політичним суверенітетом.

О. Солодка визначає цифровий суверенітет як різновид інформаційного суверенітету, оскільки останній включає не лише здатність впливати на інформаційно-комунікаційні технології загалом, але і на контент [324, с. 82]. Ю. Калайда також визнає цифровий суверенітет різновидом інформаційного суверенітету та зауважує, що він включає забезпечення цифрових прав громадян при використанні засобів масової комунікації, зміст якого охоплює не тільки захист персональних даних, а й право розпоряджатися своїми даними [342, с. 152]. Ми поділяємо таку позицію вчених та акцентуємо, що цифрові технології є складовою більш широкої категорії – інформаційної сфери.

Цифрові технології транскордонні, але в політичній сфері світ розбитий на суверенні держави. Важливою умовою для розвитку діалогу з цифрової проблематики є взаємна повага і визнання його суб'єктів, насамперед, суверенних держав. За цих умов суверенітет може виступити в ролі спільного знаменника, необхідного для подальшого розвитку міжнародного співробітництва у сфері забезпечення інформаційної безпеки за поваги до інтересів усіх держав [340]. А. Правдюк зауважує, що цифровий суверенітет на практиці виявляється відмінним від традиційного територіального суверенітету: цифровий суверенітет завжди є глобальним, зазвичай залучає корпорації, посилює державний нагляд і залишається чутливим до протекціоністських тенденцій. На перший погляд, термін «суверенітет» над частинами Інтернету може здатися абсолютно недоречним. Зрештою, однією з передумов для визнання суверенітету держави в міжнародному праві є здійснення

влади над територією [343]. Повага до суверенітету кожної держави є умовою конструктивного міжнародного діалогу з цифрової проблематики та побудови довіри у сфері інформаційної безпеки. Цифровий суверенітет – це категорія, що виходить за межі територіального підходу, тому потребує міжнародної співпраці та порозуміння, поваги до цифрових інтересів держави в умовах глобальної взаємодії. В умовах сучасності такий стан речей видається нереалістичним, отож цифровий суверенітет держав є ідеалом, до якого варто прагнути. Цифровий суверенітет держав фактично підривають транснаціональні корпорації, діяльність яких не підпорядкована їх ефективному контролю. Отож, складно узгодити національні інтереси у сфері забезпечення цифрового суверенітету з глобалізаційними процесами, наслідками відкритості та неконтрольованості мережі «Інтернет».

Кіберпростір, в якому дані є «будівельними блоками», чітко інтегрований в реальний світ, а їх розмежування більше не має сенсу. Реальні наслідки діяльності в кіберпросторі є безперечними [344]. Розуміння необхідності регулювання та забезпечення конфіденційності даних уможливлює гарантування інформаційного суверенітету в цілому.

Категорія «суверенітет даних» пов’язана саме з регулюванням даних, що знаходяться під юрисдикцією держави, в межах її визнаних кордонів. Суверенітет даних передбачає, що дані мають бути підпорядковані національному законодавству держави, в якій дані збираються, зберігаються та обробляються. Державні інституції можуть ухвалювати дієві рішення щодо регулювання даних, контролювати дотримання вимог щодо їх обробки і зберігання, доступу до них та їх захисту. Суверенітет даних поширюється на надання цифрових послуг зовнішніми суб’єктами, які зобов’язані неухильно дотримуватись внутрішнього законодавства.

Слід відзначити, що суверенітет даних не є чіткою політико-правовою категорією і в меншій мірі пов’язаний з концепцією державного суверенітету. При цьому, суверенітет даних визначається конкретними нормативними актами держави, де були створені дані. Якщо держава має «суверенітет над» певним фрагментом даних, це означає, що вона має юрисдикцію та повноваження щодо того, як ці дані можуть використовуватися та хто може отримати до них доступ. Однак часто дані

підпадають під дію законів кількох держав (місцезнаходження даних та локалізація даних), і їх регулювання, зберігання та обробка стають складнішими. У випадках, коли дані створюються в одній державі, але зберігаються та/або обробляються деінде, відповідальна за дані організація повинна забезпечити їх відповідність усім законодавчим вимогам [345]. Отже, суверенітет даних є одним із елементів досягнення інформаційного суверенітету.

Інформаційний суверенітет є ідеальною категорією, досягнення якої для України є перспективою. Гібридна військова агресія рф підірвала суверенездатність України в інформаційній сфері.

Вчені неоднозначно оцінюють наявність в України інформаційного суверенітету взагалі, а також можливості його забезпечувати [346; 343]. Саме існування та використання на території України криптовалюти порушує положення Декларації про державний суверенітет у частині самостійності України у вирішенні будь-яких питань свого державного життя.

Забезпечення інформаційного суверенітету є складним і багатокомпонентним завданням. Його розкриття сприяє поглибленому розумінню інформаційного суверенітету.

Етимологічно поняття «забезпечувати» означає – створювати надійні умови для здійснення чого-небудь, гарантувати щось [347]. Поняття «забезпечення» в юриспруденції має широкий зміст і включає в себе систематичну діяльність суб'єктів з метою досягнення комплексної мети.

О. Солодка складовими забезпечення інформаційного суверенітету держави пропонує вважати: інформаційно-правову – визначається місцем та повноваженнями держави у правовому регулюванні інформаційної сфери, інформаційно-гуманітарну – базується на формуванні інформаційно-змістовної концепції розвитку інститутів держави, суспільства та забезпеченні взаємозв'язків між ними) та інформаційно-технологічну – детермінується розвитком та використанням інформаційно-комунікаційних технологій та визначається поняттям цифрового (кібер) суверенітету, тобто як право гарантувати кібербезпеку держави, що нерозривно, пов'язано з інформаційною безпекою [348, с. 125]. С. Люлько та С. Сунєгін зауважують, що

забезпечення інформаційного суверенітету України в умовах сьогодення має інституційно-нормативну форму вираження, де ключового інтегративного значення у контексті протидії сучасним інформаційним загрозам від держави-агресора в умовах повномасштабної війни набуває діяльність Кабінету Міністрів України, Міністерства культури та стратегічних комунікацій України, Ради національної безпеки та оборони України та Центру протидії дезінформації, регламентована відповідними нормативно-правовими актами [333]. Інституційні механізми інформаційної політики представлені відповідними інституціями, які формують і реалізують державну інформаційну політику в Україні [349]. Обов'язок захисту інформаційного суверенітету покладається не тільки на державу, але й на увесь народ, окремою самостійною одиницею якого є кожен громадянин, кожна особистість, яка має правовий зв'язок з певним політико-територіальним утворенням як формою організації спільноти під управлінням уряду [325]. Отож, до структури забезпечення інформаційного суверенітету пропонується віднести: політико-правову, організаційно-інституційну, інформаційно-технічну, культурно-гуманітарну складові.

Під політико-правовою складовою слід розуміти державну інформаційну політику, нормативно-правову основу інформаційного суверенітету; під організаційно-інституційною складовою – систему інституцій, що забезпечують інформаційний суверенітет та організацію їх діяльності у цій сфері; інформаційно-технічна складова включає матеріально-технічну основу інформаційного суверенітету, інформаційну інфраструктуру; культурно-гуманітарна складова передбачає забезпечення інформаційної культури суспільства, підвищення рівня медіаграмотності, захист національної ідентичності та національної ідеї.

Стан забезпеченості інформаційного суверенітету передбачає те, що: 1) право на інформацію має належати державі або її органам влади; 2) реалізація державою інформаційного суверенітету включає забезпечення її інформаційної безпеки; 3) реалізація інформаційного суверенітету [338, с. 35]; 4) має бути гарантованою презумпція інформаційної свободи як базисний принцип реалізації інформаційного суверенітету, захищеність інформаційної приватності людини та права на

інформацію; 5) національні інтереси держави в інформаційній сфері, що обумовлені природними правами та свободами людини, мають бути визначеними та реалізованими [350, с. 21; 388]; 6) має бути сформованою дієва нормативно-правова основа, яка б якісно упорядковувала інформаційні відносини, визначала правові режими інформації, тощо; 7) має бути гарантовано стійкість національної інформаційної інфраструктури як матеріально-технічної основи інформаційного суверенітету; 8) ефективна системи управління інформаційною сферою повинно стабільно функціонувати як в умовах протидії інформаційним загрозам, так і в мирний час.

При цьому, забезпечення інформаційного суверенітету стикається з численними проблемами та перешкодами, що обумовлені внутрішніми та зовнішніми факторами об'єктивного та суб'єктивного характеру.

Ключові проблеми забезпечення інформаційного суверенітету зумовлені таким:

1) впливом глобалізаційних процесів на інформаційні відносини. Глобалізація – це процес світової інтеграції та зведення до єдиних стандартів розвитку економічної, політичної, культурної та релігійної сфери. Глобалізація становить собою трансформацію світових процесів [351]. Міжнародні цінності, норми, принципи, правила та інститути, у тому числі й державний суверенітет, завжди були схильні до змін, а міжнародне суспільство неминуче адаптувалося до нових реалій [352]. З розвитком глобалізаційних процесів на основі бурхливого розвитку науково-технічного прогресу глобалізатори обґрунтовують необхідність здійснення управління в глобальних масштабах на дедалі нижчих рівнях «глобалізованого» міжнародного простору, перетинаючи кордони суверенних держав, які стають дедалі «прозорішими» для світових процесів [326]. Ключовою проблемою забезпечення інформаційного суверенітету будь-якої держави є вплив глобалізації. Власне глобалізаційні процеси є проявами прогресу, об'єктивними і неминучими. Однак, їх результатом є «розмивання» інформаційних кордонів держави, втрата державою монополії на регулювання інформаційного простору, зростання залежності від транснаціональних цифрових платформ. Глобалізація уможливлює посилення

стороннього (в тому числі ворожого) впливу на національні інформаційні простори, що підриває інформаційний суверенітет держав.

Реальний суверенітет багатьох країн поступово слабшає під впливом глобалізаційних процесів, що викликає припущення про їх можливе зникнення з міжнародної арени в найближчому майбутньому. Цей процес також стосується інформаційного суверенітету. На нього впливають як внутрішні, так і зовнішні фактори. Внутрішніми є рівень демократії, структура захисту від негативної інформації, об'єднання суспільства навколо спільних інтересів, значення духовно-ціннісних орієнтирів, ефективність управління, стан науки, освіти, технічна база та доступ до попередніх наукових знань. Зовнішніми факторами є глобальні тенденції, вплив лідерів інформаційної сфери та проникнення чужих ідеологій у непідготовлене суспільство [343, с. 647]. Глобалізаційні процеси характеризуються новаторством, масштабністю, безальтернативністю. Правове регулювання та контроль новоутворених в процесі глобалізації інформаційних відносин є недостатньо недієвими. Глобалізація стимулює розвиток, але і створює нові виклики для збереження контролю держави над власним інформаційним простором.

2) активізацією інформаційного і технологічного прогресу. Розвиток електронних інформаційних технологій, і, особливо, супутникові лінії зв'язку значною мірою нівелювали технології організації інформаційної безпеки, напрацьовані попередніми поколіннями. Точніше, залишили їх дієвими лише для інформації, зафіксованої на паперових та інших предметних носіях [326, с. 103]. Стрімкий розвиток інформаційно-комунікаційних технологій, тотальна комп'ютеризація, створення глобального інформаційного простору зумовлює послаблення інформаційного суверенітету держави [170]. Шлях стримування інформаційного і технологічного прогресу використовується окремими державами світу з метою збереження інформаційного суверенітету, але він не веде до розвитку суспільства і держави, зміцнення свободи і демократії. Отож, раціональним є пошук нових, дієвих способів управління інформаційною безпекою, на стільки ж ефективних, на скільки цього потребують сучасні інформаційні загрози інформаційному суверенітету.

Окремо слід виділити потенційний вплив штучного інтелекту на забезпечення інформаційного суверенітету держави.

Розвиток технологій штучного інтелекту – одне з найважливіших досягнень сучасності, що зачіпає всі сфери життя, зокрема й інформаційну безпеку. Штучний інтелект відкриває нові можливості для автоматизації процесів, обробки даних і створення передових систем кіберзахисту. Водночас ця технологія може бути використана зловмисниками як потужний інструмент для проведення атак, що значно ускладнює завдання із захисту інформаційної інфраструктури країни. Штучний інтелект може автоматизувати кіберзагрози і зробити їх складнішими і масштабнішими [353, с. 161]. Зокрема, генеративні технології штучного інтелекту активно використовуються рф для інформаційних маніпуляцій та дезінформування.

3) посяганням на інформаційний суверенітет України з боку рф. Могутність провідних країн (економічна, військова, зовнішньо-політична, культурна) та їх взаємозалежність робить практично неможливим відкрите протистояння, змушуючи шукати альтернативні форми суперництва, за яких кожна з країн може збільшити свою перевагу або принаймні знизити ефективність дій суперника. За таких умов кіберпростір стає одним з важливих просторів протиборства, в тому числі через його нормативно-правову невизначеність [354, с. 203]. Інформаційне протиборство стало аксіоматичною складовою системи сучасних міжнародних відносин і дає можливість із залученням незначних фінансових та людських ресурсів, досягати потрібних цілей. Ефективність цієї боротьби безпосередньо залежить від ступеня професіоналізму суб’єктів здійснення інформаційних атак, захиститися від яких буде спроможне лише інтелектуально розвинене суспільство. Проведення багатьох операцій інформаційного протиборства практично неможливо виявити; відсутні міжнародні, юридичні та моральні норми ведення інформаційного протиборства, що надає цьому феномену множину можливостей та варіантів використання будь-яких маніпулятивних технологій для досягнення мети [355]. Однак, дії рф щодо інформаційного протиборства мають систематичний, агресивний, асиметричний характер. Інформаційне протиборство є елементом воєнної доктрини рф, компонентом її зовнішньополітичної стратегії. Рф цілеспрямовано застосовує

комплексні стратегії пропаганди, кібератаки, втручання у політичні процеси через інформаційно-комунікаційні технології тощо. Така діяльність підриває інформаційний суверенітет України, але спрямована вона одночасно й на низку інших держав світу.

Суть стратегії інформаційного протиборства, що реалізується в сучасних війнах, полягає в тому, що цілі війни багато в чому досягаються не за рахунок захоплення та утримання чужих територій, а за рахунок підриву ще в мирний час оборонного та економічного потенціалу держави-противника» [356, с. 190]. Інформаційна зброя особливо ефективно діє проти тієї країни, яка знаходиться у кризовому стані, у суспільній свідомості якої панує ціннісна амбівалентність, соціально-політична невизначеність. Застосування інформаційної зброї стає особливо ефективним, коли у державі спостерігається протистояння між політичними силами, наявною є криза моральної та правової свідомості, є слабкою патріотично налаштована еліта у всіх сферах суспільного життя» [357, с. 14]. Особливістю російської інформаційної агресії проти України стало те, що вона розпочалась задовго до військової агресії в 2014 р. Рф заздалегідь чітко спланувала використання інформаційної зброї як одного з ключових інструментів гібридної агресії проти України. Системне втручання або спроби втручання у всі ключові сфери суспільного життя України (політика, економіка, культура, освіта, духовне життя тощо) мали на меті зруйнувати стійкість та самостійність України, посягали на суспільну єдність та свідомість громадян, сприяли утвердженню ключових наративів і стереотипів, посилювали регіональні протиріччя та внутрішні кризові явища. Стратегія посилення контролю над свідомістю громадян України повинна була спростити та уможливити фізичне завоювання територій.

4) недієвість міжнародних правових механізмів гарантування інформаційного суверенітету держав. Як вже було зазначено, національний інформаційний простір є частиною глобального. Беззаперечно національний інформаційний суверенітет залежить від ефективності міжнародного правового регулювання інформаційних відносин та міжнародної інформаційної безпеки.

Сучасна міжнародна співпраця в інформаційній сфері здійснюється на договірній основі, а за відсутності договорів – на засадах взаємності, у межах міжнародних організацій, через представників державних органів, у регіональному масштабі. Вказана діяльність ґрунтується на системі правового регулювання взаємодії держав, їх компетентних органів та інших суб'єктів, яка заснована на взаємодії міжнародного та національного права, що регулюють відносини в інформаційній сфері [358, с. 275]. Але сфера інформаційного протистояння не стандартизована на міжнародному рівні, а закони і звичаї ведення інформаційної війни відсутні. Це унеможливлює встановлення відповідних міжнародних механізмів притягнення до відповідальності, а також міжнародної координації у випадках інформаційної агресії.

Світові війни – це саме та нульова точка відліку, точка кризи не тільки універсального міжнародного права, а й універсальної системи міжнародних відносин. Саме ця ситуація певною мірою «обнуляє» існуючі принципи і механізми, у тому числі і міжнародно-правові, і зазвичай приводить до народження нової системи міжнародних відносин і міжнародного права [359]. Неспроможність врегулювання російської агресії проти України міжнародно-правовими засобами загалом призвело до скептичного ставлення до ключових міжнародних інституцій та міжнародного права.

