ПРИКАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАСИЛЯ СТЕФАНИКА
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПРИКАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАСИЛЯ СТЕФАНИКА
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова праця
на правах рукопису

ГАЛІПЧАК ВОЛОДИМИР ДМИТРОВИЧ

УДК 323.28:004.738.5:32.019.5]327.7:351.78

ІНСТИТУЦІЙНІ ЧИННИКИ ІНФОРМАЦІЙНО-БЕЗПЕКОВОЇ ПОЛІТИКИ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

052 Політологія
05 Соціальні та поведінкові науки

Подається на здобуття ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають покликання на відповідне джерело _____ В. Д. Галіпчак.

Науковий керівник: Марчук Василь Васильович, доктор історичних наук, професор

Івано-Франківськ – 2025

АНОТАЦІЯ

Галіпчак В. Д. Інституційні чинники інформаційно-безпекової політики України в умовах воєнного стану. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії з галузі знань 05 Соціальні та поведінкові науки за спеціальністю 052 Політологія, Прикарпатський національний університет імені Василя Стефаника, Івано-Франківськ, 2025.

Дисертаційне дослідження присвячене розв'язанню актуального теоретико-прикладного завдання – аналізу інституційних чинників інформаційно-безпекової політики в умовах воєнного стану.

Для сучасного світу притаманний динамічний розвиток інформаційних технологій (самобутні диджиталізаційні зміни), які, першоєю чергою, детерміновані зростанням ролі інформації в житті суспільства та держави. Останнє природно зумовлює потребу виформовування ефективних механізмів захисту інформаційного простору, що вкрай актуальне щодо збереження національної безпеки. Своєю чергою, особливої значущості набуває розгляд інституційних чинників інформаційно-безпекової політики, що пов'язане з стрижневою роллю останніх щодо підґрунтя, розвитку та реалізації стратегій захисту інформаційного простору країни.

Мовиться про те, що аналіз вищезазначених чинників репрезентативний не лише щодо наявних викликів та загроз, а й локалізації, ідентифікації тощо потенційних лакун, натомість врахування останніх продукує зміцнення інформаційної безпеки. Саме тому вибір теми дослідження базований на низці релевантних складників, побутування яких корелює з актуальністю та значущістю цього напряму дослідження на сьогодні. Зокрема:

а) *геополітичний контекст* (полягає у актуалізації таких елементів як діахронія (вертикальна локалізація стану інформаційної безпеки безвідносно до її попереднього контексту (трансформаційних змін, станів, специфіки), яка

полягає у аналізі тієї чи тієї параметризації на певному етапі: до прикладу, актуальний стан) і синхронія (горизонтальна локалізація – її суть у відстеженні динаміки генези такої безпеки з низкою причиново-наслідкових зв'язків: до прикладу: мовиться про врахування таких релеватних віх як анексія Криму, події на Сході України та широкомасштабне вторгнення країни-агресора, які зумовлюють не лише військову, а й інформаційну лінію фронту);

б) *збільшувана релевантність інформаційного простору* (йдеться про зростаючу роль даних щодо впливу на громадську думку (дезінформацію, мізінформацію, пропаганду тощо), формування тих чи тих наративів як складників самобутнього сторітеллінгу, нової міфології тощо, що, своєю чергою, стають частиною модерної ідеологічної полісистеми, метою якої є маніпулювання свідомістю громадян, а також роль інформаційно-безпекової політики як інструментарію боротьби з вищезазначеними виявами в контексті національної безпеки;

в) *лакунізованість аналізованої проблематики* (репрезентована дуальною природою останньої: з одного боку, спостерігаємо зростаючу роль проблем інформаційної безпеки, що зумовлює аналіз інституційних чинників, які релевантні щодо формування та реалізації вищезазначеної політики в нашій країні; з іншого – постулюємо відсутність комплексного підходу до вищезазначеного питання й потребу у синхронічному підході до нього, який продукуватиме актуалізацію наукового спадку і забезпечить органічність, питомість, адаптивність тощо продукованих кроків заради такої політики);

г) власне, *актуальність* (детермінована гібридною російсько-українською війною, яка позначена функціонуванням цілої низки неправдивих, викривлених тощо даних, що використовуються ворогом для дискредитації влади, ЗСУ, мобілізаційних заходів та іншого й протидія яким безпосередньо пов'язана з самобутністю актуалізації інституційних чинників у безпековій політиці сучасної України) й ґ) *глобалізаційний контекст* (полягає у інтеграції міжнародного досвіду (концепцій, практик, кампаній тощо) щодо інформаційно-безпекових ініціатив й адаптації ефективного

інструментарію задля протидії низці інформаційних загроз на українському підґрунті).

Актуальність теми дослідження зумовлена експонетним зростанням наявних викликів інформаційної безпеки, посилених російською агресією в Україні. Останнє спродукувало потребу у оперативному реагуванні її уряду на поточні загрози з вибудовуванням політичних концепцій, стратегій, практик тощо. Першою чергою, це пов'язане з формуванням стійкості інформаційного простору до можливих вразливостей у майбутньому й вибудовуванням сценаріїв протидії їм. Своєю чергою, актуальним також є вивчення параметризаційних особливостей в контексті генези наукових підходів до поняття інформаційної безеки та розробки ефективних стратегій її функціонування в умовах сучасних диджиталізаційних й геополітичних загроз.

Показово, що досліджені у науковій роботі теоретико-методологічні засади поняття національної безпеки у диджиталізаційному вимірі дозволяють здійснити глибокий аналіз інформаційної безпеки як геополітичної детермінанти (державності). Натомість глибокий аналіз безпеки інформаційного простору України з екстраполяцією сучасних викликів та міжнародного досвіду продукує вичленування самобутності українського контексту та виокремлення релевантних напрямів генези інформаційно-безпекової політики.