Інформаційна агресія побудована на засадах тоталітаризму, масової пропаганди, відсутності політичного плюралізму, коли довіра до інформації зазвичай втрачає свою аксіологічну природу, базується на неякісному та клікбейтному опрацюванні інформації в ЗМІ, а не тлумачиться як «суттєва рушійна сила переконань громадян й еліти щодо легітимності глобального управління» [360]. Міжнародний злочин агресії і є одним із найсерйозніших порушень міжнародного права, проте міжнародне право, яке є основою для протидії воєнній агресії, не регулює механізми боротьби з економічними та інформаційними агресіями. У світлі цього міжнародне співтовариство має розвивати норми, що забороняють агресію у всіх її формах. Однак поки такі норми не розроблені, цей вид злочину залишається нерегульованим [361, с. 336]. Відсутність ефективної та достатньої міжнародно-правової регламентації у

сфері інформаційного протистояння та гарантування інформаційного суверенітету створює передумови для неконтрольованого і безкарного застосування будь-якої інформаційної зброї та технологій.

5) вразливістю інформаційної інфраструктури України. Інформаційна інфраструктура України як об'єкт інформаційної безпеки і матеріально-технічна основа інформаційного суверенітеті є особливо вразливою в умовах воєнного стану.

Вразливості притаманні об'єкту інформаційної безпеки, невіддільні від нього і обумовлюються недоліками процесу функціонування, організаційно-технічної і правової системи захисту, умовами експлуатації та використання. Рівень інформаційного імунітету – кількісно-якісна характеристика об'єкта інформаційної безпеки. Це стан об'єктів інформаційної безпеки, що характеризує їх здатність знижувати власну вразливість. Чим вищий інформаційний імунітет, тим менше обставин, обумовлених недоліками побудови процесу функціонування об'єктів та організаційно-технічної і правової системи захисту (вразливостей) [362].

Інформаційний імунітет національної інформаційної інфраструктури потребує посилення через комплекс правових, організаційних, технологічних, кадрових заходів з метою забезпечення її стійкості.

Розробка та впровадження ефективних технологій кіберзахисту – необхідна умова для захисту інформаційної інфраструктури країни від зовнішніх і внутрішніх загроз. Інвестиції в інноваційні технології, включно зі штучним інтелектом та інструментами для боротьби з кіберзлочинністю, допоможуть створити більш стійку систему захисту і знизити ймовірність успішних атак. Водночас важливим елементом є зміцнення нормативно-правової бази для розв'язання нових завдань цифрової трансформації та запровадження відповідних санкцій за порушення інформаційної безпеки [353, с. 161]. Для України характерними є недоліки правового регулювання функціонування та захисту національної критичної інформаційної інфраструктури, недосконаліть державної політики в сфері її захисту в умовах високого ризику вчинення диверсій і терористичних та кібератак на її об'єкти [363, с. 13]. Крім того, інформаційна інфраструктура в умовах воєнного стану активно модернізується та оновлюється, однак проблемою залишається нерівномірність та непослідовність її

розвитку, а також дефіцит висококваліфікованих кадрів у сфері інформаційної безпеки.

Потребують фінансових рішень такі проблеми, як: застарілість частини технічних засобів, апаратного та програмного забезпечення; відсутність дієвих систем виявлення та нейтралізації кібератак; недостатній рівень розвитку резервних дата-центрів; залежність від іноземних технологій в умовах воєнного стану та ін.

Це далеко не вичерпний перелік проблем, що обумовлюють складність забезпечення інформаційного суверенітету. Переважна більшість з них потребує вирішення саме на національному рівні.

Одне з найважливіших завдань для забезпечення інформаційного суверенітету – створення законодавчої бази, зокрема розроблення відповідних концепцій та стратегій інформаційного розвитку держави, а також планів їхньої реалізації. Такі стратегічні документи в правовій формі визначають напрями і перспективи розвитку держави, створюють правові засади інноваційного розвитку, визначаючи основи державної політики у сфері забезпечення інформаційного суверенітету [322]. Правове регулювання інформаційної сфери об’єктивно сприятиме її розвитку та формуванню інформаційного законодавства, яке покликано впорядкувати суспільні інформаційні відносини, що виникають у процесі здійснення інформаційної взаємодії, а також спрямовані на забезпечення не лише інформаційних та інших, пов’язаних із ними, прав та інтересів людини, суспільства та держави [348, с. 123]. Інформаційний суверенітет держави може бути забезпечений та гарантований за умови якісного і дієвого законодавчого забезпечення інформаційної безпеки.

Формування цілісної правової основи інформаційного суверенітету потребує конкретних і виважених концептуальних рішень, довгострокового стратегічного планування. Ухвалені стратегічні документи створюють правову основу державної політики у сфері інформаційної безпеки, визначають ключові загрози. Але правове забезпечення інформаційного суверенітету має не лише сприяти його системному розвитку, але й гарантувати захист інформаційних прав та інтересів особи, суспільства та держави.

Н. Казакова, Ю. Щербина та О. Фразе-Фразенко зауважують, що для машинних і когнітивних інтерфейсів, повинен бути створений новий правовий режим функціонування, який визначить правила реагування на конфліктні ситуації між суб'єктами міжмашинної взаємодії [364, с. 78]. Технології інформаційно-комунікативного конструювання суспільних процесів обираються та встановлюються у відповідності до обраної стратегії в інформаційній політиці держави, задля її реалізації з найбільшою ефективністю (результативністю) [365, с. 48]. Впровадження ефективної інформаційної політики може допомогти знизити напруженість у соціально-економічній ситуації країни та сприяти вирішенню зовнішньополітичних конфліктів [366, с. 112; 367, с. 336]. Україна має досить слабку інформаційну політику. Такий підхід недопустимий в умовах відсічі повномасштабної російської гібридної агресії.

Успіх російської пропаганди полягає в тому, що в неї є довгострокова стратегія, що робити з Україною, а в України такої довгострокової стратегії немає, що є головною проблемою інформаційної безпеки для України [323]. Ситуативні заходи не забезпечують належної стійкості в умовах гібридної війни та тривалого інформаційного протистояння. Неможливо забезпечити ефективну протидію зовнішній інформаційній агресії без комплексної, довгострокової державної інформаційної політики, яка має бути спрямованою на гарантування інформаційного суверенітету України.

Гібридна війна становить якісно нову радикальну форму геополітичних і внутрішньополітичних конфліктів латентного й асиметричного характеру, універсальний засіб безкровного забезпечення інтересів суб'єктів ведення інформаційної війни, де основною зброєю виступає інформація, інтернет-мережа та канали масової комунікації, спрямовані на бажану зміну суспільної свідомості, базових цінностей і політичних орієнтації громадян, політичної еліти та вищих керівних кадрів протиборствуючої держави й задля її інформаційного поневолення [368, с. 103]. В таких умовах різні методи відсічі інформаційних загроз вдаються ефективними в комплексі. Однак, втручання в демократичні інституції та процеси в Україні завжди викликає зростання соціальної напруги.

Пріоритет безпекової функції Української держави беззаперечний. Однак не всі засоби контролю за інформаційним простором видаються доцільними та дієвими. Зокрема, не сприяє стабілізації інформаційного простору те, що в Україні надмірно посилений державний контроль за медіапростором. Хоча в умовах воєнного стану така практика може бути необхідною, в дійсності це лише підриває демократичні принципи та знижує довіру населення до державних інституцій. Як наслідок, використання національних інформаційних платформ для донесення офіційної позиції держави до населення є малоефективним.

Крім того, використання методів пропаганди відносно українського суспільства в умовах воєнного стану призводити до посилення скептицизму щодо офіційної інформації. У довгостроковій перспективі така практика може ослабити інформаційний суверенітет.

Державна інформаційна політика повинна базуватись на забезпеченні права на достовірну, повну та своєчасну інформацію, свободу слова та інформаційну діяльність, недопущення втручання в зміст та внутрішню організацію інформаційних процесів; забезпеченні інформаційної та національно-культурної ідентифікації України у світовому інформаційному просторі; гарантуванні державної підтримки та розвитку ресурсів науково-технічної продукції та інформаційних технологій [369, с. 216]. Надмірний контроль держави за медіапростором в умовах воєнного стану призводить до звуження демократичних свобод, зниження рівня суспільної довіри до державної влади та зниження ефективності державної інформаційної політики. Пріоритетним є розвиток політики стратегічної комунікації, що підпорядкована принципам прозорості, об’єктивності, доцільності.

У суспільстві, де більша частина інформації надходить з Інтернету і соціальних мереж, важливо, щоб люди володіли достатніми знаннями про те, як захистити себе від фальшивих новин, кібератак і маніпулювання інформацією [114, с. 202]. Війна залишить кривавий відбиток не лише на економіці, демографічній та соціальній структурах українського суспільства, але й в свідомості та світогляді кожного небайдужого українця, підніме хвилю рефлексії з приводу інформаційних кампаній та вкидів, які роками здійснювали медіа та мас-медіа країни-агресорки,

актуалізує пошуки винних в інформаційних програшах та провалах [370, с. 83]. Посилення інформаційної компетентності та медіаграмотності є важливим фактором забезпечення інформаційного суверенітету.

Отже, ключовими напрямами забезпечення інформаційного суверенітету в умовах воєнного стану пропонується вважати наступні: 1) модернізація інформаційного законодавства з урахуванням сучасного стану розвитку інформаційної сфери та інформаційних відносин; 2) посилення інституційної спроможності суб'єктів забезпечення інформаційного суверенітету; 3) посилення та концептуалізація інформаційної політики держави; 4) модернізація наявних інформаційно-комунікаційних технологій та інформаційної інфраструктури; 5) посилення медіаграмотності населення, розвиток Української національної ідеї, активізація національної консолідації; 6) розвиток співпраці з міжнародними інституціями для вироблення спільного механізму протидії інформаційним загрозам.

Проведене дослідження дозволяє дійти таких висновків.

1. Інформаційний суверенітет пропонується розуміти як виключне право та реальну здатність України, відповідно до національного і міжнародного законодавства самостійно і незалежно визначати, формувати та реалізувати внутрішню й зовнішню інформаційну політику, визначати внутрішні та зовнішні національні інтереси, розпоряджатися національними інформаційними ресурсами та інфраструктурою, контролювати й регулювати інформаційні потоки в межах власної юрисдикції. Державний суверенітет є цілісним, неподільним, тому поняття «інформаційний суверенітет» позначає прояв державного суверенітету в інформаційній сфері. Сутність поняття «інформаційний суверенітет» викривлене традиційним розумінням «державного суверенітету» в системі міжнародних відносин і загалом у політико-правовій науці. Інформаційний простір держави не обмежений її територіальними кордонами, адже сучасні інформаційні процеси обумовлюють транснаціональний інформаційний обіг.

2. Поряд із поняттям «інформаційний суверенітет» застосовується термін «цифровий суверенітет». Цифровий суверенітет – це категорія, що виходить за межі територіального підходу, тому потребує міжнародної співпраці та порозуміння,

поваги до цифрових інтересів держави в умовах глобальної взаємодії. Суміжна категорія «суверенітет даних» пов'язана з регулюванням даних, що знаходяться під юрисдикцією держави, в межах її визнаних кордонів. Суверенітет даних передбачає, що дані мають бути підпорядковані національному законодавству держави, в якій дані збираються, зберігаються та обробляються.

3. Інформаційний суверенітет обумовлює і визначає зміст механізму забезпечення інформаційної безпеки. Реальний інформаційний суверенітет держави можливий за умови забезпеченості інформаційної безпеки. Інформаційна безпека є практичним результатом інформаційної політики, тому якщо вона є неефективною інформаційний суверенітет не забезпечується на належному рівні. Загрози інформаційній безпеці підривають інформаційний суверенітет, а втрата державою контролю над інформаційним простором унеможливлює інформаційну безпеку. Раціональним є пошук нових, дієвих способів управління інформаційною безпекою, на скільки ж ефективних, на скільки цього потребують сучасні інформаційні загрози інформаційному суверенітету.

4. Забезпечення інформаційного суверенітету включає в себе політико-правову, організаційно-інституційну, інформаційно-технічну, культурно-гуманітарну складові. Під політико-правовою складовою слід розуміти державну інформаційну політику, нормативно-правову основу інформаційного суверенітету; під організаційно-інституційною складовою – систему інституцій, що забезпечують інформаційний суверенітет та організацію їх діяльності у цій сфері; інформаційно-технічна складова включає матеріально-технічну основу інформаційного суверенітету, інформаційну інфраструктуру; культурно-гуманітарна складова передбачає забезпечення інформаційної культури суспільства, підвищення рівня медіаграмотності, захист національної ідентичності та національної ідеї.

5. Ключові проблемами забезпечення інформаційного суверенітету обумовлені наступним: 1) впливом глобалізаційних процесів на інформаційні відносини; 2) активізацією інформаційного і технологічного прогресу; 3) посяганням на інформаційний суверенітет України з боку рф; 4) недієвість міжнародних правових

механізмів гарантування інформаційного суверенітету держав; 5) вразливістю інформаційної інфраструктури України.

Відсутність ефективної та достатньої міжнародно-правової регламентації у сфері інформаційного протистояння та гарантування інформаційного суверенітету створила передумови для неконтрольованого і безкарного застосування будь-якої інформаційної зброї та технологій. Спроби рф системно втручатися у всі ключові сфери суспільного життя України (політика, економіка, культура, освіта, духовне життя тощо) мали на меті зруйнувати стійкість та суверенздатність України, посягали на суспільну єдність та свідомість громадян, сприяли утвердженню ключових наративів і стереотипів, посилювали регіональні протиріччя та внутрішні кризові явища.

6. Ключовими напрямами забезпечення інформаційного суверенітету в умовах воєнного стану пропонується вважати наступні: 1) модернізація інформаційного законодавства з урахуванням сучасного стану розвитку інформаційної сфери та інформаційних відносин; 2) посилення інституційної спроможності суб'єктів забезпечення інформаційного суверенітету; 3) посилення та концептуалізація інформаційної політики держави; 4) модернізація наявних інформаційно-комунікаційних технологій та інформаційної інфраструктури; 5) посилення медіаграмотності населення, розвиток Української національної ідеї, активізація національної консолідації; 6) розвиток співпраці з міжнародними інституціями для вироблення спільного механізму протидії інформаційним загрозам. Ситуативні заходи не забезпечують належної стійкості в умовах гібридної війни та тривалого інформаційного протистояння. Для забезпечення ефективної протидії зовнішній інформаційній агресії необхідна комплексна, довгострокова державна інформаційна політика, яка має бути спрямованою на гарантування інформаційного суверенітету України.

Висновки до розділу 2

1. Правове забезпечення інформаційної безпеки України потребує подальшої модернізації та удосконалення. Воно здійснюється на трьох взаємопов'язаних рівнях: у сфері національної безпеки і оборони; інформаційних відносин та інформаційної безпеки; а також правового статусу суб'єктів забезпечення інформаційної безпеки. Нормативну основу становлять Конституція та закони України, підзаконні акти, а також міжнародні договори, ратифіковані ВРУ. Міжнародні стандарти мають орієнтовний характер і слугують базою для гармонізації національного законодавства, тоді як держава самостійно визначає способи реалізації національних інтересів з урахуванням загроз і можливостей. Актуальним є завдання систематизації та кодифікації інформаційного законодавства, зокрема шляхом можливого прийняття Інформаційного кодексу України, а також посилення правового забезпечення медіаграмотності населення через її інтеграцію в освітні програми всіх рівнів.

2. Інституційна складова забезпечення інформаційної безпеки – організована система уповноважених суб'єктів, діяльність яких нормативно врегульована та спрямована на формування і реалізацію державної політики у сфері інформаційної безпеки, а також на забезпечення належного рівня захищеності життєво важливих інтересів особи, суспільства і держави в інформаційній сфері. До системи суб'єктів забезпечення інформаційної безпеки України пропонується віднести інституції державного сектору та недержавні інституції. *Ключовими проблемами інституційного забезпечення інформаційної безпеки* є фрагментарність системи, слабка координація, нечіткий розподіл відповідальності, недостатня спроможність окремих суб'єктів, слабка інтеграція недержавних акторів і низька медіаграмотність населення. *Напрями удосконалення:* систематизація та кодифікація правової бази; узгодження функцій, повноважень і меж відповідальності ключових суб'єктів; розвиток публічно-приватного партнерства та посилення координації між державними й недержавними учасниками; зміцнення інституційної спроможності через розвиток кадрового, фінансового, наукового й технічного забезпечення;

активізація стратегічних комунікацій і підвищення рівня інформаційної та медіаграмотності населення.

3. Кібербезпека є системоутворюючою складовою інформаційної безпеки держави, що поєднує правові, організаційні та політичні інструменти захисту. Нормативно-правова та інституційна система кібербезпеки недостатньо враховує умови воєнного стану, а також характеризується відсутністю універсальних міжнародних норм щодо кваліфікації кібератак як актів агресії. Виявлені вразливості, зокрема технологічна залежність і кадровий дефіцит, обумовлюють необхідність закріплення принципу технологічного суверенітету. Баланс між кібербезпекою та правами людини має ґрунтуватися на принципах пропорційності, підконтрольності та тимчасовості обмежень. Ключовими напрямами реформ визначено: удосконалення правових режимів кібербезпеки у воєнний час; кодифікацію кіберзагроз; правове врегулювання кібердобровольчих формувань; створення єдиного координаційного центру; впровадження єдиного протоколу реагування на кіберінциденти; інтеграцію міжнародних стандартів; розвиток технологічного суверенітету та кадрового потенціалу; а також удосконалення механізмів кібердоказування і міжнародного співробітництва.

4. Інформаційний суверенітет визначається як здатність держави самостійно формувати та реалізовувати інформаційну політику, управляти інформаційними ресурсами та контролювати інформаційні потоки в межах юрисдикції. Поряд із ним цифровий суверенітет і суверенітет даних відображають нові виміри державної незалежності в умовах глобалізації та цифрової взаємодії. Його забезпечення охоплює політико-правову, організаційно-інституційну, інформаційно-технічну та культурно-гуманітарну складові. Основними проблемами є глобалізаційний тиск, технологічна залежність, інформаційна агресія рф, слабкість міжнародних механізмів та вразливість інфраструктури. Напрями зміцнення включають модернізацію інформаційного законодавства, посилення інституційної спроможності, розвиток інформаційної політики та інфраструктури, підвищення медіаграмотності й національної консолідації, а також розширення міжнародного співробітництва у сфері протидії інформаційним загрозам.

ВИСНОВКИ

1. Методологія дослідження інформаційної безпеки України постає як цілісна концептуальна основа дослідження, що визначає логіку наукового аналізу, формує сучасне бачення інформаційної безпеки як системоутворюючого елемента національної безпеки та орієнтує дослідження на врахування взаємодії правових, безпекових, технологічних і соціальних чинників. Багатовимірна природа інформаційної безпеки розкривається через комплекс взаємопов'язаних методологічних підходів і методів наукового пізнання, що забезпечують її цілісний аналіз як динамічної соціально-правової системи. Застосування загальнонаукових і спеціально-юридичних методів у поєднанні із системним, синергетичним, герменевтичним, антропологічним і кібернетичним підходами дозволяє виявити елементи інформаційної безпеки, закономірності їх функціонування, а також забезпечити інтеграцію проблематики кібербезпеки, інформаційного суверенітету та захисту прав людини у єдину наукову конструкцію. Сучасні вітчизняні та зарубіжні наукові підходи до дослідження інформаційної безпеки відображають тенденцію до формування інтегрованих методологічних моделей, що ґрунтуються на міждисциплінарності, ризик-орієнтованому підході, концепції кіберстійкості, мережевому аналізі та багаторівневому безпековому врядуванні. Їх використання розширює методологічні можливості юридичної науки та сприяє адаптації національних досліджень до умов глобалізованого інформаційного простору і сучасних воєнних викликів. Сформована методологічна конструкція дослідження інформаційної безпеки України створює теоретико-методологічне підґрунтя для подальшого розвитку правових засад її забезпечення, а також для вдосконалення нормативного та інституційного механізму функціонування системи інформаційної безпеки в умовах воєнного стану.

2. Попри значний масив наукових досліджень, проблематика інформаційної безпеки, особливо в умовах воєнного стану, не набула належної теоретико-правової систематизації та не має цілісної концепції як складової національної безпеки. В умовах гібридних загроз вона набуває ознак самостійного функціонального елемента

системи національної безпеки, тісно пов’язаного з кібербезпекою, інформаційною політикою та стратегічними комунікаціями, а інформаційний простір розглядається як окремий домен протиборства, що потребує вдосконалення механізмів державного регулювання. Еволюція наукових підходів демонструє перехід від фрагментарного розгляду до становлення інформаційної безпеки як самостійного напряму наукового пізнання, що зумовлено розвитком інформаційного суспільства та сучасними безпековими викликами. Водночас відсутнє уніфіковане її розуміння, а домінує міждисциплінарний підхід, який поєднує правові, політичні, соціально-комунікаційні, безпекові та технологічні аспекти. У цьому контексті інформаційна безпека розглядається як стратегічний ресурс держави, що визначає стійкість інституцій і ефективність публічного управління. Подальший розвиток її дослідження пов’язаний із інтеграцією концепцій кіберстійкості, управління ризиками та протидії дезінформації, що формує сучасну модель інформаційної безпеки, адаптовану до цифрових і воєнних викликів.

3. Інформаційна безпека є складовою національної безпеки України, що включає перманентний процес і результат забезпечення стану захищеності національних інтересів та інших життєво важливих інтересів людини, суспільства і держави в інформаційній сфері України від зовнішніх і внутрішніх, реальних та потенційних загроз. Її *ознаки:* є об’єктивним, цілісним явищем, що зумовлене розвитком інформаційної сфери конкретної держави і суспільства; має складну структуру; є багаторівневою; є складовою національної безпеки, формою її прояву в інформаційній сфері та виконує функцію консолідації всіх інших складових національної безпеки; поєднує в собі статичний та динамічний аспекти; існує у тісному взаємозв’язку з іншими сферами, що забезпечують суверенітет; регламентована нормативно-правовими актами; має матеріально-технічну, соціально-гуманітарну, правову, політичну, економічну та культурну сторони; розвивається шляхом впровадження нових стратегій реагування на інформаційні загрози та ін. *Складові інформаційної безпеки*: 1) об’єкти, які оберігаються від загроз; 2) загрози (реальні й потенційні, внутрішні та зовнішні); 3) система забезпечення інформаційної безпеки. Загрозами інформаційній безпеці в умовах воєнного стану є:

1) внутрішні загрози: низький рівень медіаграмотності та інформаційної компетентності населення; недосконаліть нормативно-правового та організаційного забезпечення інформаційної безпеки; низька ефективність державної інформаційної політики; низький рівень захищеності критичної інформаційної інфраструктури; правопорушення посадових осіб у інформаційній сфері; неефективність державного реагування на маніпулювання інформацією та суспільною думкою; слабка захищеність кіберпростору; слабка захищеність персональних даних громадян; брак цілеспрямованого інформування міжнародної спільноти про російську агресію в Україні; *2) зовнішні загрози:* комплексна інформаційна агресія рф проти України; інформаційний вплив держав-партнерів рф на Україну та міжнародне співтовариство; розвідувальна діяльність іноземних спецслужб; втручання у внутрішньополітичні процеси через інформаційно-комунікаційні технології; кібератаки, загрози кіберзлочинності та кібертероризму; дезінформація міжнародної спільноти про російську агресію в Україні; розробка та поширення нової інформаційно-психологічної зброї; неконтрольовані інформаційні деструктивні процеси в глобальній мережі «Інтернет».

4. Адаптація зарубіжного досвіду забезпечення інформаційної безпеки в умовах воєнного конфлікту має здійснюватися на засадах принципу пропорційності, що дозволяє відокремити правові механізми, спрямовані на легітимний захист національної безпеки від практик, які не відповідають європейським стандартам захисту прав людини та зобов'язанням України у межах євроінтеграції. Правове регулювання інформаційної безпеки доцільно здійснювати відповідно до системної нормативно-правової моделі, що поєднує норми інформаційного, безпекового та адміністративного права. Такий підхід є характерним для Німеччини, Франції, Естонії, Іспанії та ін., де правове регулювання інформаційної та кібербезпеки вибудовується на основі узгодження загальних актів безпекового характеру, спеціального інформаційного законодавства та адміністративних механізмів публічного управління. Це сприяє узгодженості правового регулювання в умовах кризових і воєнних загроз, підвищує ефективність реалізації безпекових рішень і водночас зменшує ризики правових колізій та непропорційного втручання держави в

інформаційну сферу. Стратегічні комунікації слід розглядати не лише як елемент інформаційної політики, а як окрему функцію сектору безпеки і оборони. Їх ефективність безпосередньо залежить від чіткого інституційного закріплення, розмежування повноважень між суб'єктами публічної влади та налагодженої міжвідомчої координації. Поєднання публічно-правових інструментів із механізмами державно-приватного партнерства у сфері кібербезпеки дозволяє підвищити стійкість інформаційних систем без надмірного розширення державного контролю. Потрібен післявоєнний перегляд правових режимів, запроваджених у сфері інформаційної безпеки, через можливість існування ризику збереження надзвичайних обмежень поза межами їх фактичної необхідності, що зумовлює потребу забезпечення балансу між безпековими обмеженнями та гарантіями інформаційних прав.

5. Правове забезпечення інформаційної безпеки України потребує подальшої модернізації та удосконалення. Воно здійснюється на трьох взаємопов'язаних рівнях: у сфері національної безпеки і оборони; у сфері інформаційних відносин та інформаційної безпеки; а також у сфері правового статусу суб'єктів забезпечення інформаційної безпеки. Нормативно-правову основу становлять Конституція та закони України, підзаконні нормативно-правові акти, а також міжнародні договори, згоду на обов'язковість яких надано ВРУ. Міжнародні стандарти у сфері інформаційної безпеки мають переважно орієнтовний характер і використовуються як важливий орієнтир для гармонізації та розвитку національної правової системи, тоді як держава самостійно визначає способи та обсяг реалізації національних інтересів в інформаційній сфері з урахуванням характеру загроз і наявних можливостей. У цьому контексті актуальним є завдання систематизації, узгодження та гармонізації інформаційного законодавства, що передбачає уточнення термінології, вдосконалення механізмів реалізації правових норм та імплементацію європейських стандартів, зокрема через можливе прийняття єдиного кодифікованого акта – Інформаційного кодексу України. Окремої уваги потребує посилення правового забезпечення медіаграмотності населення як складової інформаційної безпеки, оскільки розвиток критичного мислення громадян є не менш важливим, ніж технічні засоби захисту. У зв'язку з цим доцільним є нормативне закріплення

обов’язкового включення елементів медіаграмотності до освітніх програм усіх рівнів освіти.

6. Інституційна складова забезпечення інформаційної безпеки – організована система уповноважених суб’єктів, діяльність яких нормативно врегульована та спрямована на формування і реалізацію державної політики у сфері інформаційної безпеки, а також на забезпечення належного рівня захищеності життєво важливих інтересів особи, суспільства і держави в інформаційній сфері. До системи суб’єктів забезпечення інформаційної безпеки України пропонується віднести: *інституції державного сектору* (ВРУ, Президент України, РНБО України, КМУ, органи сектору безпеки і оборони та ін.); *недержавні інституції* (ОМС; ІГС та ін.). В Україні немає єдиного органу, відповідального за інформаційну безпеку. В умовах воєнного стану пріоритет – посилення спроможності наявних суб’єктів і покращення координації між ними. *Ключовими проблемами інституційного забезпечення інформаційної безпеки* є фрагментарність системи, слабка координація, нечіткий розподіл відповідальності, недостатня спроможність окремих суб’єктів, слабка інтеграція недержавних акторів і низька медіаграмотність населення. *Напрями удосконалення:* систематизація та кодифікація правової бази; узгодження функцій, повноважень і меж відповідальності ключових суб’єктів; розвиток публічно-приватного партнерства та посилення координації між державними й недержавними учасниками; зміцнення інституційної спроможності через розвиток кадрового, фінансового, наукового й технічного забезпечення; активізація стратегічних комунікацій і підвищення рівня інформаційної та медіаграмотності населення.

7. Кібербезпека є системоутворюючою складовою інформаційної безпеки держави, що поєднує правові, організаційні та політичні інструменти захисту. Нормативно-правова та інституційна система кібербезпеки переважно не враховує специфіку воєнного стану. Відсутні міжнародні універсальні норми, котрі б однозначно встановлювали правову кваліфікацію кібератак як акту воєнної агресії. Залежність від іноземних рішень, нестача вітчизняних криптографічних технологій і кадровий дефіцит у сфері кіберзахисту формують критичні вразливості оборонного потенціалу. Принцип технологічного суверенітету потребує нормативного

закріплення. Баланс між забезпеченням кібербезпеки та дотриманням прав людини у період воєнного стану має ґрунтуватися на принципах пропорційності, підконтрольності та тимчасовості обмежень. Серед ключових напрямів реформ слід виокремити: розробку та прийняття спеціального закону або розділу в законі про національну безпеку, що визначав би правові режими кібербезпеки під час воєнного стану; кодифікацію й введення у правову систему чітких категорій кіберзагроз із відповідними кваліфікаціями та санкціями; законодавче врегулювання діяльності добровольчих кібервійськ; формування єдиного кіберкоординатора або національного центру кібербезпеки; удосконалення процедур реагування у контексті введення єдиного протоколу інцидент-менеджменту, обов'язкове повідомлення про інциденти, санкції за неналежне реагування; інтеграцію міжнародних стандартів і практик у національне законодавство; розвиток національного технологічного суверенітету; підсилення кадрового потенціалу; впровадження спеціального режиму цифрових доказів в умовах воєнного стану, стандартів атрибуції, угод про міжнародне співробітництво у зборі і визнанні кібердоказів, врегулювання використання доказів іноземним партнерам.

8. Інформаційний суверенітет – виключне право та реальна здатність України, відповідно до національного і міжнародного законодавства самостійно і незалежно визначати, формувати та реалізувати внутрішню й зовнішню інформаційну політику, визначати внутрішні та зовнішні національні інтереси, розпоряджатися національними інформаційними ресурсами та інфраструктурою, контролювати й регулювати інформаційні потоки в межах власної юрисдикції. Цифровий суверенітет – це категорія, що виходить за межі територіального підходу, тому потребує міжнародної співпраці та порозуміння, поваги до цифрових інтересів держави в умовах глобальної взаємодії. Суміжна категорія «суверенітет даних» передбачає, що дані мають бути підпорядковані національному законодавству держави, в якій дані збираються, зберігаються та обробляються.

Забезпечення інформаційного суверенітету включає політико-правову, організаційно-інституційну, інформаційно-технічну та культурно-гуманітарну складові. *Проблеми забезпечення інформаційного суверенітету зумовлені:* впливом

глобалізаційних процесів на інформаційні відносини; активізацією інформаційного і технологічного прогресу; посяганням на інформаційний суверенітет України з боку рф; недієвістю міжнародних правових механізмів гарантування інформаційного суверенітету держав; вразливістю інформаційної інфраструктури України. *Напрямами забезпечення інформаційного суверенітету в умовах воєнного стану визначено:* модернізацію інформаційного законодавства з урахуванням сучасного стану розвитку інформаційної сфери та інформаційних відносин; посилення інституційної спроможності суб'єктів забезпечення інформаційного суверенітету; посилення та концептуалізацію інформаційної політики держави; модернізацію наявних інформаційно-комунікаційних технологій та інформаційної інфраструктури; посилення медіаграмотності населення, розвиток Української національної ідеї, активізація національної консолідації; розвиток співпраці з міжнародними інституціями для вироблення спільного механізму протидії інформаційним загрозам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Петришин О. В. Методологія правової науки. Загальна теорія держави і права : підруч. ; за ред. М. В. Цвіка, О. В. Петришина. Харків : Право, 2009. С. 25-35.

2. Рабінович П. М. Основи загальної теорії права та держави: навчальний посібник. Вид. 10-е, доповнене. Львів : Край, 2008. 162 с. URL: https://fpk.in.ua/images/biblioteka/3fmb_finan/Rabinovych-theory_philosophy_prava_posibnik_2021.pdf.

3. Теорія держави і права в схемах та таблицях : навч. посіб. / Л. Р. Наливайко та ін. ; Заг. ред. Л. Наливайко. Київ : Хай-Тек Прес, 2020. 296 с. URL: https://fpk.in.ua/images/biblioteka/1bac_pravo/TDP-skhemy-2020.pdf.

4. Косович В. Сучасна загальна теорія права та держави: тенденції розвитку. *Visnyk of the Lviv University. Series Law*. 2020. № 70. С. 3–9. URL: https://doi.org/10.30970/vla.2020.70.003.

5. Бобровник С. В. Актуальне видання з "Теорії держави і права" як фундаментальної юридичної навчальної дисципліни. *Публічне право*. 2017. № 1 (25). С. 279–280.

6. Скрипнюк О. В. Принцип верховенства права і держава: деякі питання методологічного забезпечення теоретичного аналізу проблеми. *Бюлетень Міністерства юстиції України*. 2008. № 9. С. 49–56.

7. Manuel C. The rise of the network society. Cambridge, Mass : Blackwell Publishers, 2009. 556 p. URL: https://doi.org/ 10.1002/9781444319514.

8. Горбулін В. П., Додонов О., Ланде Д. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія. Київ : Інтертехнологія, 2009. 164 с. URL: http://dwl.kiev.ua/art/gdl/gdl.pdf.

9. Горбулін В. П., Бєлов О. Ф., Литвиненко О. Національна безпека України: порядок денний для XXI століття. Київ : Стилос, 2009. 128 с.

10. Данильян О. Г., Дзьобань О. П., Максимов С. І. Філософія права. Харків : Право, 2009. 208 с. URL: https://library.nlu.edu.ua/POLN_TEXT/KNIGI_2009_2/FilosofUchebn2009.pdf.

11. Akhverdyan A. G. Values and General Legal Principles of Law: Theoretical and Legal Analysis. *Herald of Dagestan State University*. 2024. Vol. 39, no. 3. P. 51–56. URL: https://doi.org/10.21779/2500-1930-2024-39-3-51-56.

12. Webster F. Theories of the Information Society. London : Routledge, 2014. 416 p. URL: https://doi.org/10.4324/9781315867854.

13. Floridi L. Steps Forward in the Philosophy of Information. *SSRN Electronic Journal*. 2012. URL: https://doi.org/10.2139/ssrn.3859194.

14. Бандурка О. М., Головко О. М., Передерій О. С. Теорія держави і права : підручник. Харків : Харків. нац. ун-т внутр. справ, 2018. 416 с. URL: https://dspace.univd.edu.ua/entities/publication/4e4dfc1f-b477-48f3-9026-ad79be462141.

15. Козюбра М. І. Праворозуміння: поняття, типи та рівні. *Право України*. 2010. № 4. С. 10–21. URL: https://ekmair.ukma.edu.ua/handle/123456789/37290.

16. Погребняк С. П., Лук'янов Д. В. Порівняльне правознавство / Заг. ред. О. Петришин. Харків : Право, 2012. 272 с. URL: https://intrel.lnu.edu.ua/wp-content/uploads/2017/09/Петришин-ред.-Порівняльне-правознавство.pdf.