Отже, вибір теми дослідження детермінований не лише актуальністю аналізованої проблематики, а й потребою у випрацюванні ґрунтовного, комплексного й вичерпного підходу до побутування інформаційного простору України. Останній проаналізовано у межах дисертації в контексті гарантування сталого розвитку (стабільності, генези тощо) й безпеки (захисту, збереження та іншого). Своєю чергою, це продукує потребу у глибокому аналізі інституційних чинників й випрацювання ефективних стратегій щодо протидії наявним і потенційним загрозам для такого простору.

Метою роботи є комплексне та всебічне вивчення інституційних

аспектів формування та реалізації інформаційно-безпекової політики України, виявлення основних проблем та викликів, що стоять перед державою у цій сфері в контексті зовнішньої агресії, а також розробка рекомендацій щодо оптимізації інституційного механізму забезпечення інформаційної безпеки на базі кращих національних та міжнародних практик.

Об'єктом дослідження є інституційні чиннинки інформаційно-безпекової політики України в умовах зовнішніх загроз та впливів.

Предмет дослідження становлять процеси та закономірності формування й реалізації інформаційно-безпекової політики України з урахуванням міжнародного досвіду для боротьби проти російської агресії.

Досягнення вищезазначеної мети, об'єкта, предмета дисертаційної роботи відбулося шляхом розв'язання низки дослідницьких *завдань*:

– доповнити й систематизувати теоретико-методологічні засади дослідження поняття національної безпеки та її диджиталізаційний вимір у контексті інституційних чинників інформаційно-безпекової політики;

– висвітлити трансформаційні зміни категорійно-понятійного апарату інформаційно-безпекової політики України щодо його динаміки, специфіки тощо задля виокремлення кореляцій між поняттям національної та інформаційної безпеки;

– виокремити самобутню генезу поняття національних інтересів у диджиталізаційному вимірі, категоризувавши, структурувавши, вибудувавши за значущістю щодо зовнішніх / внутрішніх складників;;

– відстежити особливості побутування системи інформаційного простору, диференціюючи останню щодо функційної параметризації покладених на неї питомих завдань;

– сформулювати власне визначення поняття державно-правового механізму інформаційної безпеки, проаналізувавши джерельну (нормативно-правову базу) та оцінивши ефективність наявних моделей інформаційної безпеки;

– схарактеризувати сучасні виклики безпеці інформаційного простору

України в контексті параметризаційних особливостей розгортання гібридної російсько-української війни та інформаційної агресії, яка її супроводжує;

– екстраполювати міжнародний досвід західних держав-партнерів щодо інформаційного протистояння під час гібридних й інформаційних воєн;

– ідентифікувати види наявних та потенційних загроз, продукованих російською федерацією для України, задля формування рекомендацій до адаптації й імплементації вищезазначених практик, стратегій тощо.

У результаті проведеного дослідження здобувачем одержано такі наукові результати, зумовлені комплексним, ґрунтовним вивченням самобутності генези інституційних чинників інформаційно-безпекової політики України. Остання досліджена у корелятивному зв'язку з низкою викликів в умовах гібридної та інформаційної російсько-української війни. Зокрема, наукова робота заповнює такі лакуни у аналізованій проблематиці:

Уперше: а) комплексно досліджено підходи до розуміння інформаційної безпеки як складника національної безпеки держави й локалізовано роль і місце інституційних чинників у її функціонуванні; б) розроблено та обґрунтовано теоретичну модель інституційної взаємодії в царині інформаційної безпеки, яка враховує специфіку гібридної війни та потребу адаптації національної безпекової стратегії до змінюваних умов внутрішнього і зовнішнього середовища; в) опрацьовано широкий масив історіографії та репрезентативну джерельну базу з аналізованої проблематики задля відстеження генези інституційних чинників інформаційно-безпекової політики України та їх ролі у цьому процесі; г) запропоновано авторське визначення поняття національної безпеки та інформаційно-безпекової політики; г) ідентифіковано види наявних та потенційних загроз, продукованих російською федерацією для України, сформовано рекомендації до адаптації й імплементації практик, стратегій тощо вищезазначеної політики; д) проведено вивчення інформаційно-безпекових практик на основі SWOT-аналізу та методів прогнозування, що дозволило визначити ключові напрями оптимізації державної політики у цій царині.

Уточнено та вдосконалено: а) теоретико-методологічні засади дослідження поняття національної безпеки та її диджиталізаційний вимір у контексті інституційних чинників інформаційно-безпекової політики; б) категорійно-понятійний апарат такої політики щодо динаміки, специфіки тощо останнього задля виокремлення кореляцій між поняттям національної та інформаційної безпеки; в) особливості побутування системи інформаційного простору з диференціацією останньої щодо функційної параметризації покладених на неї питомих завдань.

Новий рівень отримали положення про: а) самобутню генезу поняття національних інтересів у диджиталізаційному вимірі щодо їх категоризації, структуризації та іншого з вибудовуванням за значущістю щодо зовнішніх/внутрішних складників й кореляцією з впливом законодавчих і нормативних документів на формування інформаційного простору України; б) роль інституційних чинників в процесі формування й реалізації інформаційно-безпекової політики в контексті міжнародного досвіду (інформаційного протистояння під час гібридних й інформаційних воєн) та виокремлення оптимальних моделей взаємодії між різними інституційними суб'єктами (включаючи державні органи, громадські інституції та міжнародні організації); в) ключові принципи та механізми міжнародної кооперації у галузі інформаційної безпеки, що може стати основою для розробки нових міжнародних договорів та угод, а також низки викликів безпеці інформаційного простору в контексті параметризаційних особливостей розгортання гібридної російсько-української війни й інформаційної агресії, яка її супроводжує.