17. Тацій В. Я., Святоцький О. Д., Максимов С. І. Правова доктрина України / Заг. ред. О. В. Петришин. Харків : Право, 2013. Т. 1 : Загальнотеоретична та історична юриспруденція. 976 с.

18. Зозуля Є. В., Туренко О. С., Іванов І. В. Історія вчень про державу і право. Херсон : Олді-Плюс, 2018. 308 с. URL: https://org2.knuba.edu.ua/pluginfile.php/112035/mod_resource/content/1/posibnik_zozulia.pdf.

19. Earley J. E. Order Out of Chaos: Man's New Dialogue With Nature. *Process Studies*. 1985. Vol. 14, no. 3. P. 204–205. URL: https://doi.org/10.2307/44798209.

20. Данильян О. Г., Дзьобань О. П. Філософія інформаційного права : навч. посіб. Харків : Право, 2023. 322 с.

21. Gadamer H.-G. Truth and method. London : Bloomsbury, 2013. 623 p. URL: https://web.mit.edu/kaclark/www/gadamer_truth_and_method.pdf.

22. Застосування судами Конституції України: доктрина і практика :

монографія. Київ : BAITE, 2022. 604 с. URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/rizne/Monografua.pdf..

23. Баранов О. А. Правове забезпечення інформаційної сфери: теорія, методологія і практика : монографія. Київ : Едельвейс, 2014. 497 с. URL: https://www.academia.edu/24949621/Правове_забезпечення_інформаційної_сфери_теорія_методологія_і_практика_монографія.

24. Pylypchuk V. G. Theoretical and Legal Basis for the Security and Defense Strategic Communications System Development. *Journal of the National Academy of Legal Sciences of Ukraine*. 2019. Vol. 26, no. 3. P. 32–50. URL: https://doi.org/10.31359/1993-0909-2019-26-3-32.

25. Serrano A. S. The challenge of global cybersecurity. *Global Cybersecurity and International Law*. London, 2024. P. 230. URL: https://doi.org/10.4324/9781003344124-1.

26. Melaku H. M. A Dynamic and Adaptive Cybersecurity Governance Framework. *Journal of Cybersecurity and Privacy*. 2023. Vol. 3, no. 3. P. 327–350. URL: https://doi.org/10.3390/jcp3030017.

27. Rusydi M. T. Evaluating Global Cybersecurity Laws: Efectiveness of Legal Frameworks and Enforcement Mecanism in the Digital Age. *Walisongo Law Review*. 2024. No. 6(1). P. 71–83. URL: https://doi.org/10.21580/walrev.2024.6.1.20960.

28. Jaber A. Cybersecurity governance and political structures: Comparing centralized and decentralized approaches to cyber defense. *Comparative Strategy*. 2025. P. 752–771. URL: https://doi.org/10.1080/01495933.2025.2507310.

29. Adeyeri A., Abroshan H. Geopolitical Ramifications of Cybersecurity Threats: State Responses and International Cooperations in the Digital Warfare Era. *Information*. 2024. Vol. 15, no. 11. P. 682. URL: https://doi.org/10.3390/info15110682.

30. Tang R., Zhang W. Comparative Legal Perspectives on Cyberspace Security Governance: A Review of Frameworks and Implication. *Journal of Computer Science Research*. 2025. Vol. 7, no. 1. P. 1–10. URL: https://doi.org/10.30564/jcsr.v7i1.8555.

31. Rid T. Cyber War Will Not Take Place. *Journal of Strategic Studies*. 2012. № 35 (1). P. 5–32. DOI:10.1080/01402390.2011.608939.

32. World Economic Forum. Global Cybersecurity Outlook. Geneva : World Economic Forum, 2024. 39 p. URL: https://www.weforum.org/publications/global-cybersecurity-outlook-2024/.

33. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley & Sons, Incorporated, John, 2020. 1232 p. URL: https://doi.org/10.1002/9781119644682.

34. ENISA Threat Landscape 2024. *European Union Agency for Cybersecurity*. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

35. Schmitt M. N. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* / ed. by M. N. Schmitt. Cambridge, 2017. P. 638. URL: https://doi.org/10.1017/9781316822524.006.

36. Buchanan B. Hacker and the State: Cyber Attacks and the New Normal of Geopolitics. Harvard University Press, 2022. URL: https://doi.org/10.33458/uidergisi.1490691.

37. Цимбалюк В. С. Інформаційне право: концептуальні положення до кодифікації інформаційного законодавства : монографія. Київ : Освіта України, 2011. 426 с.

38. Баранов О. А. Інформаційне право України: стан, проблеми та перспективи розвитку. *Держава і право*. 2005. № 52. С. 225–231. URL: https://www.academia.edu/29215619/Інформаційне_право_України_стан_проблеми_перспективи.

39. Домбровський Л. В. Інформаційна безпека держави у системі національної безпеки України. *Вісник державного управління Національного університету цивільного захисту України. Серія: Державне управління*. 2024. № 1(20)2024. С. 109–116. URL: https://doi.org/10.52363/2414-5866-2024-1-12.

40. Дєгтяр О., Носков О., Мілевський К. Інформаційна безпека у сфері національної безпеки України в умовах сучасних викликів. *Національні інтереси України*. 2025. № 4(9). С. 117–129. URL: https://doi.org/10.52058/3041-1793-2025-4(9)-117-129.

41. History. *G.E. Pukhov Institute for Modelling in Energy Engineering. National*

Academy of Sciences of Ukraine. URL: https://ipme.kiev.ua/en/history-2/.

42. Костецька Т. А. До питання про державний контроль за дотриманням інформаційного законодавства: поняття, окремі види і форми. *Al'manah prava*. 2019. № 10. С. 312–318. URL: https://doi.org/10.33663/2524-017x-2019-10-312-318.

43. Cybersecurity Governance / K. B. Oh et al. Singapore : *Springer Nature Singapore*. 2025. 260 p. URL: https://doi.org/10.1007/978-981-95-3865-2.

44. Lashkari A. H., Lukings M. Understanding Cybersecurity Law in Data Sovereignty and Digital Governance: An Overview from a Legal Perspective. Cham : *Springer International Publishing AG*. 2022. URL: http://dx.doi.org/10.1007/978-3-031-14264-2.

45. Інформаційні війни сучасності та застосування мережецентричних систем управління військового призначення / О. В. Беспалько та ін. *Системи озброєння і військова техніка*. 2023. № 2 (74). С. 87–93. URL: https://doi.org/10.30748/soivt.2023.74.09.

46. Інформаційні війни та їх вплив на міжнародну репутацію країни / Є. Срібна та ін. *Бюлетень Національного університету водних ресурсів та екологічної інженерії*. 2024. Т. 4, № 108. С. 298–308. URL: https://doi.org/10.31713/ve4202427.

47. Марчук В. В. Національна безпека України : навч. посіб. Львів : Liha-Pres, 2025. 372 с. URL: https://doi.org/10.36059/978-966-397-494-1.

48. Інформаційна безпека: філософське та організаційно-правове підґрунтя рефлексії національних інтересів україни / О. Данильян та ін. Харків : Нац. юрид. ун-т ім. Ярослава Мудрого, 2024. 224 с.

49. Селіхов Д. Кібербезпека як складова інформаційної безпеки: теоретичні та прикладні аспекти. *Аналітично-порівняльне правознавство*. 2026. Вип. 1, №. 1. С. 94–99. URL: https://doi.org/10.24144/2788-6018.2026.01.1.14.

50. Nye J. S. Soft Power and Great-Power Competition. Singapore : *Springer Nature Singapore*. 2023. URL: https://doi.org/10.1007/978-981-99-0714-4.

51. Singer P. W., Brooking E. T. LikeWar: The Weaponization of Social Media. Houghton Mifflin Harcourt Publishing Company, 2018. 400 p.

URL: https://www.researchgate.net/publication/335149861_Like_War_-_The_Weaponization_of_Social_Media_by_P_W_Singer_and_Emerson_T_Brooking?__cf_chl_tk=eFKDuyRmHdCnlxlzolRerH58.lEiGdOvF6ywHI8VFaM-1773765578-1.0.1.1-rVpN7xjAHR3RYAZiiwd6DSkn5q7PY1BGuuwc7SV.QZ0.

52. Wardle C., Derakhshan H. Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. Strasbourg : Council of Europe, 2017. 107 p. URL: https://www.researchgate.net/publication/339031969_INFORMATION_DISORDER_Toward_an_interdisciplinary_framework_for_research_and_policy_making_Information_Disorder_Toward_an_interdisciplinary_framework_for_research_and_policy making.

53. Bradshaw S., Howard P. N. The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation. Oxford : Oxford Internet Institute, University of Oxford, 2019. 26 p. URL: https://www.oii.ox.ac.uk/news-events/reports/the-global-disinformation-order-2019-global-inventory-of-organised-social-media-manipulation/.

54. Michael G. A Review of: "Richard A. Clarke and Robert K. Knake.Cyber War: The Next Threat to National Security and What To Do About It.". *Terrorism and Political Violence*. 2010. Vol. 23, no. 1. P. 124–126. URL: https://doi.org/10.1080/09546553.2011.533082.

55. Floridi L. Ethics after the information revolution. *The Ethics of Information*. 2013. P. 1–18. URL: https://doi.org/10.1093/acprof:oso/9780199641321.003.0001.

56. ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected. European Union Agency for Cybersecurity (ENISA), 2020. URL: https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020.

57. Cavelty M. D. Cyber-Security and Threat Politics: US Efforts to Secure the Information Age. Taylor & Francis Group, 2007. 192 p. URL: https://www.researchgate.net/publication/277714726_Cyber-Security_and_Threat_Politics_US_Efforts_to_Secure_the_Information_Age.

58. Kello L. Virtual Weapon and International Order. Yale University Press, 2019.

320 p. URL: https://doi.org/10.12987/9780300226294.

59. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. / M. Brundage et al. University of Oxford, 2018. 101 p. URL: https://doi.org/10.48550/arXiv.1802.07228.

60. Information terrorism as a threat to the global security system of the 21st century / Y. Kobets et al. *Cuestiones Políticas*. 2022. Vol. 40, no. 75. P. 274–284. URL: https://doi.org/10.46398/cuestpol.4075.18.

61. OECD Reviews of Risk Management Policies Good Governance for Critical Infrastructure Resilience. Paris : OECD Publishing, 2019. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/04/good-governance-for-critical-infrastructure-resilience_7d5a9993/02f0e5a0-en.pdf.

62. Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe / T. Helmus et al. RAND Corporation, 2018. URL: https://doi.org/10.7249/rr2237.

63. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization : of 19.11.2010. URL: https://www.nato.int/content/dam/nato/legacy-wcm/media_pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf.

64. Strategic Communications Centre of Excellence : Annual Report of 31.12.2021. URL: https://stratcomcoe.org/uploads/Gada%20Parskati/Annual_Report_2021_audited.pdf.

65. Tackling Online Disinformation: A European Approach. : of 26.04.2018 no. COM(2018) 236. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018DC0236.

66. Наливайко Л.Р., Вітвіцький С.С. Право на доступ до публічної інформації в контексті контролю громадян за діяльністю держави. *Право і суспільство*. 2014. No 5(2). С. 28–33.

67. Nalyvaiko L. R. Transparency as a democratic standard of the government functioning. *Evropský Politický a Právní Diskurs*. 2014. Svazek 1., 4. vydání. C. 51–62.

68. Наливайко Л. Р., Грицай І., Дніпров О. С. Неурядові правозахисні організації України : навч. посіб. Київ : Хай-Тек Прес, 2014. 432 с.

69. Гуровський В. О. Роль органів державної влади у сфері забезпечення інформаційної безпеки України. Вісник Української академії державного управління при Президентові України. 2014. № 3. С. 21-31.

70. Ліпкан В. А. Сучасний зміст інформаційних операцій проти України. Міжнародна інформаційна безпека: сучасні концепції і практика: матер. другої наук. конф. (Київ, 18 березня 2011р.). Київ: Київський національний університет імені Тараса Шевченка Інститут міжнародних відносин, 2011. С. 34-43.

71. Лобода Д. О. Прямухіна Н. В. Боротьба з дезінформацією як частина інформаційної безпеки держави. *Прикладні аспекти сучасних міждисциплінарних досліджень*: мат. ІІ Міжн. науково-практ. конф. (24 листопада 2023 р., м. Вінниця). Вінниця: ДонНУ імені Василя Стуса, 2024. С. 95-96.

72. Лугіна Н. А. Кібербезпека в умовах війни. Свобода, безпека та незалежність: правовий вимір: мат. XIII Міжн. науково-практ. конф. (24 лютого 2023 р. м. Київ). Київ: Національний авіаційний університет, 2023. С. 346-349.

73. Милосердна І. М. Інформаційна безпека як елемент національної безпеки: теоретичний вимір та особливості впровадження. *Науковий журнал «Політикус».* 2024. № 4. С. 179-185.

74. Fruhlinger J. What is information security? Definition, principles, and jobs. CSO United States. 2020. URL: https://www.csoonline.com/article /3513899/what-is-information-security-definitionprinciples-and-jobs.html.]

75. Інформаційна безпека. Навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. Харків: Вид. ХНЕУ, 2008. 352 с.

76. Сопілко І. М. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. *Юридичний вісник*. 2021. № 2 (59). С. 110-115.

77. Словник української мови: в 11 тт. / АН УРСР. Інститут мовознавства; за ред. І. К. Білодіда. Київ: Наукова думка, 1970-1980. Т. 1.

78. Словарь української мови: в 4-х тт. / За ред. Б. Грінченка. Київ., 1907-1909. Т. 1.

79. Словник української мови : в 11 т. / АН Української РСР, Ін-т мовознав. ім. О. О. Потебні ; редкол.: І. К. Білодід. Київ : Наук. думка, 1970-1980. Т. 4 : І-М / ред.

тому: А. А. Бурячок, П. П. Доценко. 1973. 840 с.

80. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с.

81. Шемчук В.В. Інформаційна безпека та інформаційна оборона в контексті розвитку вітчизняної доктрини й законодавчої основ. Вчені записки ТНУ імені І.В. Вернадського. Серія: юридичні науки. Том 30 (69) No 4 2019. С. 31-37.

82. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки. Інтернет архів Waybackmachine. 2015.: веб-сайт. URL: https://web.archive.org/web/20151110042232/http://journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php.

83. Інформаційна безпека держави: навч. посіб. / В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. 166 с.

84. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: навч. посібник. Київ, 2004. 384 с.

85. Лук'янова В. В., Лаутар А. Ю.Інформаційна безпека в умовах розвитку інформаційної системи. *Вісник Хмельницького національного університету. Економічні науки.* 2013. № 2. Т. 3. С. 97-101.

86. Данільян О.Г. Національна безпека України: сутність, структура та напрямки реалізації : навчальний посібник / О.Г. Данільян [та ін.]. Х. : Фоліо, 2002. 285 с.

87. Баранов О. П. Передумови створення Державної спеціальної служби транспорту та її завдання в системі національної безпеки України / О.П. Баранов // Вісник Національної академії державного управління при Президентові України. 2014. № 3. С. 60-65., с. 60-62

88. Петрик В.М., Галамба М.В. Інформаційна безпека України: поняття, сутність та загрози. *Юридичний журнал*. 2006. №11. С. 49-52.

89. Тихомиров О.О. Перспективи зміни розуміння інформаційної безпеки // Правова інформатика. 2010. № 4 (28). С. 68-75.

90. Фокіна-Мезенцева К. Інформаційна безпека у глобальному суспільстві. *Scientia fructuosa*. 2021. № 139 (5). С. 61-71.

91. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: навчальний посібник. Київ : КНТ, 2006. 280 с.

92. Малашко О. Є., Ковалів М. В. Теоретична конструкція поняття «інформаційна безпека». *Міжнародний науковий журнал «Інтернаука». Серія: «Юридичні науки».* 2020. № 10. https://doi.org/10.25313/2520-2308-2020-10-6350.

93. Ісмайлов К.Ю. Поняття «кібезбезпека та «інформаційна безпека». Типологія безпеки. *Міжнародна науково-практична конференція «Актуальні проблеми автоматизації та управління».* Луцьк. 2016.

94. Про національну безпеку України: Закон України від 21 червня 2018 р. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.

95. Стратегія інформаційної безпеки, затверджена Указом Президента України від 28 грудня 2021 року № 685/2021. https://www.president.gov.ua/documents/6852021-41069.

96. Наливайко Л.Р. Інформаційна безпека та інформаційна політика в Україні: конституційно-правовий аспект. *Вісник Запорізького державного університету*. 2003. №1. С. 60-65.

97. Гончаренко Г.А. До проблеми визначення та розмежування дефініцій «інформаційна безпека» і «кібербезпека». Аналітично-порівняльне правознавство. 2024. № 5. С. 466-471.

98. Харченко Л.С., Ліпкан В А., Логінов О.В.Інформаційна безпека України: Глосарій І За загальною редакцією доктора юридичних наук, професора Р. А. Калюжного. Київ : «Текст», 2004. 180 с.

99. Литвиненко О.В. Проблеми забезпечення інформаційної безпеки в пострадянських країнах (на прикладі України та Росії) : автореф. дис. ... канд. політ. наук. Київ, 1997.18 с.

100. Ткачук Т.Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір : монографія. Київ: ТОВ «Видавничий дім «АртЕк», 2018. 422 с.