Практичне значення роботи полягає у можливості використання її наукових здобутків у навчальному процесі (зокрема, лекційних, семінарських заняттях, контрольних роботах, іспитах тощо у закладах вищої освіти). Поза тим, дані дисертаційного дослідження можуть бути актуалізовані під час розробки навчальних курсів з низки політологічних, соціологічних та інших дисциплін. Зокрема, за такими напрямами підготовки як «Національна

безпека», «Політологія», «Міжнародні відносини», «Європейські студії», «Інформаційна безпека» та інші. Окрім того, його результати доцільно використати для створення навчальних підручників, посібників, методичних рекомендацій тощо, а також під час написання кваліфікаційних наукових праць. Результати наукового пошуку покликані сприяти подальшому розвитку та безпосередньому внеску в посилення національної безпеки України, формування стійкості інформаційного простору до зовнішніх та внутрішніх викликів, а також у забезпеченні сприятливих умов для розвитку інформаційного суспільства в країні.

Ключові слова: війна, воєнний стан, гібридна війна, дезінформація, діджиталізація, , інформаційна безпека, інформаційно-безпекова політика інформаційна політика, інформаційне суспільство, інформаційний простір, Європейський Союз, європейська інтеграція, національна безпека, політична комунікація, політична участь.

ABSTRACT

Galipchak V. D. Institutional factors of information and security policy of Ukraine in the conditions of martial law. – Qualifying scientific work on the rights of the manuscript.

Dissertation for the degree of Doctor of Philosophy in the field of knowledge 05 Social and behavioral sciences with a specialty 052 Political Science, Vasyl Stefanyk Precarpathian National University, Ivano-Frankivsk, 2024.

The dissertation research is devoted to solving an urgent theoretical and applied task – analyzing the institutional factors of information and security policy under martial law.

The modern world is characterized by the dynamic development of information technologies (original digitalization changes), primarily determined by the growing role of information in society and the state. The latter naturally leads to the need to develop effective mechanisms for protecting the information space, which is extremely important for maintaining national security. In turn, the

consideration of institutional factors of information and security policy is of particular importance, which is related to the latter's pivotal role in the foundation, development, and implementation of strategies for protecting the country's information space.

The point is that the analysis of the above factors is representative not only of existing challenges and threats but also of localization, identification, etc. of potential gaps while considering that the latter leads to the strengthening of information security. That is why the choice of the research topic is based on several relevant components, the existence of which correlates with the relevance and importance of this area of research today. In particular:

a) *geopolitical context* (consists in the actualization of such elements as diachrony (vertical localization of the state of information security without regard to its previous context (transformational changes, states, specifics), which consists in the analysis of a particular parameterization at a certain stage: for example, the current state) and synchrony (horizontal localization - its essence is to track the dynamics of the genesis of such security with several cause-and-effect relationships: for example, it is about taking into account such relevant milestones as the annexation of Crimea, events in eastern Ukraine and the large-scale invasion of the aggressor country, which determine not only the military but also the information front line);

b) *the increasing relevance of the information space* (this refers to the growing role of data in influencing public opinion (disinformation, misinformation, propaganda, etc.), the formation of certain narratives as components of original storytelling, new mythology, etc., which, in turn, become part of a modern ideological poly system aimed at manipulating the consciousness of citizens, as well as the role of information and security policy as a tool to combat the above-mentioned manifestations in the context of national security;

c) *the lacunarity of the analyzed issues* (represented by the dual nature of the latter): on the one hand, we observe the growing role of information security issues, which leads to the analysis of institutional factors relevant to the formation and

implementation of the above policy in our country; on the other hand, we postulate the lack of a comprehensive approach to the above issue and the need for a synchronous approach to it, which will produce an actualization of the scientific heritage and ensure the organicity, specificity, adaptability, etc. of the steps taken for such a policy);

d) *actual relevance* (determined by the hybrid russian-Ukrainian war, which is marked by the functioning of several false, distorted, etc. data used by the enemy to discredit the government, the Armed Forces of Ukraine, mobilization activities, etc., and counteracting them is directly related to the originality of the actualization of institutional factors in the security policy of modern Ukraine); and g) the globalization context (involves the integration of international experience (concepts, practices, campaigns, etc.) in information and security initiatives and the adaptation of effective tools to counter several information threats on Ukrainian soil).

The relevance of the research topic is due to the exponential growth of existing information security challenges, exacerbated by russian aggression in Ukraine. The latter has created a need for the government to respond promptly to current threats by developing political concepts, strategies, practices, etc. First of all, this is related to the formation of the information space's resilience to possible future vulnerabilities and the development of scenarios to counter them. In turn, it is also relevant to study parameterization features in the context of the genesis of scientific approaches to the concept of information security and the development of effective strategies for its functioning in the context of modern digitalization and geopolitical threats.

It is noteworthy that the theoretical and methodological foundations of the concept of national security in the digitalization dimension studied in the research paper allow for an in-depth analysis of information security as a geopolitical determinant (statehood). In turn, a deep analysis of the security of Ukraine's information space with extrapolation of modern challenges and international experience produces a distinction between the identity of the Ukrainian context and the identification of relevant areas of the genesis of information and security policy.

Thus, the choice of the research topic is determined not only by the relevance of the analyzed issues but also by the need to develop a thorough, comprehensive, and exhaustive approach to the existence of the information space of Ukraine. The latter is analyzed in this thesis in the context of ensuring sustainable development (stability, genesis, etc.) and security (protection, preservation, etc.). In turn, this creates the need for an in-depth analysis of institutional factors and the development of effective strategies to counteract existing and potential threats to such a space.

The purpose of the study is to comprehensively and comprehensively study the institutional aspects of the formation and implementation of Ukraine's information and security policy, identify the main problems and challenges facing the state in this area in the context of external aggression, and develop recommendations for optimizing the institutional mechanism for ensuring information security based on the best national and international practices.

The object of the study is the institutional factors of Ukraine's information and security policy in the context of external threats and influences.

The subject of the study is the processes and patterns of formation and implementation of Ukraine's information and security policy, taking into account international experience, to combat russian aggression.

Achievement of the above goal, object, and subject of the dissertation was achieved by solving several research *tasks*:

– to supplement and systematize the theoretical and methodological foundations of the study of the concept of national security and its digitalization dimension in the context of institutional factors of information and security policy;

– to highlight the transformational changes in the categorical and conceptual apparatus of the above-mentioned policy in terms of dynamics, specificity, etc. of the latter to highlight the correlations between the concepts of national and information security;

– to distinguish the original genesis of the concept of national interests in the digitalization dimension and to categorize, structure, etc., arranging it by importance in terms of external/internal components;

– to trace the peculiarities of the information space system, differentiating the latter in terms of functional parameterization of its specific tasks;

– to study and formulate the author's definition of the concept of the state-legal mechanism of information security, analyzing the source (regulatory framework) and evaluating the effectiveness of existing models of the latter;

– to analyze current challenges to the security of Ukraine's information space in the context of the parameterization features of the deployment of the hybrid russian-Ukrainian war and the information aggression that accompanies it;

– extrapolate the international experience of Western partner states in information confrontation during hybrid and information wars;

– to identify the types of existing and potential threats posed by the Russian Federation to Ukraine to formulate recommendations for the adaptation and implementation of the above practices, strategies, etc.

As a result of the study, the applicant obtained the following scientific results, which are due to a comprehensive, thorough study of the originality of the genesis of institutional factors of Ukraine's information and security policy. The latter is studied in correlation with several challenges in the context of the hybrid and information russian-Ukrainian war. In particular, the scientific work fills the following gaps in the analyzed issues:

For the first time: a) approaches to understanding information security as a component of the national security of the state are comprehensively studied and the role and place of institutional factors in its functioning are localized; b) developed and substantiated a theoretical model of institutional interaction in the field of information security is developed and substantiated, which takes into account the specifics of hybrid warfare and the need to adapt the national security strategy to changing conditions of the internal and external environment; c) a wide range of historiography and a representative source based on the analyzed issues were processed to trace the genesis of institutional factors of Ukraine's information and security policy and their role in this process; d) the author's definition of the concept of national security and information and security policy was proposed on the above

basis; e) the types of existing and potential threats posed by the Russian Federation to Ukraine were identified, recommendations for the adaptation and implementation of practices, strategies, etc. of the above-mentioned.

The author clarifies and improves: a) the theoretical and methodological foundations of the study of the concept of national security and its digitalization dimension in the context of institutional factors of information and security policy; b) the categorical and conceptual apparatus of such a policy regarding the dynamics, specificity, etc. of the latter to highlight the correlations between the concepts of national and information security; c) the peculiarities of the information space system with the differentiation of the latter in terms of the functional parameterization of its specific tasks.

A new level was given to the provisions on: a) the original genesis of the concept of national interests in the digitalization dimension in terms of their categorization, structuring, etc. with the alignment of importance in terms of external/internal components and correlation with the impact of legislative and regulatory documents on the formation of the information space of Ukraine; b) the role of institutional factors in the process of forming and implementing information and security policy in the context of international experience (information confrontation during hybrid and information wars) and the identification of optimal models of interaction between different institutional actors (including government agencies, public institutions and international organizations); c) key principles and mechanisms of international cooperation in the field of information security, which can become the basis for the development of new international treaties and agreements, as well as several challenges to the security of the information space in the context of the parametrization features of the hybrid russian-Ukrainian war and the information aggression that accompanies it.

The practical significance of the study lies in the possibility of using its scientific achievements in the educational process (in particular, lectures, seminars, tests, exams, etc. in higher education institutions). In addition, the data of the dissertation research can be actualized in the development of training courses in

several political science, sociology, and other disciplines. In particular, in such areas of training as “National Security”, “Political Science”, “International Relations”, “European Studies”, “Information Security” and others. In addition, its results can be used to create textbooks, manuals, guidelines, etc., as well as in writing scientific research (term papers, diploma papers, master’s, PhD, and doctoral dissertations). Also, the materials of the scientific work are intended to contribute to the further development and direct contribution to strengthening the national security of Ukraine, building the resilience of the information space to external and internal challenges, as well as to ensuring favorable conditions for the development of the information society in the country.

Key words: war, martial law, hybrid war, disinformation, digitalization, information security, information security policy, information policy, information society, information space, European Union, European integration, national security, political communication, political participation.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях України:

1. Галіпчак В. Інформаційна війна як складова гібридної війни в умовах російьскої агресії. *Вісник Прикарпатського університету. Політологія.* 2023. №15. С. 26-32.

DOI: https://doi.org/10.32782/2312-1815/2024-1-4

URL: http://politicus.od.ua/index.php/2023-ukr?id=64

2. Галіпчак В. Інституційні чинники інформаційної політики євроінтеграції України: безпековий вимір. *Політикус.* 2023. №3. С. 97-102.

DOI https://doi.org/10.24195/2414-9616.2023-3.17

URL: http://politicus.od.ua/index.php/2023-ukr?id=64

3. Галіпчак В. Безпека інформаційного простору України в умовах російської агресії на сучасному етапі: основні завдання та виклики. *Науковий журнал «Регіональні студії»,* 2023. №34. С. 81-85.