101. Марущак А.І. Інформаційне право: доступ до інформації: навч. посіб. для

студ. ВНЗ. Київ, 2007. 531 с.

102. Перун Т. С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні: дис. … канд. юрид. наук. Львів, 2019. 268 с.

103. Воропаєва Т., Авер'янова Н. Штучний інтелект в системі інформаційної безпеки україни в умовах російсько-української війни. *Collection of Scientific Papers «SCIENTIA»* (August 23, 2024; Valencia, Spain). P. 62–67.

104. Золотар О.О. Інформаційна безпека людини:теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с.

105. Косогов О.М. Інформаційна безпека у сфері оборони як складова воєнної безпеки України. Системи обробки інформації. 2016. Вип. 8 (145). С. 115–117.

106. Левченко О. В. Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування : монографія. Житомир : Видавець ПП "Євро-Волинь", 2021. 172 с.

107. Богданович В. Ю., Ворович Б. О., Марко Є. І. Інформаційна безпека як основа воєнної безпеки держави та суспільства. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України.* 2018. № 3 (64). С. 44-48.

108. Нижник Н.Р., Ситник Г.П., Білоус В.Т. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): Навчальний посібник І За заг. ред. П.В. Мельника, Н.Р.Нижник. - Ірпінь, 2000.-304 с, с. 5.

109. Аніщук В.В. Інформаційна безпека як об'єкт посягання злочинів проти основ національної безпеки України. *Науковий вісник Ужгородського національного університету. Серія ПРАВО*. 2023. № 77. Ч. 2. С. 139-143.

110. Авер'янова Н., Воропаєва, Т. Інформаційна безпека україни: соціально-філософські аспекти. Молодий вчений, 2020. № 10 (86). С. 297-303.;

111. Бондар І.Р. Інформаційна безпека як основа національної безпеки. *Механізм регулювання економіки*. 2014. № 1. С. 68–75.

112. Войціховський А. В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). *Вісник Харківського національного університету імені В. Н. Каразіна. Серія "ПРАВО"*. 2020. № 29. С.

281–288. DOI: 10.26565/2075-1834-2020-29-38.

113. Правові засади інформаційної безпеки України: монографія / П. Д. Біленчук, Л. В. Борисова, І.М. Неклонський., В.О. Собина; за ред. П.Д. Біленчука. Харків: 2018. 289 с.

114. Гаврильців М.Т. Інформаційна безпека держави в системі національної безпеки України. Юридичний науковий журнал. 2020. № 2. С. 200-203.

115. Кононенко В.П, Новікова Л.В., Копицька П.О. Політика міжнародних організацій з питань інформаційної безпеки. Науковий вісник Ужгородського національного університету. Серія Право. 2021. No 65. Т. 1. С. 353–358.;

116. Котляров, В. Аналіз сучасного стану інформаційної безпеки в україні. *Mechanism of an Economic Regulation*. 2024. №2 (104). С. 101-104.

117. Конах В. К. Забезпечення інформаційної безпеки держави як складової системи національної безпеки (приклад США): дис. ... канд. політ. наук: 21.01.01. Київ, 2005. 171 с.;

118. Кучер В.О. Права людини та інформаційна безпека в умовах військової агресії. *Науковий вісник Ужгородського Національного Університету. Серія ПРАВО.* 2024. № 81. Ч. 1. С. 125-130.

119. Медвідь Ф. М. Інформаційна безпека україни: генеза і становлення. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління.* 2024. № 2 (25). С. 116-122.

120. Ряполов А. П. Захист інформаційного простору України в умовах гібридної війни: межі між свободою слова та інформаційною безпекою. *Національні інтереси України.* 2025. № 5 (10). С. 746-757.

121. Мужанова Т. М. Інформаційна безпека держави: навчальний посібник. Київ: [б.в.], 2019. 131 с.

122. Панченко О. Інформаційна складова національної безпеки. *Вісник Національної академії Державної прикордонної служби України. Серія: державне управління.* 2019. № 3. https://periodica.nadpsu.edu.ua/index.php/governance/article/view/296/297.

123. Русакевич А. Інформаційна безпека в умовах воєнного стану у аспекті

забезпечення інформаційних прав громадян. *Law. State. Technology*. 2024. №2. С. 58-62.

124. Старостін О. Ю. Забезпечення інформаційної безпеки як складової національної безпеки України. *Вісник кримінологічної асоціації України.* 2024. № 1 (31). С. 466-474.

125. Супрун В. М. Інформаційний суверенітет як один з елементів інформаційної безпеки держави: теоретико-правовий аспект. http : // www.nbuv.gov.ua/portal/natural/vkhnu / Pravo / 2009.

126. Торяник В. М. Інформаційна безпека як складова національної безпеки держави. Роль ЗМІ в забезпечення інформаційного суверенітету України. *Право і Суспільство*. 2016. №2. С. 151-156.

127. Шевчук М.О. До питання генези поняття інформаційної безпеки як складової національної безпеки. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2023. Т.2. No78. С. 134-139.

128. Біленчук П.Д. Правові засади інформаційної безпеки України. Харків, 2018. 289 с.

129. Остапенко О., Баїк О. Адміністративно-правова природа інформаційної безпеки. *Вісник Національного університету «Львівська політехніка». Серія: «Юридичні науки».* 2021. № 3(31). С. 167 179.

130. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України : монографія. Одеса : Юридична література, 2003. 472 с.

131. Дзьобань О. П., Панфілов О. Ю., Чемчикаленко Р. А. Методологічний контекст дослідження проблеми інформаційної безпеки. *Зовнішня торгівля: економіка, фінанси, право*. 2014. № 2. С. 171–180.

132. Лизанчук В.В. Інформаційна безпека України: теорія і практика: підручник. Львів: ЛНУ ім. Івана Франка, 2017. 725 с.

133. Довгань О.Д. Правові засади формування і розвитку системи забезпечення інформаційної безпеки України. *Інформаційна безпека людини, суспільства, держави*. 2015, No 3 (19). С. 6-17.

134. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та

інформаційна безпека: сутність, визначення, відмінності. *Інформація і право*. 2012. № 2(5). С. 162-175.

135. Боднар І.Р. Державна політика та інформаційна безпека України: післякризові виклики. *Актуальні проблеми післякризового відновлення економіки України:* Зб. мат. наук.-прак. конференції викладацького складу і аспірантів навчальнонаукового комплексу "Академія". Л., 2013.

136. Кузьменко А. М. Особливості проблем законодавчого забезпечення інформаційної безпеки держави, суспільства і громадянина в умовах інформаційно-психологічного протиборства. Часопис Київського університету права. 2010. No 4. С. 317–321.

137. Барабаш О. О. Право на інформаційну безпеку як складова права людини на безпеку: концептуальні положення захисту інформаційних прав. *Юридичний науковий електронний журнал*. 2024. № 2. С. 560-563.

138. Торічний В.О. Проблема інформаційної безпеки в умовах розвитку інформаційного суспільства. *Теорія та практика державного управління.* 2019. № 2 (65). С. 256-252.

139. Інформаційна безпека (соціально-правові аспекти) : підручник / В. В. Остроухов, В. М. Петрик, М. М. Присяжнюк та ін. Київ: КНТ, 2010. 776 с.

140. Смотрич Д., Бріалко Л. Інформаційна безпека в умовах воєнного стану. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2023. Вип. 77 , ч. 2. С. 121-127.

141. Морозов О.Л. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності. *Віче*. 2007. No12. С. 23-25.

142. Котерлін І. Б. Інформаційна безпека в умовах воєнного стану у аспекті забезпечення інформаційних прав та свобод. *Актуальні проблеми вітчизняної юриспруденції.* 2022. № 1. С. 145-150.

143. Інформаційна безпека. Менеджмент інформаційної безпеки держави : курс лекцій: навч. посіб. / В. О. Ананьїн, В. В. Горлинський, А. В. Гангал. ІСЗЗІ КПІ ім. Ігоря Сікорського. Електронні текстові дані (1 файл: 2,73 Мбайт). Київ : ІСЗЗІ КПІ ім. Ігоря Сікорського 2025. 140 с.

144. Ряполов А. П. Інституційне забезпечення інформаційної безпеки України. *Конституційні права і свободи людини та громадянина в умовах війни та післявоєнний період* : матер. наук. семінару, м. Львів, 21 червня 2024 р. Львів : ЛьвДУВС, 2024. С. 167-170.

145. Пилипчук В., Дзьобань О. Глобальні виклики й загрози національній безпеці в інформаційній сфері. *Вісник Національної академії правових наук України*. No 3 (78) 2014. С. 43-52.

146. Новицький В.Я. Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах. *Інформація і право.* 2022. № 1(40). С. 111-118.

147. Соломін Є. О. Інформаційна безпека в умовах війни та втручань у медіасередовище. Держава та регіон. Серія: Соціальні комунікації. 2023. № 2(54). С. 40-47.

148. Клочко А. Забезпечення інформаційної безпеки в умовах сучасного суспільства. *Наукові праці Міжрегіональної академії управління персоналом. Політичні науки та публічне управління*. 2022. №3 (63). С. 38-42.

149. Ряполов А. П. Інформаційна безпека України в умовах воєнного стан: проблеми та перспективи. *Юридична весна: права людини в умовах воєнного стану: з*бірник тез Науково-практичної конференції (м. Харків, 15 квітня 2024 року). Харків : Національний юридичний університет імені Ярослава Мудрого, редкол.: А. М. Мерник, М. Д. Вовченко. 2024. 215 с.

150. Buzan B., Wæver O., Wilde J. Security: A New Framework for Analysis. Lynne Rienner Pub, 1997. 239 p.

151. Libicki M. C. Cyberdeterrence and Cyberwar. RAND Corporation, 2009. 238 p. https://www.jstor.org/stable/10.7249/mg877af.

152. Nye J. Protecting Democracy in an Era of Cyber Information War. Belfer Center for Science and International Affairs. Cambridge, MA: Harvard Kennedy School, 2019. URL: https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/ProtectingDemocracy.pdf.

153. Van Niekerk, B. Cyber Operations in Peace and War: A Framework for Persistent Engagement. *International Conference on Cyber Warfare and Security*. 2024. №

19 (1). P. 395–404. https://doi.org/10.34190/iccws.19.1.2092.

154. Liebetrau T. Cyber conflict short of war: a European strategic vacuum. *European Security*. 2022. № 31. P. 497–516. https://doi.org/10.1080/09662839.2022.2031991.

155. Ruohonen J., Rindell K., Busetti S. From Cyber Security Incident Management to Cyber Security Crisis Management in the European Union. *Computers & Security*. 2025. № 159. 104689 p. https://doi.org/10.1016/j.cose.2025.104689.

156. Gouliev Z. Propaganda and information dissemination in the Russo-Ukrainian war: natural language processing approaches to information warfare analysis. arXiv preprint. 2025. URL: https://arxiv.org/abs/2506.01807.

157. Fyshchuk I., Noesgaard M., Nielsen J. Managing cyberattacks in wartime: The case of Ukraine. *Public Administration Review*. 2024. № 85. P. 619–627. https://doi.org/10.1111/puar.13895.

158. Carrapico H., Farrand B. The new geopolitics of EU cybersecurity: security, economy and strategic autonomy. *International Affairs*. 2024. № 6 (100). P. 2379–2397. http://dx.doi.org/10.1093/ia/iiae231.

159. Радутний О. Е. Об'єкт суспільно небезпечних посягань на відносини, предметом яких виступають окремі види інформації. *Проблеми законності*. 2009. № 104. С. 177–188. https://dspace.nlu.edu.ua/handle/123456789/2701.

160. Радутний О. Е. Інформація як універсальний предмет злочинів. *Держава і право. Юридичні і політичні науки*. 2009. № 46. С. 458–462. https://nasplib.isofts.kiev.ua/handle/123456789/9132.

161. Радутний О. Е. Публічні заклики та заперечення як форми інформаційної колаборaційної діяльності за Кримінальним кодексом України. 2022. *Інформація і право*. № 2 (41). С. 99–115. http://jnas.nbuv.gov.ua/article/UJRN-0001355254ю

162. Ліпкан В. А. Інформаційна безпека як складова національної безпеки України. *Інформаційні технології в економіці, менеджменті і бізнесі: Проблеми науки, практики і освіти* : Зб. наук. праць VIII Міжнар. наук.-практ. конф. Ч. 2. Київ : Вид-во Європ. ун-ту, 2003. С. 443–453.

163. Semenenko O., Palamarchuk S., Poberezhets T., Palamarchuk N., Mytchenko S.

Cybersecurity in Modern Armed Conflicts: Threats and Responses. *International Journal of Advances in Soft Computing and its Applications*. 2025. № 17 (1). P. 32–48. DOI: 10.15849/IJASCA.250330.03.

164. Медіадискурс війни: український та закордонний досвід : монографія / [М. Житарюк, Т. Балда, Т. Лильо та ін.] ; наук. ред., упорядк., вступ, висновки проф. М. Житарюк. Веб-версія. Львів : ЛНУ імені Івана Франка, 2025. 296 с.

165. Kuperstein L., Lukichov V., Radetska A., Dudatyev A. System for Organizing Cyber Operations in the Context of Military Aggression. *Science and Innovation*. 2025. № 21 (3). P. 86–98. https://doi.org/10.15407/scine21.03.086.

166. Ignatiev A., Burlakov S., Terletski A., Skryl S., Shovkun Y. (2025). Assessing modern challenges and threats affecting national security by full-scale military operations. *Dixi*. .025. № 27 (2). P. 1–14. https://doi.org/10.16925/2357-5891.2025.02.02/

167. Kravchenko O., Veklych V., Krykhivskyi M., Madryha T. Cybersecurity in the face of information warfare and cyberattacks. *Multidisciplinary Science Journal*. 2024. № 6. https://doi.org/10.31893/multiscience.2024ss0219.

168. Parkhomenko-Kutsevil O. Problems of information security during military operations and hostilities. *Public management and administration in Ukraine*. 2022. № 29. P. 89–93. https://doi.org/10.32843/pma2663-5240-2022.28.35/

169. Грабар Н. С. Зарубіжний досвід правового регулювання забезпечення інформаційної безпеки. *Теорія та практика державного управління і місцевого самоврядування*. 2020. № 1. DOI: https://doi.org/10.35546/kntu2308-8834/2020.1.2.

170. Ковальов К. Є. Інформаційна безпека: міжнародно-правовий аспект. *Інформація і право*. 2023. № 4. С. 159–167. http://nbuv.gov.ua/UJRN/Infpr_2023_4_17.

171. Шемчук В.В. Конституційно-правове забезпечення інформаційної безпеки сучасних держав: порівняльно-правовий аналіз : дис. … док-ра юрид. наук : 12.00.02. Ужгород, 2020. 410 с.

172. Ржевська Н. Ф. Сучасна інформаційна політика: досвід США для України. *Політичні дослідження*. 2024. № 1. С. 68–85.

173. Буга Л. В. Досвід США та Німеччини щодо забезпечення інформаційної безпеки в Збройних силах України. *Наукові записки Львівського університету бізнесу*

і права. 2018. № 19. С. 174–178.

174. Шемчук В. В. Зарубіжний досвід забезпечення інформаційної безпеки держави. *Порівняльно-аналітичне право*. 2019. № 2. С. 34–40. https://dspace.lvduvs.edu.ua/handle/1234567890/6820.

175. Таран Є. І. Державна політика забезпечення інформаційної безпеки у США та ЄС. *Вісник Львівського університету. Серія філос.-політолог. студії*. 2019. № 26. С. 201–207. DOI https://doi.org/10.30970/2307-1664.2019.26.25.

176. Недохлєбов І. І. Інформаційна безпека України в умовах сучасних загроз: організаційно-правові аспекти : дис. ... канд. юрид. наук : 12.00.07. Запоріжжя, 2024. 240 с.

177. Izmailov Y., Yegorova I. Possibilities of adapting the EU experience in information security to the conditions of Ukraine. *Economics and Technical Engineering*. 2023. № 1 (1). P. 35–43. https://doi.org/10.62911/ete.2023.01.01.03.

178. Пугачов О. Зарубіжний досвід забезпечення інформаційної безпеки держави. *Проблеми сучасних трансформацій. Серія «Право, публічне управління та адміністрування».* 2024. № 13. С. 2–7.

179. Buzan B. People, States and Fear: An Agenda for International Security Studies in the Post Cold War Era. New York : Harvester Wheatsheaf, 1991. 393 p.

180. NATO’s approach to counter information threats. URL: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/10/18/natos-approach-to-counter-information-threats.

181. A strategic compass for security and defence. URL: https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf.

182. Questions relating to information : resolutions / adopted by the General Assembly. United Nations General Assembly, 79th session. Resolution A/RES/79/93 A–B, 12 December 2024. URL: https://docs.un.org/en/A/RES/79/93a-b.

183. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act. URL: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf.

184. National Emergencies Act. URL: https://www.law.cornell.edu/

uscode/text/50/chapter-34.

185. Civil Contingencies Act. URL: https://www.legislation.gov.uk/ukpga/2004/36/contents

186. Investigatory Powers Act. URL: https://www.legislation.gov.uk/ukpga/2016/25/contents.

187. Emergency Powers (Defense) Regulations. URL: https://www.nevo.co.il/law_html/law01/320_001.htm.

188. Loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence. URL: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000696350.