DOI https://doi.org/10.32782/2663-6170/2023.34.13

URL: http://regionalstudies.uzhnu.uz.ua/index.php/34

4. Галіпчак В. Трансформація інформаційного простору України під впливом російськоїагресії: зміни та виклики. *Політикус.* 2023. №4. С. 26-31.

DOI https://doi.org/10.24195/2414-9616.2023-4.4

URL: http://politicus.od.ua/index.php/2023-ukr?id=65

5. Галіпчак В. Державно-правовий механізм інформаційної безпеки України в умовах російської агресії. *Політикус.* 2023. №5. С. 19-24.

DOI https://doi.org/10.24195/2414-9616.2023-5.3

URL: http://politicus.od.ua/index.php/2023-ukr?id=66

6. Галіпчак В. Сучасні виклики та стратегії забезпечення інформаційної безпеки України в умовах російської агресії: перспективи та завдання. *Науковий журнал «Регіональні студії».* 2023. №35. С. 65-70.

DOI https://doi.org/10.32782/2663-6170/2023.35.10

URL: http://regionalstudies.uzhnu.uz.ua/index.php/35

Статті у періодичних наукових виданнях інших держав, включених до міжнародних наукометричних баз Scopus/Web of Science:

7. Slobodianiuk A., Vonsovych S., Bezerovska-Chmil O., Nykorovych Y., Halipchak V. Political aspects of decision-making . *AD ALTA: Journal of Interdisciplinary Research. Web of Science. The Czech Republic.* 2023. Volume 13. Issue 2. Page 23-26.

URL: https://www.magnanimitas.cz/ADALTA/130236/papers/A_04.pdf

Список публікацій здобувача, які додатково відображають наукові результати дисертації:

8. Галіпчак В. Здійснення інформаційної політики євроінтеграції. Безпека інформаційного суспільства ЄС. *Прикарпатський вісник НТШ. Думка.* 2021. №5. С. 21-24.

URL:https://pnu.edu.ua/wp-content/uploads/2021/04/Програма-звітної-конференції-викладачів-за-2020-рік-2.pdf

9. Галіпчак В. Державно правовий механізм забезпечення інформаційної безпеки. *Матеріали ІІІ Всеукраїнської науково-практичної конференції «Політичні процеси сучасності: глобальний та регіональний вимір» (м.Івано-Франківськ, 27-28 травня 2021р.).* Івано-Франківськ: Прикарпатський національний університет імені Василя Стефаника, 2021.

URL:https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/56376/1/Збірник%20Конференції%2027-28%20травня%202021%20%28Івано-Франківськ%29.pdf

10. Галіпчак В. Основні методологічні засади поняття національної безпеки: інформаційий вимір. *POLITIA. Вісник наукових робіт молодих вчених.* Івано-Франківськ: ЯРИНА, 2023. Вип. 5. С. 192–225.

URL:https://kpip.pnu.edu.ua/wp-content/uploads/sites/121/2023/04/politia-5.pdf

11. Галіпчак В. Державно-правовий механізм здійснення інформаційної безпеки: агенти і методи впливу. *Матеріали Всеукраїнської науково-практичної конференції « Теоретичні та практичні аспекти політичного розвитку в Україні і світі в умовах повномасштабної російсько-української війни (пам'яті Любомири Мандзій)» (м.Львів, 10 травня 2023р.).* Львів: Львівський національний університет імені Івана Франка, 2023. С. 40-42.

URL:https://filos.lnu.edu.ua/wpcontent/uploads/2023/05/Conf_Program_May23.pdf

12. Галіпчак В. Роль інституційних механізмів у запезпеченні інформаційної безпеки: аспекти управління та взаємодії. *IX Міжнародна науково-практична конференція «Практичні та теоретичні питання розвитку науки та освіти» (м. Львів, 29-30 жовтня 2023 року).* Львів: Львівський науковий форум, 2023р. С. 35-37.

URL:http://www.lviv-forum.inf.ua/save/2023/29-30.10/Збірник.pdf

13. Галіпчак В. Вплив інформаційних технологій на захист національних інтересів в Україні: виклики та можливості. *X Міжнародна науково-практичніа конференція «Пріоритетні шляхи розвитку науки і освіти» (м. Львів, 29-30 листопада 2023 року).* Львів: Львівський науковий форум, 2023р. С. 70-73.

URL:http://www.lviv-forum.inf.ua/save/2023/29-30.11/Збірник.pdf

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

АІЗ	Автоматизовані інтелектуальні засоби
АРК	Автономна Республіка Крим
АТО	Антитерористична операція
ВПС	Всесвітній поштовий союз
ВРУ	Верховна Рада України
ГДЄСПІС	Генеральний Директорат ЄС з проблем інформаційного суспільства
ГІ	Глобальна інформаційна інфраструктура
ГО	Громадська організація
ГУР	Головне управління розвідки
ДКЗІУ	Державний комітет зв'язку та інформатизації України
ДБР	Державне бюро розслідувань
Держспецзв'язку	Державна служба спеціального зв'язку та захисту інформації України
ДІП	Державна інформаційна політика
ДПС	Державна прикордонна служба
ДПМ	Державно-правовий механізм
ЗЗСО	Заклад загальної середньої освіти
ЄАЕС	Євразійський економічний союз
ЄК	Європейська комісія
ЄР	Європейська Рада
ЄС	Європейський Союз
ЄСЦБ	Європейська система центральних банків
ЗВО	Заклад вищої освіти
ЗМІ	Засоби масової інформації
ЗСУ	Збройні сили України
ІА	Інформаційна атака
ІБ	Інформаційна безпека
ІБП	Інформаційно-безпекова політика

ІВ	Інформаційна війна
ІВі	Інформаційні відносини
ІЗ	Інформаційна загроза
ІК	Інформаційна комунікація
ІКС	Інформаційно-комунікаційний процес
ІКТ	Інформаційно-комунікативні технології
ІО	Інформаційні одиниці
ІП	Інформаційна політика
ІПр	Інформаційний простір
ІПС	Інформаційно-пошукова система
ІР	Інформаційні ресурси
ІС	Інформаційний суверенітет
ІТ	Інформаційні технології
ІТС	Інформаційно-телекомунікаційна система
ІТТ	Інформаційні та телекомунікаційні технології
ІФ	Інформаційна безпека
КМІС	Київський міжнародний інститут соціології
КПНБО	Комітет з питань національної безпеки та оборони
КМУ	Кабінет Міністрів України
МБ	Міжнародна безпека
МВС	Міністерство внутрішніх справ України
МДА	Місцеві державні адміністрації
Міноборони	Міністерство оборони України
Мінцифри	Міністерство цифрової трансформації України
МІП	Міністерство інформаційної політики
МСЕ	Міжнародний союз електрозв’язку
НАТО	Північноатлантичний альянс
НБ	Національна безпека
НБУ	Національний банк України
НГУ	Національна гвардія України

НІ	Національні інтереси
НІД	Національні інтереси держави
НКСДМ	Національна комісія зі стандартів державної мови
НС	Надзвичайна ситуація
НЦК	Національний центр кібербезпеки
ОБСЄ	Організація з безпеки і співробітництва в Європі
ОМС	Органий місцевого самоврядування
ОУН	Організація українських націоналістів
ПК	Персональний комп'ютер
РНБО	Рада національної безпеки і оборони
рф	російська федерація
р.	рік
РДС	Реєстр державних сертифікатів
СБУ	Служба безпеки України
СВО	Спеціальна воєнна операція
СЕРЇ	Європейська конференція адміністрацій зв'язку
СПІБ	Система продукування інформаційної безпеки
СРСР	Союз Радянських Соціалістичних Республік
ст.	століття
США	Сполучені Штати Америки
УПА	Українська повстанська армія
ФІС	Форум інформаційного суспільства
ЦА	Цільова аудиторія
ЦНАП	Центр надання адміністративних послуг
ЦОВВ	Центральні органи виконавчої влади
ЦПД	Центр протидії дезінформації
COSME	Competiveness of Small and Medium Enterprises
CORDIS	Community Research and Development Information Service
EDA	European Defence Agency

eIDAS	electronic IDentification, Authentication and trust Services
eEurope	Electronic Europe
EEA	European Environment Agency
EPO	European Patent Office
ETSI	European Telecommunications Standards Institute
FRA	European Union Fundamental Rights Agency
FRONTEX	European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union
G7	Велика Сімка (Група Семи)
ITU	International Telecommunication Union
UPU	Universal Postal Union

ВСТУП

Для сучасного світу притаманний динамічний розвиток інформаційних технологій (самобутні диджиталізаційні зміни), які, першоєю чергою, детерміновані зростанням ролі інформації в житті суспільства та держави. Останнє природно зумовлює потребу виформовування ефективних механізмів захисту інформаційного простору, що вкрай актуальне щодо збереження національної безпеки. Особливу увагу при цьому слід звернути на здатність інформаційного простору впливати не лише на стратегічні комунікації, а й на політичну участь громадян, що в умовах війни стає критично важливим аспектом демократичного державотворення. Своєю чергою, особливої значущості набуває розгляд інституційних чинників інформаційно-безпекової політики, що пов'язане з стрижневою роллю останніх щодо підґрунтя, розвитку та реалізації стратегій захисту інформаційного простору країни.

Мовиться про те, що аналіз вищезазначених чинників репрезентативний не лише щодо наявних викликів та загроз, а й локалізації, ідентифікації тощо потенційних лакун, натомість врахування останніх продукує зміцнення інформаційної безпеки. Саме тому вибір теми дослідження базований на низці релевантних складників, побутування яких корелює з актуальністю та значущістю цього напряму дослідження на сьогодні. Зокрема:

а) *геополітичний контекст* (полягає у актуалізації таких елементів як діахронія (вертикальна локалізація стану інформаційної безпеки безвідносно до її попереднього контексту (трансформаційних змін, станів, специфіки), яка полягає у аналізі тієї чи тієї параметризації на певному етапі: до прикладу, актуальний стан) і синхронія (горизонтальна локалізація – її суть у відстеженні динаміки генези такої безпеки з низкою причиново-наслідкових зв'язків: до прикладу: мовиться про врахування таких релеватних віх як анексія Криму, події на Сході України та широкомасштабне вторгнення країни-агресора, які зумовлюють не лише військову, а й інформаційну лінію фронту);

б) *збільшувана релевантність інформаційного простору* (йдеться про зростаючу роль даних щодо впливу на громадську думку (дезінформацію, мізінформацію, пропаганду тощо), формування тих чи тих наративів як складників самобутнього сторітеллінгу, нової міфології тощо, що, своєю чергою, стають частиною модерної ідеологічної полісистеми, метою якої є маніпулювання свідомістю громадян, впливаючи, зокрема, й на рівень політичної участі — через формування штучних електоральних наративів, фейкових мобілізаційних меседжів або спроби делегітимізувати участь у виборах, акціях, дискусіях;

в) *лакунізованість аналізованої проблематики* (репрезентована дуальною природою останньої: з одного боку, спостерігаємо зростаючу роль проблем інформаційної безпеки, що зумовлює аналіз інституційних чинників, які релевантні щодо формування та реалізації вищезазначеної політики в нашій країні; з іншого – постулюємо відсутність комплексного підходу до вищезазначеного питання й потребу у синхронічному підході до нього, який продукуватиме актуалізацію наукового спадку і забезпечить органічність, питомість, адаптивність тощо продукованих кроків заради такої політики);

г) власне, *актуальність* (детермінована гібридною російсько-українською війною, яка позначена функціонуванням цілої низки неправдивих, викривлених тощо даних, що використовуються ворогом для дискредитації влади, ВСУ, мобілізаційних заходів та іншого й протидія яким безпосередньо пов’язана з самобутністю актуалізації інституційних чинників у безпековій політиці сучасної України) й ґ) *глобалізаційний контекст* (полягає у інтеграції міжнародного досвіду (концепцій, практик, кампаній тощо) щодо інформаційно-безпекових ініціатив й адаптації ефективного інструментарію задля протидії низці інформаційних загроз на українському підґрунті).