189. Basic Law (Grundgesetz). URL: https://www.gesetze-im-internet.de/englisch_gg/.

190. Emergency Act. URL: https://www.riigiteataja.ee/en/eli/512062020001/consolide.

191. Cybersecurity Act. URL: https://www.riigiteataja.ee/en/eli/519082024019/consolide.

192. Law on the State of Emergency. URL: https://e-seimasx.lrs.lt/rs/legalact/TAD/29e103b04aaf11f0a19dcea0bcc863ad/.

193. Case of Handyside v. the United Kingdom (Application no. 5493/72) : Judgment of the ECtHR, 7 December 1976 // HUDOC. URL: https://hudoc.echr.coe.int/eng?i=001-57499.

194. Case of Leander v. Sweden (Application no. 9248/81) : Judgment of the ECtHR, 26 March 1987 // HUDOC. URL: https://hudoc.echr.coe.int/eng?i=001-57519.

195. Case of Şener v. Turkey (Application no. 26680/95) : Judgment of the ECtHR, 18 July 2000 // HUDOC. URL: https://hudoc.echr.coe.int/eng?i=001-58753.

196. Чернухін І. О. Досвід Федеративної Республіки Німеччини в побудові системи захисту інфраструктури від кібернетичних загроз. *Information Security of the Person, Society and State*. 2014. № 1 (14). С. 27–43.

197. Про правовий режим воєнного стану: Закон України від 12.05.2015. *Відомості Верховної Ради України.* 2015. № 28. Ст. 250.

198. Валюшко І.О. Інформаційна безпека України в контексті російсько-

українського конфлікту: дис. … канд. політ. наук (доктора філософії). Миколаїв, 2018. 210 с.

199. Золотар О.О. Генеза суспільних відносин щодо інформаційної безпеки людини. Інформація і право. 2018. No 1 (24). С. 139–148.

200. Проць І. М. Правове регулювання інформаційної безпеки у державному управлінні. *Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України:* мат. Науково-практ. конф. (Львів, 22 грудня 2023) / упорядник: Т. В. Магеровська. Львів : ЛьвДУВС, 2024. С. 138-139.

201. Конституція України : від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.

202. Антонов В. О. Проблема формування нової нормативно-правової бази національної безпеки України на тлі нових викликів та загроз. Часопис Київського університету права. 2015. №3. С.70-73.

203. Про оборону України: Закону України від 06.12.1991 р. *Відомості Верховної Ради України.* 1992. № 9. Ст. 106.

204. Про інформацію : Закон України від 02.10.1992 № 2657-XII : URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

205. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

206. Про Стратегію інформаційної безпеки»: Указ Президента України від 14.05.2021 р. № 187/2021. *Президент України*. URL : https://zakon.rada.gov.ua/laws/show/187/2021.

207. Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021. https://zakon.rada.gov.ua/laws/show/447/2021#Text.

208. Статут Організації Об’єднаних Націй: Міжнародний документ від 26 червня 1945 р. https://unic.un.org/aroundworld/unics/common/documents/publications/uncharter/UN%20Charter_Ukrainian.pdf.

209. План дій Ради Європи для України «Стійкість, відновлення та відбудова на

2023-2026 рр., затверджений Комітетом міністрів Ради Європи 14 грудня 2022 р. CM/Del/Dec(2022)1452/2.4) https://rm.coe.int/action-plan-ukraine-2023-2026-ukr/1680aa8282.

210. Про рішення Ради національної безпеки і оборони України від 19.03.2021 р. «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»: Указ Президента України від 23.03.2021 р. № 109/2021. *Президент України*. URL : https://zakon.rada.gov.ua/ laws/show/109/2021.

211. Кримінальний кодекс України : Кодекс України від 05.04.2001 № 2341-III : URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

212. Про телебачення і радіомовлення: Закон України від 21.12.1993 р. № 3759-XII. Верховна Рада України. URL : https://zakon.rada.gov.ua/laws/show/ 3759-12.

213. Корх О., Решетніченко А., Романенко В. Публічне управління процесами інформаційної безпеки держави. URL: http://www.kbuapa.kharkov.ua/e-book/putp/2010-2/doc/2/04.pdf.

214. Троянський, О. А. Інформаційна безпека в Україні: сучасний стан та перспективи розвитку. *Науковий вісник Льотної академії. Серія: Економіка, менеджмент та право*. Випуск 5. Київ : "Центр учбової літератури", 2021. С. 185-194.

215. Рижков Е. В. Законодавче забезпечення інформаційної безпеки України в умовах воєнного стану. *Інформаційно-аналітичне забезпечення діяльності органів сектору безпеки і оборони України:* мат. Науково-практ. конф. (Львів, 22 грудня 2023) / упорядник: Т. В. Магеровська. Львів : ЛьвДУВС, 2024. С. 140-142.

216. Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018. EUR-Lex. URL : https://eur-lex.europa.eu/eli/dir/2018/1808/oj.

217. Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, Grand Chamber Judgment of 27 June 2017. *HUDOC*. URL : https://hudoc.echr.coe.int/ fre?i=001-175121.

218. Білодід І. К. Словник української мови: в 11 т. Київ: Наук. думка, 1972. Т. 3: З. 744 с.

219. Загальна теорія держави та права : підручник для студентів юридичних

вищих навчальних закладів / М.В. Цвік, О.В. Петришин, Л.В. Авраменко та ін.; за ред. д-ра юрид. наук, проф., акад. АПрН України М.В. Цвіка, д-ра юрид. наук, проф., акад. АПрН України О.В. Петришина. Харків : Право, 2011. 584 с.;

220. Рабінович П. М. Проблеми юридичного забезпечення прав людини (загальнотеоретичний аспект). *Український часопис прав людини*. 1995. No 2. С. 16–23.

221. Марцеляк О.В. Інститут омбудсмена: теорія і практика. Харків : Вид-во Нац. ун-ту внутр. справ, 2004. 206 с.

222. Волинка К. Механізм забезпечення прав і свобод особи: питання теорії і практики : автореф. дис. ... канд. юрид. наук : спец. 12.00.01. Київ, 2000. 25 с.

223. Степаненко К. Адміністративно-правове забезпечення прав і свобод громадян України за кордоном : дис. ... канд. юрид. наук : спец. 12.00.07. Дніпропетровськ, 2009. 229 с.

224. Ієрусалімова І. Механізм адміністративно-правового забезпечення прав і свобод людини та громадянина : дис. ... канд. юрид. наук : спец. 12.00.07. Київ, 2006. 84 с.

225. Наливайко Л. Р. Державний лад України: теоретико-правова модель: монографія. Харків: Право, 2009. 600 с.

226. Мінакова Є.В. Інституційна система забезпечення прав і свобод внутрішньо переміщених осіб в умовах воєнного стану: теоретичні та правові аспекти. *Наука і техніка сьогодні*. 2023. №12 (26). С. 201.

227. Наливайко І. Ефективність правового регулювання соціальних стандартів та гарантій: проблеми та перспективи. *Наукові перспективи*. 2023. № 7 (37). С. 494-509.

228. Опольська Н. Механізм забезпечення прав та свобод людини у динамічному вимірі. *Підприємництво, господарство і право*. 2019. № 4. С. 191-195.

229. Олійник О. В. Теоретико-методологічні засади адміністративно-правового забезпечення інформаційної безпеки України: монографія. К. : Укр. Пріоритет, 2012. 400 с.

230. Ткачук Т. Суб’єкти забезпечення інформаційної безпеки держави:

функціональний аналіз. *Jurnalul juridic naţional: teorie şi practică.* 2017. № 6. С. 42-46.

231. Радовецька Л. В. Суб'єкти забезпечення державної безпеки України: теоретикоправові аспекти: автореф. дис.... канд. юрид. наук. Київ, 2015. 24 с.

232. Тихомиров О. О. Діяльнісний підхід у дослідженнях забезпечення інформаційної безпеки: об'єкти і суб'єкти. *Інформаційна безпека людини, суспільства, держави.* 2012. № 2 (9). С. 18-24.

233. Довгань О. Д., Ткачук Т. Ю. Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс. *Інформація і право*. 2018. № 2 (25). С. 73-85.

234. Маслій І. В. Інституційний механізм протидії криміналізації економіки: кримінологічне дослідження: дис. ... канд. юрид. наук. Одеса, 2015. 228 с.

235. Правове забезпечення інформаційної діяльності в Україні / [заг. ред. Ю. С. Шемшученко, І. С. Чиж]. Київ : ТОВ «Вид-во Юридична думка», 2006. 384 с.

236. Білько С. Інституційне забезпечення інформаційної безпеки України. *Науковий журнал «Економіка і регіон».* 2021. Т. 3 (82). С. 36-41.

237. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України: дис. … доктора юр. наук: спец. Одеса, 2004. 427 с.

238. Словник української мови : у 20 т. / НАН України, Укр. мов.-інформ. фонд. Київ: Наукова думка, 2010. Т. 6: Згага — Кварта / [уклад.: І. В. Шевченко та ін.; наук. ред.: О. О. Тараненко, С. Я. Єрмоленко]. Київ: Укр. мов.-інформ. фонд, 2015. 991 с.

239. Ткачова О. К. Специфіка інституціоналізації в сфері управління митною справою. *Державне управління: удосконалення та розвиток*. 2012. № 1. http : //www.dy.nayka.com.ua.

240. Іншаков О. В., Фролов Д. П. Інституція – ключ до розуміння економічних інститутів. *Економічна теорія*. 2011. № 1. С. 52-62.

241. Фелонюк Д. Л. Сучасна екологічна політика України: правові засади інституційно-функціонального забезпечення формування та здійснення: автореф. дис. ... канд. юрид. наук: 12.00.06. Одеса, 2023. 20 с.

242. Макаренко Н. А. Правове регулювання екологічної безпеки в сфері видобування нафти і газу в Україні: автореф. дис. ... канд. юрид. наук: 12.00.06. Київ,

2015. 18 с.

243. Ломакіна І. Ю. Державно-правове регулювання сільського господарства в Україні.: автореф. дис. ... канд. юрид. наук: 12.00.06. К., 2010. 19 с.

244. Леоненко Н.А., Поступна О.В. Інформаційна безпека України : механізми, сучасні виклики та загрози в умовах інформаційного глобалізму. *Вісник НУЦЗ України. Серія: Державне управління.* 2022. № 2 (17). С. 113-120.

245. Стоєцький О. Суб'єкти забезпечення інформаційної безпеки України: адміністративно-правові засади. *Інформаційне право*. 2009. No 11. С. 161-164.

246. Новицький А. Інституційна теорія формування інформаційного суспільства. *Соціологія права*. 2011. № 1. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/39577/06-Novickiy.pdf?sequence=1.

247. Пашковський В. Ф. Інституційний механізм інформаційної безпеки України в умовах гібридної війни: характер та перспективи трансформацій. *Політикус*. 2021. № 1. С. 69-78.

248. Голікова Є. О Юридичний механізм реалізації трудових прав працівників: поняття та мета. *Європейські перспективи*. 2012. № 4 (2). С.130-132.

249. Інформаційне забезпечення управлінської діяльності в умовах інформатизації: організаційно-правові питання теорії і практики: підручник / за ред. Р.А. Калюжного та В.О. Шамрая. Київ: Академія державно-податкової служби України, 2012. 296 с.

250. Баран М. В. Суб'єкти забезпечення інформаційної безпеки в Україні. *Юридичний науковий електронний журнал*. 2022. № 6. С. 220-223.

251. Крупнова А. О. Система суб'єктів адміністративно-правового забезпечення інформаційної безпеки в Україні. Науковий вісник Ужгородського Національного Університету. 2024. № 83 (2). С. 277-287.

252. Зозуля О. С. Інституційна система державного управління інформаційною безпекою України: сучасний стан та шляхи удосконалення. Інвестиції: практика та досвід. 2015. № 6. С. 147-156.

253. Захаренко К. В. Проблеми консолідації суб'єктів інформаційної безпеки.

Проблеми соціальної роботи: філософія, психологія, соціологія. 2018. № 1 (11). С. 36-43, с. 42.

254. Любиченко О.О. Удосконалення правового механізму взаємодії державних і недержавних суб'єктів забезпечення інформаційної безпеки в умовах гібридної війни в Україні. *Суспільство та національні інтереси*. 2024. № 5 (5). С. 584-594.

255. Яковлєв П. О. Взаємодія суб'єктів публічного управління та інститутів громадянського суспільства в забезпеченні інформаційної безпеки України. *Прикарпатський юридичний вісник.* 2019. Вип. 3(2). С. 139-142.

256. Салаєв Т. Г. огли Питання і суть взаємодії між суб'єктами щодо адміністративно-правового забезпечення інформаційної безпеки у митній сфері. Юридичний вісник. 2019. № 4 (53). С. 92-98.

257. Черниш Р.Ф. Протидія деструктивному інформаційному впливу в україні: правові та організаційні аспекти. Юридичний науковий електронний журнал. 2022. № 1. С. 213-216.

258. Про Раду національної безпеки і оборони України : Закон України від 05.03.1998 р. № 183/98-ВР. URL: https://zakon.rada.gov.ua/ laws/card/183/98-вр.

259. Ткаченко В.В. Загрози інформаційній безпеці україни як проблематика національної безпеки. Юридичний науковий електронний журнал. 2022. № 10. С.496-498.

260. Зайцев М. М. Суб'єкти забезпечення інформаційної безпеки України. *Форум права*. 2013. № 3. С. 231–238.

261. Ряполов А. П. Організаційно-правові питання взаємодії органів публічної влади у сфері забезпечення інформаційної безпеки України. Права людини і громадянина під час дії воєнного стану: зб. наук. ст. за матеріалами наук.-практ. конф. з нагоди 75-ї річниці Заг. декларації прав людини, м. Харків, 8 груд. 2023 р.: електрон. наук. вид. Харків: Право, 2023. С. 260-264.

262. Косиця О.О. Інституціональний механізм системи інформаційної безпеки. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/3d130e83-16eb-4cdc-b32e-c70b53618061/content.

263. 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 : URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text.

264. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

265. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР : URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text.

266. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / ed. by M. N. Schmitt. Cambridge : Cambridge University Press, 2017. URL: https://doi.org/10.1017/9781316822524.

267. Advancing responsible State behaviour in cyberspace in the context of international security: draft resolution : of 18.10.2015 no. A/RES/73/266. URL: https://digitallibrary.un.org/record/1649077?v=pdf.

268. Cyber Defence Pledge : of 08.07.2016. URL: https://www.nato.int/cps/en/natohq/official_texts_133177.htm

269. Directive 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) : of 14.12.2022 no. 32022L2555. URL: http://data.europa.eu/eli/dir/2022/2555/oj.

270. Regulation 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) : of 27.04.2016 no. 32016R0679. URL: http://data.europa.eu/eli/reg/2016/679/oj

271. European Union Agency for Cybersecurity. *European Union.* URL: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_en

272. United Nations Charter : of 26.06.1945. URL: https://www.un.org/en/about-

us/un-charter/full-text.

273. Pollard M. A Case Study of Russian Cyber-Attacks on the Ukrainian Power Grid: Implications and Best Practices for the United States. *Pepperdine Policy Review*. 2024. No. 16. URL: https://digitalcommons.pepperdine.edu/ppr/vol16/iss1/1?utm_source=digitalcommons.pepperdine.edu/ppr/vol16/iss1/1&utm_medium=PDF&utm_campaign=PDFCoverPages.

274. Review of cybersecurity news in Ukraine, tendencies, and world events related to the First World Cyber War. 2024. URL: https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/CyberDigest_2024_01_ENG.pdf.

275. Distributed Denial of Service (DDoS) Attacks: A Practical Guide for Government Information Security Teams. *INE*. URL: https://ine.com/newsroom/distributed-denial-of-service-ddos-attacks-a-practical-guide-for-government-information-security-teams.

276. Дмитренко М. Інформаційно-психологічні операції в контексті інформаційної безпеки України. *Інформація і право*. 2025. № 1(52). С. 112–122. URL: https://doi.org/10.37750/2616-6798.2025.1(52).324704.

277. Information and Psychological Operations (IPSO) as a Discovery of False Narratives in the Conditions of Military Conflict in the Media / N. Shulska et al. *Journal of Interdisciplinary Research*. 2023. Vol. 13, no. 1. P. 156–162. URL: https://evnuir.vnu.edu.ua/handle/123456789/22192ю

278. Zetter K. Everything We Know About Ukraine’s Power Plant Hack. *Wired*. URL: https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/.

279. Marsh S. US joins UK in blaming Russia for NotPetya cyber-attack. *the Guardian*. URL: https://www.theguardian.com/technology/2018/feb/15/uk-blames-russia-notpetya-cyber-attack-ukraine.

280. Update: Destructive Malware Targeting Organizations in Ukraine. *An official website of the U.S. Department of Homeland Security*. URL: https://www.cisa.gov/news-

events/cybersecurity-advisories/aa22-057a.

281. Report: Digital incidents in the Ukrainian public sector in the first quarter of 2023. *Лабораторія цифрової безпеки*. URL: https://dslua.org/publications/report_dsl_1quarter/.

282. Rising Number of Cyberattacks Targeting the Security and Defense Sector: Threats to Know About. *State Service of Special Communications and Information Protection of Ukraine*. URL: https://cip.gov.ua/en/news/zrostannya-kilkosti-kiberatak-na-sektor-bezpeki-i-oboroni-pro-yaki-zagrozi-treba-znati.

283. CERT-UA минулого року опрацювала 4315 кіберінцидентів. *Державна служба спеціального зв'язку та захисту інформації України*. URL: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv.