Актуальність теми дослідження зумовлена експонетним зростанням наявних викликів інформаційної безпеки, посилених російською агресією в Україні. Останнє спродукувало потребу у оперативному реагуванні її уряду на

поточні загрози з вибудовуванням політичних концепцій, стратегій, практик тощо. Першою чергою, це пов'язане з формуванням стійкості інформаційного простору до можливих вразливостей у майбутньому й вибудовуванням сценаріїв протидії їм. Своєю чергою, актуальним також є вивчення параметризаційних особливостей в контексті генези наукових підходів до поняття інформаційної безеки та розробки ефективних стратегій її функціонування в умовах сучасних диджиталізаційних й геополітичних загроз.

Показово, що досліджені у науковій роботі теоретико-методологічні засади поняття національної безпеки у диджиталізаційному вимірі дозволяють здійснити глибокий аналіз інформаційної безпеки як геополітичної детермінанти (державності). Натомість глибокий аналіз безпеки інформаційного простору України з екстраполяцією сучасних викликів та міжнародного досвіду продукує вичленування самобутності українського контексту та виокремлення релевантних напрямів генези інформаційно-безпекової політики.

Отже, вибір теми дослідження детермінований не лише актуальністю аналізованої проблематики, а й потребою у випрацюванні ґрунтовного, комплексного й вичерпного підходу до побутування інформаційного простору України. Останній проаналізовано у межах дисертації в контексті гарантування сталого розвитку (стабільності, генези тощо) й безпеки (захисту, збереження та іншого). Своєю чергою, це продукує потребу у глибокому аналізі інституційних чинників й випрацювання ефективних стратегій щодо протидії наявним і потенційним загрозам для такого простору.

Зв'язок дослідження з науковими програмами, планами й темами. Робота виконана на кафедрі політичних наук Прикарпатського національного університету імені Василя Стефаника.

Мета і завдання дослідження. *Метою роботи* є комплексне та всебічне вивчення інституційних аспектів формування та реалізації інформаційно-безпекової політики України, виявлення основних проблем та викликів, що

стоять перед державою у цій сфері в контексті зовнішньої агресії, а також розробка рекомендацій щодо оптимізації інституційного механізму забезпечення інформаційної безпеки на базі кращих національних та міжнародних практик.

Досягнення вищезазначеної мети дисертаційної роботи можливе через розв'язання низки дослідницьких *завдань*:

– доповнити й систематизувати теоретико-методологічні засади дослідження поняття національної безпеки та її диджиталізаційний вимір у контексті інституційних чинників інформаційно-безпекової політики;

– висвітлити трансформаційні зміни категорійно-понятійного апарату інформаційно-безпекової політики України щодо його динаміки, специфіки тощо задля виокремлення кореляцій між поняттям національної та інформаційної безпеки;

– виокремити самобутню генезу поняття національних інтересів у диджиталізаційному вимірі, категоризувавши, структурувавши, вибудувавши за значущістю щодо зовнішніх/внутрішніх складників;

– відстежити особливості побутування системи інформаційного простору, диференціюючи останню щодо функційної параметризації покладених на неї питомих завдань;

– сформулювати власне визначення поняття державно-правового механізму інформаційної безпеки, проаналізувавши джерельну (нормативно-правову базу) та оцінивши ефективність наявних моделей останнього;

– проаналізувати сучасні виклики безпеці інформаційного простору України в контексті параметризаційних особливостей розгортання гібридної російсько-української війни та інформаційної агресії, яка її супроводжує;

– екстраполювати міжнародний досвід західних держав-партнерів щодо інформаційного протистояння під час гібридних й інформаційних воєн;

– ідентифікувати види наявних та потенційних загроз, продукованих російською федерацією для України, задля формування рекомендацій до адаптації й імплементації вищезазначених практик, стратегій тощо.

Об'єктом дослідження є інституційні чиннинки інформаційно-безпекової політики України в умовах зовнішніх загроз та впливів.

Предмет дослідження становлять процеси та закономірності формування й реалізації інформаційно-безпекової політики України з урахуванням міжнародного досвіду для боротьби проти російської агресії.