284. Done W. D. The Information Technology Army of Ukraine and Cyber Warfare Doctrine. *Journal of Strategic Security,*. 2023. Vol. 16, no. 4. P. 15–33. URL: https://doi.org/10.5038/1944-0472.16.4.2127.

285. Constantinescu V. Ukrainian Cyber Alliance Disrupts Trigona Ransomware Operations, Exfiltrates Key Data. *Bitdefender*. URL: https://www.bitdefender.com/en-au/blog/hotforsecurity/ukrainian-cyber-alliance-disrupts-trigona-ransomware-operations-exfiltrates-key-data.

286. Private-public initiatives for cybersecurity: the case of Ukraine / L. Axon et al. *Journal of Cyber Policy*. 2025. P. 1–24. URL: https://doi.org/10.1080/23738871.2025.2451256.

287. Про введення воєнного стану в Україні : Указ Президента України від 24.02.2022 № 64/2022. URL: https://zakon.rada.gov.ua/laws/show/64/2022#Textю

288. Gisel L., Rodenhäuser T., Dörmann K. Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. *International Review of the Red Cross*. 2020. P. 1–48. URL: https://doi.org/10.1017/s1816383120000387

289. Mačák K. Military Objectives 2.0: The Case for Interpreting Computer Data as

Objects under International Humanitarian Law. *Israel Law Review*. 2015. Vol. 48, no. 1. P. 55–80. URL: https://doi.org/10.1017/s0021223714000260.

290. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану : Закон України від 24.03.2022 № 2149-IX. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text.

291. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27.03.2025 № 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/4336-20#Text.

292. Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі : Постанова Каб. Міністрів України від 04.04.2023 № 299. URL: https://zakon.rada.gov.ua/laws/show/299-2023-п#Text.

293. ICRC Position Paper: International humanitarian law and cyber operations during armed conflicts. The International Committee of the Red Cross, 2020. URL: https://international-review.icrc.org/articles/ihl-and-cyber-operations-during-armed-conflicts-913.

294. Skochylias-Pavliv O. Legal mechanisms for ensuring information security in Ukraine. *Visnik Nacional'nogo universitetu «Lvivska politehnika». Seria: Uridicni nauki*. 2024. Vol. 11, no. 42. P. 151–158. URL: https://doi.org/10.23939/law2024.42.151.

295. Річний аналітичний огляд. Рада нац. безпеки і оборони України, 2024. URL: https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20250109/Year%20in%20review_UKR_upd.pdf?fbclid=IwY2xjawI-fZRleHRuA2FlbQIxMAABHcaZdkgcVIlSJ0eGnBO78x5xRCDcoBwcJ1GKrT4SAVS5reEAtY5u8ssd4w_aem_0xN1oMO3-toIy6vpuA27mA.

296. Wachs J. Digital traces of brain drain: developers during the Russian invasion of Ukraine. *EPJ Data Science*. 2023. Vol. 12, no. 1. URL: https://doi.org/10.1140/epjds/s13688-023-00389-3.

297. Кримінальний процесуальний кодекс України : Кодекс України від 13.04.2012 № 4651-VI : URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.

298. Murzo Y., Halchenko V. Electronic evidence as a means of proof during the pillage investigation. *Naukovij vìsnik Nacìonal'noï akademìï vnutrìšnìh sprav*. 2023. Vol. 28, no. 3. P. 48–57. URL: https://doi.org/10.56215/naia-herald/3.2023.48.

299. Lyseiuk A., Svintsytska T. Legal providing of cyber security Ukraine under the conditions of martial state and European integration. *Law and innovations*. 2024. No. 4 (48). P. 32–38. URL: https://doi.org/10.37772/2518-1718-2024-4(48)-4.

300. Solutions to win: Ukraine forms Cyber Forces as new branch of military. *Rubryka*. URL: https://rubryka.com/en/2024/10/24/v-ukrayini-anonsuvaly-stvorennya-kibersyl-zsu-yak-okremogo-rodu-syl/.

301. Tallinn Manual 2.0 Clarifies How International Law Applies to Cyber Operations. *Atlantic Council*. URL: https://www.atlanticcouncil.org/news/press-releases/tallinn-manual-2-0-clarifies-how-international-law-applies-to-cyber-operations/.

302. Ряполов А. П. Теоретико-правові засади взаємодії інституту військової експертизи з органами державної влади. *Військова експертиза в умовах сьогодення: проблемні питання та шляхи їх вирішення*: матер. Всеукр. наук.-практ. конф., м. Дніпро, 25 квітня 2025 р. Дніпро : ДНДІСЕ МЮУ, 2025. С. 151-155.

303. Deutsch A., van den Berg S., Pearson J. Exclusive-ICC Probes Cyberattacks in Ukraine as Possible War Crimes, Sources Say. *Reuters / US News*. URL: https://www.reuters.com/world/europe/icc-probes-cyberattacks-ukraine-possible-war-crimes-sources-2024-06-14/.

304. Ukraine becomes a member of the NATO's Cooperative Cyber Defense Center of Excellence. *National Security and Defense Council of Ukraine*. URL: https://www.rnbo.gov.ua/en/Diialnist/6335.html.

305. Agreement between the European Union and European Atomic Energy Community of the one part and Ukraine of the other part, on the participation of Ukraine in Horizon Europe – the Framework Programme for Research and Innovation and the Research and Training Programme of the European Atomic Energy Community (2021-2025) complementing Horizon Europe – the Framework Programme for Research and Innovation : of 23.03.2022 no. 22022A0323(01). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:22022A0323(01).

306. Cyber resilience act: Council adopts new law on security requirements for digital products. *Council of the European Union*. URL: https://www.consilium.europa.eu/en/press/press-releases/2024/10/10/cyber-resilience-act-council-adopts-new-law-on-security-requirements-for-digital-products/.

307. Ukraine Signs the Council of Europe Framework Convention on AI. *The Council of Europe*. URL: https://www.coe.int/en/web/artificial-intelligence/-/ukraine-signs-the-council-of-europe-framework-convention-on-ai.

308. Buchatskiy C. How Ukrainian export controls stifle defense innovation. *Counteroffensive Pro*. URL: https://counteroffensive.pro/p/how-ukrainian-export-controls-stifle-defense-innovation

309. Bondar K. Understanding the Military AI Ecosystem of Ukraine. *Center for Strategic and International Studies*. URL: https://www.csis.org/analysis/understanding-military-ai-ecosystem-ukraine

310. Cyber Defence. *NATO's Strategic Warfare Development Command*. URL: https://www.act.nato.int/activities/cyber/

311. Who we are. The European Union Agency for Cybersecurity. Towards a Trusted and Cyber Secure Europe. *ENISA. European Union Agency for Cybersecurity*. URL: https://www.enisa.europa.eu/about-enisa/who-we-are.

312. Залєвська І. І., Удренас Г. І. Інформаційна безпека України в умовах російської військової агресії. *Південноукраїнський правничий часопис*. 2022. № 1. С. 20-26.

313. Словник української мови : [в 11 т.] / АН Української РСР, Ін-т мовознав. ім. О. О. Потебні ; редкол.: І. К. Білодід (голова) [та ін.]. Київ: Наук. думка, 1970-1980. Т. 9 : С / ред. тому: І. С. Назарова [та ін.]. 1978. 916 с.

314. Політологічний енциклопедичний словник ; упорядник В.П. Горбатенко ; за ред. Ю.С. Шемшученка, В.Д. Бабкіна, В.П. Горбатенка. [2-е вид., доп. і перероб.]. Київ: Генеза, 2004.

315. Словник іншомовних слів / Нац. ун-т ім. Тараса Шевченка, Київ. нац. екон. ун-т ім. Вадима Гетьмана ; [уклад.: Л. В. Музичко, Л. М. Шкарапута, С. М. Морозов]. Вид. 2-ге, допов. та доопрац. Київ: Наукова думка, 2019. 785 с.

316. Соціологія : короткий енциклопедичний словник ; уклад. В.І. Волович, В.І. Тарасенко. М.В. Захарченко та ін. ; під заг. ред. В.І. Воловича. Київ: Укр. Центр духовн. культури, 1998. 614 с.

317. Ковтун В. І. Гарантії державного суверенітету України: конституційні аспекти : монографія. Харків: Фактор, 2014. 216 с.

318. Декларація про державний суверенітет України від 16.07.1990 р. *Відомості Верховної Ради УРСР*. 1990. № 31. Ст. 429.

319. Бєлєвцева В. Державний суверенітет, його ознаки та властивості. *Підприємництво, господарство і право.* 2009. №10. С. 7-10.

320. Тернавська В. М. Концепція державного суверенітету в аспекті глобального інформаційного простору. *Інформація і право.* 2021. № 4 (39). С. 80-89.

321. Михальський Я. В., Пишна А. Г. Сучасні особливості інформаційного суверенітету та доктрини інформаційної безпеки України. *Південноукраїнський правничий часопис.* 2020. № 4. С. 38-44.

322. Солодка О. Пріоритетні напрями забезпечення інформаційного суверенітету України. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2024. Том 3. № 85. С. 134-138.

323. Кубальський В. Н. Особливості поняття «державний суверенітет» у сучасному міжнарод-ному праві. *Правова держава*. 2017. Випуск 28. С. 400–410.

324. Солодка О.М. Забезпечення інформаційного суверенітету держави: правовий дискурс. *Інформація і право*. 2020. № 1 (32). С. 80-87.

325. Радутний О.Е. Ілюзія та реальність інформаційного суверенітету. Інформація і право.No 4(35)/2020. С. 22-38.

326. Довгань О.Д. Національний інформаційний суверенітет – об’єкт інформаційної безпеки. *Інформація і право*. 2014. № 3(12). С. 102-112.

327. Чайка О.І. Інформаційний суверенітет як складова національної безпеки. https://api.dspace.khadi.kharkov.ua/server/api/core/bitstreams/2ef37a43-aea4-4c81-ac98-c25ff292444a/content. С. 128-131.

328. Єсімов С. С. Превентивне регулювання: теоретичні аспекти. *Соціально-правові студії*. 2020. Випуск 3 (9). С. 40-47.

329. Талдикін О. Інформаційний суверенітет та його зміст. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2023. № 2 (123). С. 132-138.

330. Олійник О. В., Соснін О. В., Шиманський Л. Є. Політико-правові аспекти формування інформаційного суспільства суверенної і незалежної держави. *Держава і право. Юридичні і політичні науки*. 2001. Вип. 13. С. 534-541.

331. Олійник О. В. Організаційно-правові засади захисту інформаційних ресурсів України: автореф. дис. ... канд. юрид. наук: 12.00.07. Харків, 2006.

332. Ярема О. Зміст інформаційного суверенітету у контексті державного суверенітету. *Юридичний науковий електронний журнал*. 2022. № (3). С. 191-194.

333. Люлько С., Сунєгін С. Інформаційний суверенітет держави: сутнісні характеристики. *Collection of Scientific Papers «ΛΌГОΣ»* (May 9, 2025, Cambridge, UK). Cambridge, 2025. P. 178–181. https://doi.org/10.36074/logos-09.05.2025.034.

334. Супрун В.М. Теоретико-правові основи інформаційного суверенітету: автореф. дис. ... канд. юрид. наук: 12.00.01. Харьків. 2010. 21 с.

335. Олійник О.В. Інформаційна безпека України: доктрина адміністративно-правового регулювання: дис. …докт. юрид. наук. Київ, 2013. 450 с.

336. Національний інформаційний суверенітет у контексті розвитку новітніх інформаційних технологій / [О. С. Онищенко, В. М. Горовий, В. І. Попик та ін.] ;НАН України, Нац. б-ка України ім. В. І. Вернадського. Київ : НБУВ, 2011. 154 с.

337. Information Sovereignty: Data Privacy, Sovereign Powers and the Rule of Law : monograph / Radim Polcak, Dan Jerker B. Svantesson. Cheltenham: Edward Elgar Publishing, 2017. 268 p.

338. Супрун В. М. Інформаційний суверенітет у системі суміжних юридичних категорій. *Вісник Харківського національного університету внутрішніх справ.* 2008. № 40. С. 31-39.

339. Larsen Benjamin Cedric The Geopolitics of AI and the Rise of Digital Sovereignty. *Brookings.* 2022. https://www.brookings. edu/articles/the-geopolitics-of-ai-and-the-rise-of-digitalsovereignty/.

340. Милосердна І. М. Цифровий суверенітет держави: наукова риторика та

реальні зміни. *Політикус.* 2024. № 6. С.154-160.

341. Ротар Н. Особливості концептуалізації ідеї цифрового суверенітету в сучасній політичній науці. *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2023. № 3 (17).

342. Калайда Ю.П. Забезпечення цифрового суверенітету в умовах геополітичного протиборства: кращі практики зарубіжного досвіду. *Інформація і право.* 2021. № 2 (37). С. 145-154.

343. Правдюк А.Л. Інформаційний суверенітет в контексті інформаційної безпеки. *Наукові інновації та передові технології*. 2024. № 11 (39). С. 639-651

344. Information Sovereignty: Data Privacy, Sovereign Powers and the Rule of Law : monograph / Radim Polcak, Dan Jerker B. Svantesson. Cheltenham: Edward Elgar Publishing, 2017. 268 p.

345. Flinder M., Smalley I. What is data sovereignty? https://www.ibm.com/think/topics/data-sovereignty.

346. Дубов В. Цифровий суверенітет у сучасному світі: виклики та можливості для України. *Вісник Національної академії керівних кадрів культури і мистецтв.* 2015. No 1.С. 205-209

347. Словник української мови : [в 11 т.] / АН Української РСР, Ін-т мовознав. ім. О. О. Потебні ; редкол.: І. К. Білодід (голова) [та ін.]. Київ: Наук. думка, 1970-1980. Т. 3 : З / ред. тому: Г. М. Гнатюк, Т. К. Черторизька. 1972. 744 с.

348. Солодка О. М. Сутнісні складові забезпечення інформаційного суверенітету України. *Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки.* 2025. № 1. Том 36 (75). С. 121-126.

349. Іванченко Ю. М. Сутність, головні напрями та способи державної інформаційної політики в Україні. URL: http://academy.gov.ua/ej/ej2/txts/ philo/05ijmipu. pdf.

350. Солодка О. М. Свобода інформації як основа забезпечення інформаційного суверенітету. *Інформація і право*. 2020. № 3 (34). С. 18-25.

351. Сергієнко Т. І., Бабарикіна Н. А. Міжнародні організації та їх роль у вирішенні глобальних проблем щодо врегулювання політичних конфліктів.

Humanities Studies. 2021. № 9 (86). С. 101-108.

352. Держава, суверенітет, національна безпека крізь призму глобалізації / Алєксєєнко І. В., Курас А. І., Рябінін Є. В.; Дніпропетр. держ. ун-т внутр. справ, Маріупол. держ. ун-т. Ніжин : Лисеенко М. М. [вид.], 2018. 303 с.

353. Шевчук М. О. Сучасні виклики і загрози в сфері інформаційної безпеки держави. А*ктуальні проблеми вітчизняної юриспруденції.* 2024. № 6. С. 160-166.

354. Задерейко О. В., Троянський О. В., Чанишев Р. І., Дика А. І. Концептуальні основи захисту інформаційного суверенітету України : монографія. 2-ге вид., перероб. і доп. Одеса : Фенікс, 2022. 220 с.

355. Шемчук В. В. Проблеми забезпечення національного інформаційного суверенітету в умовах агресії РФ. *Невідкладні заходи з протидії російській агресії з Криму:* політичні, юридичні, економічні, управлінські та соціальні аспекти : матеріали науково-практичної конференції (4 вересня2018 р., м. Київ). / Представництво Президента України в АРК. Київ-Одеса : Фенікс, 2018. С. 160-164.

356. Панфілов О.Ю. Інформаційне насильство як соціальний феномен. *Вісник Національного юридичного університету імені Ярослава Мудрого. Серія: філософія, філософія права, політологія, соціологія.* 2023. No 1 (56). С. 188-200.

357. Мануйлов Є. М., Калиновський Ю. Ю. Аксіологічний вимір інформаційної безпеки української держави. *Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». Серія : Філософія, філософія права, політологія, соціологія*. 2017. No 3. С. 13–30.

358. Гічко О. В. Інформаційний суверенітет як передумова міжнародної співпраці України в інформаційній сфері: питання захисту в умовах збройної агресії. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2024. Том 3 № 86. С. 272-277.

359. Короткий Т. Р. Генезис міжнародної правосуб'єктності інтеграційних утворень і еволюція міжнародного права. *Наукові праці Нац. ун-ту «Одеська юридична академія».* 2013. С. 439-440.

360. Dellmuth L., Aart Scholte J., Tallberg J., Verhaegen S. Legitimacy in Global Governance. Chapter 1. Citizens, Elites, and the Legitimacy of Global Governance.

Oxford: Oxford University Press, 2022. 289 p.

361. Шабан Ю. Поняття агресії в міжнародному праві. *Право і суспільство.* 2024. №о 2. С. 331-336.

362. Юдкова К.В. Побудова правової моделі інформаційної безпеки. *Інформація і право*. 2014. № 1(10). С. 68-72.

363. Мельник Д. Захист національної критичної інформаційної інфраструктури: актуальні проблеми та шляхи їх вирішення. *Адміністративне право і процес.* 2022. № 3 (38). С. 5-16.

364. Казакова Н. Ф., Щербина Ю. В., Фразе-Фразенко О. О. Проблеми безпеки сучасних кіберфізичних систем. *Кібербезпека в Україні: правові та організаційні питання:* матеріали Всеукраїнської науково-практичної конференції, м. Одеса, 17 лист. 2017 р. Одеса : Одеський державний університет внутрішніх справ, 2017. С. 77-78.

365. Малик І. Р. Принцип «розділяй і владарюй» як інформаційно-комунікаційна технологія конструювання суспільних процесів. *Регіональні студії.* 2024. № 37. С. 45-50.

366. Ліпкан В. А. Національна безпека України : навчальний посібник. 2-ге вид. Київ : КНТ, 2009. 576 с.

367. Олійник А. А. Організація безпеки інформаційного суверенітету для України як об’єкта глобальних інформаційних впливів. *Національна парадигма правового розвитку сучасної України:* збірник тез Всеукраїнського науково-практичного юридичного форуму (Дніпро, 18 травня2023 р.). Дніпро: Ліра, 2023. 348 с. С. 334-339.

368. Радченко О., Чмир Я. Гібридна війна як ключова загроза національному суверенітету україни. *Таврійський науковий вісник. Серія: Публічне управління та адміністрування.* 2022. № 3. С. 100-108.

369. Державний суверенітет в умовах глобалізації: теорія та практика : монографія / Н. А. Бабарикіна, Н. В. Горло, М. Ф. Заболотна, О. М. Кіндратець, Т. І. Сергієнко; за заг. ред. О. М. Кіндратець. Запоріжжя : Запорізький національний університет, 2022. 226 с.

370. Куцепал С. В. Інформаційний суверенітет та інформаційна безпека України: виклики та реалії війни. *Полтавський правовий часопис.* 2023. № 1. С. 78-88.

371. Norris M. J. The Law of Attack in Cyberspace: Considering the Tallinn Manual's Definition of 'Attack' in the Digital Battlespace. *Inquiries Journal/Student Pulse*. 2013. Vol. 5, no. 10. URL: http://www.inquiriesjournal.com/a?id=775.

372. Вавринчук М.П., Когут О. В. Інформаційна безпека держави. *Правові засади організації та здійснення публічної влади* : зб. тез II Всеукр. наук.-практ. інтернет-конф. (м. Хмельницький, 2-8 трав. 2019 р.). Хмельницький : ХУУП, 2019. С. 37-40.

373. Ліпкан В. А. Основи національної безпеки України. Київ: Правова єдність, 2010. 352 с.

374. Любиченко О. О. Державні та недержавні суб'єкти забезпечення інформаційної безпеки у протидії дестабілізації системи суспільних відносин в умовах гібридної війни в Україні. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Публічне управління та адміністрування*. 2024.Том 35 (74). № 4. С. 95-100.

375. Ряполов А. П. Нормативно-правові основи інформаційної безпеки України в умовах гібридної агресії. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2025. Т. 3, № 89. С. 87-91.

376. Державна політика забезпечення національної безпеки України: основні напрямки та особливості здійснення : монографія / Криштанович М.Ф., Пушак Я.Я., Флейчук М.І., Франчук В.І. Львів: Сполом, 2020. 418 с.

377. Ряполов А. П. Гібридна агресія проти України як виклик модернізації правової політики у сфері інформаційної безпеки. *Український політико-правовий дискурс.* 2025. № 10. С. 1-14.

378. Сокуренко В. В., Передерій О. С., Абламська В. В. Втягнення неповнолітніх в кримінально протиправну діяльність в кіберпросторі: феномен та засади протидії. *Вісник Кримінологічної асоціації України*. 2025. № 1 (34). С. 632-635.

379. Ряполов А. П. Теоретико-правова характеристика інформаційної безпеки в умовах воєнного стану. *Modernization of science and its influence on global processes:* collection of scientific papers «SCIENTIA» with Proceedings of the III International

Scientific and Theoretical Conference, Bern, April 14, 2023. Bern, Swiss Confederation : European Scientific Platform, 2023. P. 41-43.

380. Кобко Є. В. Поняття та значення національної безпеки держави як об'єкту адміністративно-правової охорони та захисту. *Європейські перспективи*. 2022. № 2. С. 28-33.

381. Ряполов А. П. Окремі напрями удосконалення забезпечення інформаційної безпеки в умовах війни. *Science and Practice: Implementation to Modern Society:* with the Proceedingsof the 14 th International Scientific and Practical, Manchester, April 26-28, 2023. Manchester : Peal Press Ltd., 2023. P. 303-307.

382. Кобко Є. В. Подолання загроз національній безпеці України: адміністративно-правовий аспект. *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* 2024. № 1. С. 15-23.

383. Ряполов А. П. Співвідношення понять «інформаційна безпека» та «безпека інформації» у сучасному науковому просторі. *Актуальні проблеми державотворення та правозастосування :* матер. Всеукр. наук.-практ. конф., м. Дніпро, 7 груд. 2023 р. Дніпро : ДДУВС, 2024. С. 143-146.

384. Юнін О. С. Адміністративно-правове забезпечення національної безпеки України в умовах надзвичайного стану: проблеми теорії та практики. *Підприємництво, господарство і право.* 2025. № 2. С. 79-85.

385. Ряполов А. П. Суб'єкти забезпечення інформаційної безпеки України. *Проблеми юридичної науки очима молодих науковців*: матеріали XVIII Всеукр. наук.-практ. онлайн-конф., м. Рівне, 17 жовтня 2024 р. Рівне : Національний університет біоресурсів та природокористування України, 2024. С. 64-67.

386. Ряполов А. П. Інформаційна безпека людини та громадянина як складова національної безпеки держави: загрози та виклики. *Міжнародна та національна безпека: теоретичні і прикладні аспекти :* матер. IX Міжнар. наук.-практ. конф., м. Дніпро, 21 березня 2025 р. ; у 2-х ч. Ч. II. Дніпро : ДДУВС, 2025. С. 458-459.

387. Самотуга А. В. Організаційно-інституційне забезпечення зовнішньої інформаційної політики України. *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* 2022. № 1. С. 186-192.

388. Ряполов А. П. Свобода вибору та межі інформаційної безпеки в умовах воєнного стану: баланс між національною безпекою та свободою вираження поглядів. *Міжнародна та національна безпека: теоретичні і прикладні аспекти:* матер. ХМіжнар. наук.-практ. конф., м. Дніпро, 16 березня 2026 р. ; у 2-х ч. Ч. ІІ. Дніпро : ДДУВС, 2026. С. 476-477.

389. Передерій О. С. Організаційно-правові засади протидії загрозам кібербезпеки в аспекті європейської інтеграції України. *Вісних Харківського національного університету імені В. Н. Каразіна. Серія «Право».* 2025. № 39. С. 70-75.

390. Самотуга А. В. Свобода і плюралізм медіа у механізмі верховенства права ЄС та вимоги до України. *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* 2024. № 1. С. 110-120.

ДОДАТКИ

Додаток А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ ТА ВІДОМОСТІ ПРО АПРОБАЦІЮ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковано основні наукові результати дисертації:

1. Ряполов А. П. Нормативно-правові основи інформаційної безпеки України в умовах гібридної агресії. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2025. Т. 3, № 89. С. 87-91. URL: https://visnyk-pravo.uzhnu.edu.ua/article/view/336476/325112

2. Ряполов А. П. Гібридна агресія проти України як виклик модернізації правової політики у сфері інформаційної безпеки. *Український політико-правовий дискурс.* 2025. № 10. С. 1-14. URL: https://ppdnz.com.ua/index.php/home /article/view/236/151

3. Ряполов А. П. Захист інформаційного простору України в умовах гібридної війни: межі між свободою слова та інформаційною безпекою. *Національні інтереси України.* 2025. № 5 (10). С. 746-757. URL: https://perspectives.pp.ua/index.php/niu /article/view/23746/23719

Наукові праці, які засвідчують апробацію матеріалів дисертації:

1. Ряполов А. П. Теоретико-правова характеристика інформаційної безпеки в умовах воєнного стану. *Modernization of science and its influence on global processes:* collection of scientific papers «SCIENTIA» with Proceedings of the III International Scientific and Theoretical Conference, Bern, April 14, 2023. Bern, Swiss Confederation : European Scientific Platform, 2023. P. 41-43.

2. Ряполов А. П. Окремі напрями удосконалення забезпечення інформаційної безпеки в умовах війни. *Science and Practice: Implementation to Modern Society:* with

the Proceedingsof the 14 th International Scientific and Practical, Manchester, April 26-28, 2023. Manchester : Peal Press Ltd., 2023. P. 303-307.

3. Ряполов А. П. Співвідношення понять «інформаційна безпека» та «безпека інформації» у сучасному науковому просторі. *Актуальні проблеми державотворення та правозастосування :* матер. Всеукр. наук.-практ. конф., м. Дніпро, 7 груд. 2023 р. Дніпро : ДДУВС, 2024. С. 143-146.

4. Ряполов А. П. Організаційно-правові питання взаємодії органів публічної влади у сфері забезпечення інформаційної безпеки України. *Права людини і громадянина під час дії воєнного стану*: зб. наук. ст. за матеріалами наук.-практ. конф. з нагоди 75-ї річниці Заг. декларації прав людини, м. Харків, 8 груд. 2023 р.: електрон. наук. вид. Харків : Право, 2023. С. 260-264.

5. Ряполов А. П. Інформаційна безпека України в умовах воєнного стану: проблеми та перспективи. *Юридична весна: права людини в умовах воєнного стану:* збірник тез наук.-практ. конф., м. Харків, 15 квітня 2024 р. Харків : Національний юридичний університет імені Ярослава Мудрого, 2024. С. 170-175.

6. Ряполов А. П. Інституційне забезпечення інформаційної безпеки України. *Конституційні права і свободи людини та громадянина в умовах війни та післявоєнний період* : матер. наук. семінару, м. Львів, 21 червня 2024 р. Львів : ЛьвДУВС, 2024. С. 167-170.

7. Ряполов А. П. Суб’єкти забезпечення інформаційної безпеки України. *Проблеми юридичної науки очима молодих науковців*: матеріали XVIII Всеукр. наук.-практ. онлайн-конф., м. Рівне, 17 жовтня 2024 р. Рівне : Національний університет біоресурсів та природокористування України, 2024. С. 64-67.

8. Ряполов А. П. Інформаційна безпека людини та громадянина як складова національної безпеки держави: загрози та виклики. *Міжнародна та національна безпека: теоретичні і прикладні аспекти :* матер. IX Міжнар. наук.-практ. конф., м. Дніпро, 21 березня 2025 р. ; у 2-х ч. Ч. II. Дніпро : ДДУВС, 2025. С. 458-459.

9. Ряполов А. П. Теоретико-правові засади взаємодії інституту військової експертизи з органами державної влади. *Військова експертиза в умовах сьогодення: проблемні питання та шляхи їх вирішення*: матер. Всеукр. наук.-практ. конф., м. Дніпро, 25 квітня 2025 р. Дніпро : ДНДІСЕ МЮУ, 2025. С. 151-155.

10. Ряполов А. П. Свобода вибору та межі інформаційної безпеки в умовах воєнного стану: баланс між національною безпекою та свободою вираження поглядів. *Міжнародна та національна безпека: теоретичні і прикладні аспекти:* матер. ХМіжнар. наук.-практ. конф., м. Дніпро, 16 березня 2026 р. ; у 2-х ч. Ч. ІІ. Дніпро : ДДУВС, 2026. С. 476-477.

Додаток Б

ЗАТВЕРДЖУЮ
Голова Дніпропетровського
окружного адміністративного суду
Володимир ГОРБАЛІНСЬКИЙ
«13» квітня 2026 р.

АКТ

«13» квітня 2026 р.

м. Дніпро №_____

про використання результатів дисертаційного дослідження
Ряполова Антона Павловича
«Інформаційна безпека в умовах воєнного стану:
теоретико-правова характеристика»
на здобуття ступеня доктора філософії зі спеціальності 081 «Право»

Цей акт склала комісія у складі:

Голова комісії	КОРЕНЕВ Андрій Олексійович
Член комісії	ЛУНІНА Олена Станіславівна
Член комісії	ПРУДНИК Сергій Володимирович

Комісія підтверджує, що результати дисертаційного дослідження РЯПОЛОВА Антона Павловича «Інформаційна безпека в умовах воєнного стану: теоретико-правова характеристика» були використані у діяльності Дніпропетровського окружного адміністративного суду. Зокрема, теоретичні положення та практичні рекомендації, викладені у наукових публікаціях дисертанта, знайшли застосування під час:

– аналізу правових засад забезпечення інформаційної безпеки органів судової влади України в умовах воєнного стану, зокрема щодо захисту персональних даних учасників судових процесів від несанкціонованого доступу і кібератак;

– застосування теоретико-правових підходів, розроблених у дисертації, при оцінці відповідності заходів обмеження доступу до інформації вимогам законодавства України про інформаційну безпеку та Конституції України;

– використання висновків дисертанта щодо правового регулювання інформаційних відносин в умовах воєнного стану при розгляді адміністративних спорів, пов'язаних із захистом прав громадян на доступ до публічної інформації в умовах обмежень воєнного часу;

– впровадження науково обґрунтованих рекомендацій щодо інституційних механізмів захисту інформаційного суверенітету держави у практику застосування суддями норм законодавства у сфері кіберзахисту критичної інфраструктури;

– підвищення кваліфікації суддів та працівників апарату суду з питань правового забезпечення інформаційної безпеки, протидії кібератакам та дезінформації, систематизованих у дисертаційному дослідженні.

Зазначені результати відображено у таких наукових працях здобувача:

Тези доповідей:

1. Ряполов А. П. Теоретико-правова характеристика інформаційної безпеки в умовах воєнного стану. Modernization of science and its influence on global processes: collection of scientific papers «SCIENTIA» with Proceedings of the III International Scientific and Theoretical Conference, Bern, April 14, 2023. Bern, Swiss Confederation : European Scientific Platform, 2023. P. 41–43.
2. Ряполов А. П. Окремі напрями удосконалення забезпечення інформаційної безпеки в умовах війни. Science and Practice: Implementation to Modern Society: with the Proceedings of the 14th International Scientific and Practical, Manchester, April 26–28, 2023. Manchester : Peal Press Ltd., 2023. P. 303–307.
3. Ряполов А. П. Співвідношення понять «інформаційна безпека» та «безпека інформації» у сучасному науковому просторі. Актуальні проблеми державотворення та правозастосування : матер. Всеукр. наук.-практ. конф., м. Дніпро, 7 груд. 2023 р. Дніпро : ДДУВС, 2024. С. 143–146.

4. Ряполов А. П. Організаційно-правові питання взаємодії органів публічної влади у сфері забезпечення інформаційної безпеки України. Права людини і громадянина під час дії воєнного стану: зб. наук. ст. за матеріалами наук.-практ. конф. з нагоди 75-ї річниці Заг. декларації прав людини, м. Харків, 8 груд. 2023 р. Харків : Право, 2023. С. 260–264.
5. Ряполов А. П. Інформаційна безпека України в умовах воєнного стану: проблеми та перспективи. Юридична весна: права людини в умовах воєнного стану: збірник тез наук.-практ. конф., м. Харків, 15 квітня 2024 р. Харків : Національний юридичний університет імені Ярослава Мудрого, 2024. С. 170–175.
6. Ряполов А. П. Інституційне забезпечення інформаційної безпеки України. Конституційні права і свободи людини та громадянина в умовах війни та післявоєнний період: матер. наук. семінару, м. Львів, 21 червня 2024 р. Львів : ЛьвДУВС, 2024. С. 167–170.
7. Ряполов А. П. Суб'єкти забезпечення інформаційної безпеки України. Проблеми юридичної науки очима молодих науковців: матеріали XVIII Всеукр. наук.-практ. онлайн-конф., м. Рівне, 17 жовтня 2024 р. Рівне : Національний університет біоресурсів та природокористування України, 2024. С. 64–67.
8. Ряполов А. П. Інформаційна безпека людини та громадянина як складова національної безпеки держави: загрози та виклики. Міжнародна та національна безпека: теоретичні і прикладні аспекти: матер. IX Міжнар. наук.-практ. конф., м. Дніпро, 21 березня 2025 р. Ч. II. Дніпро : ДДУВС, 2025. С. 458–459.
9. Ряполов А. П. Теоретико-правові засади взаємодії інституту військової експертизи з органами державної влади. Військова експертиза в умовах сьогодення: проблемні питання та шляхи їх вирішення: матер. Всеукр. наук.-практ. конф., м. Дніпро, 25 квітня 2025 р. Дніпро : ДНДІСЕ МЮУ, 2025. С. 151–155.

10. Ряполов А. П. Свобода вибору та межі інформаційної безпеки в умовах воєнного стану: баланс між національною безпекою та свободою вираження поглядів. Міжнародна та національна безпека: теоретичні і прикладні аспекти: матер. X Міжнар. наук.-практ. конф., м. Дніпро, 16 березня 2026 р. Дніпро : ДДУВС, 2026.

Результати наукових досліджень Ряполова А. П. було використано під час підготовки аналітичних матеріалів, застосування теоретичних положень у судовій практиці та підвищення правової обізнаності суддів і працівників апарату Дніпропетровського окружного адміністративного суду у сфері інформаційної безпеки та кіберзахисту в умовах воєнного стану. Особливу практичну цінність мають матеріали дисертації, в яких систематизовано правові механізми забезпечення інформаційного суверенітету України, захисту судових інформаційних систем від кібератак та дезінформаційних впливів.

Члени комісії:

Андрій КОРЕНЕВ

Олена ЛУНІНА

Сергій ПРУДНИК