Методи дослідження. Специфіка вищезазначених мети, об'єкта, предмета дослідження продукують широту спектра його методології як низки відносних системно-організованих способів аналізу. Зокрема, у дисертаційній роботі актуалізовано загально-, спеціально-наукові та філософсько-світоглядні методи дослідження. У межах останніх виділимо: *аналітичний метод* (використано для аналізу теоретико-методологічної (історіографії) та джерельної (нормативно-правових документів) бази дослідження, є продуктивним для локалізації стрижневих принципів, підходів та викликів інформаційно-безпекової царини); *емпіричний метод* (актуалізовано для збору первинних даних (під час опитування, інтерв'ю й анкетування експертів, державних службовців, представників медіа та громадськості), що висвітлюють актуальний стан інформаційної безпеки в Україні); *компаративний аналіз (порівняльний метод)* (репрезентативний щодо порівняння інформаційно-безпекових політик України та інших країн, наслідком чого є можливість визначення найпродуктивніших практик, стратегій та іншого й окреслення перспектив їх імплементації на українському підґрунті); *метод системного аналізу* (дозволив дослідити самобутність інформаційної безпеки як складної системи взаємопов'язаних елементів: нормативно-правової бази, інституційної структури, механізмів взаємодії та низки зовнішніх впливів); *метод кейс-стаді* (застосовано для глибокого аналізу низки інформаційних атак, кіберзагроз та/або прикладів успішних стратегій, практик, кампаній тощо в царині інформаційної безпеки); *SWOT-аналіз* (використано для унаочнення функційних особливостей детермінант, які впливають на інформаційно-безпекову політику України, а також аналізу останньої в контексті розробки ефективних стратегій інформаційної безпеки);

метод документального аналізу (репрезентативний у роботі з вищезазначеною джерельною базою: нормативно-правовими документами та іншим); *метод моделювання* (став у нагоді в процесі побудови теоретичних моделей інформаційно-безпекової політики, що можуть бути використані для прогнозування перебігу подій та аналізу потенційних сценаріїв розвитку ситуації у досліджуваній царині); *метод прогнозування* (використано для визначення потенційних сценаріїв розвитку інформаційно-безпекової ситуації в Україні щодо російської агресії та низки внутрішніх викликів); *метод контент-аналізу* (актуалізовано для ґрунтовного, комплексного вивчення інформаційного контенту, який поширюється через масмедіа, соціальні мережі, нормативно-правові документи та інші ресурси в контексті ідентифікування дезінформаційних осередків й виокремлення специфіки розповсюдження ними неправдивих даних); *івент-аналіз (аналіз подій)* (дозволив здійснити систематичне вивчення релевантних подій, що впливають на інформаційно-безпекову ситуацію в Україні (інциденти кібербезпеки, інформаційні кампанії, політичні заяви та інші значущі події) й продукують вибудовування причиново-наслідкових зв'язків між ними й динамікою інформаційних потоків, а також специфікою реагування на них державних і недержавних інституцій). Отже, вищезазначені методи забезпечили фундаментальний, комплексний підхід до аналізу інституційних чинників інформаційно-безпекової політики в Україні та дозволили вивчити аналізовану проблематику на належному рівні.

Теоретико-методологічне підґрунтя дослідження інституційних чинників інформаційно-безпекової політики України становить широкий спектр історіографії. Зокрема, праці таких дослідників, як: Р. Алямкін, І. Арістова, А. Атрохов, Ю. Бабенко, А. Бабінська, А. Баранов, І. Беззуб, О. Березовська-Чміль, П. Біленчук, В. Білоус, В. Богданович, Л. Борисова, В. Богуш, І. Боднар, О. Боднарчук, О. Бодрук, В. Бондаренко, В. Брижко, М. Вавринчук, О. Власюк, О. Войтенко, Т. Ворожко, О. Гальченко, І. Герасимов, А. Геращенко, О. Гіда, Н. Голуб'як, О. Гончаренко, Ю. Горбань,

В. Горбулін, В. Горленко, В. Гриценко, В. Гурковський, В. Гусаров, С.Даниленко, О. Данільян, О. Дзьобан, В. Демченко, С. Дерев'янко, Н. Дніпренко, А. Добровольська, О. Довгань, К. Долженко, О. Дубас, Д. Дуцик, О. Єрмак, С. Єсімов, В. Єфімова, М. Загирняк, І. Залевська, К. Захаренко, І. Зіма, О. Зозуля, Д. Іваненко, О. Іванов, О. Іванова, Є. Іванова, С. Кавун, Р. Калюжний, А. Катренко, Є. Кирильчук, О. Кириченко, О. Кісілевич-Чорнойван, С. Климовський, Ю. та Т. Кобець, А. Козьміних, В. Конах, Я. Кондратьєв, М. Копійка, Б. Кормич, С. Корнієнко, М. Корольов, О. Косогоров, Л. Кочубей, Є. Кравець, Ю. Кравченко, Н. Крилова, Р. Кузьмінська, М. Левицька, О. Левченко, Є. Лисицин, М. Литвин, О. Литвиненко, М. Лібікі, В. Ліпкан, О. Лісовський, О. Логінов, І. Логовський, М. Лях, Є. Магда, Є. Макаренко, Ю. Максименко, І. та Я. Малик, О. Манжай, В. Марков, Р. Марутян, В. Марчук, С. Матвієнків, М. Махній, О. Мацегора, М. Міщук, О. Мороз, В. Недбай, І. Неклонський, Г. Несвіт, Н. Нижник, І. Ніколаєв, О. Ніщименко, Н. Новицька, В. Носов, О. Олійник, В. Олуйко, В. Отрешко, В. Павловський, М. Панов, О. Панченко, А. Парубій, В. Петрик, В. Пилипчук, І. Поліщук, Почепцов, М. Присяжнюк, Д. Приходько, І. Проноза, Ю. Радковець, Л. Рачковська, М. Рибак, Ю. Романчук, Н. Ротар, І. Рудь, І. Рущенко, Г. Сащук, В. Світлична, А. Семенченко, Н. Семенюк, О. Семченко, М. Сенченко, Г. та Т. Ситник, А. Сірик, В. Собина, В. Сливка, І. Сопілко, О. Соснін, В. Степаненко, А. Суббот, А. Тарасюк, Т. Ткачук, А. Турчак, Г. Удренас, Ч. Фань, О. Федорук, О. Фомін, Л. Харченко, В. Хімей, О. Холод, Г. Хоружий, В. Цимбалюк, В. Чмельов, Е. Чубарова, А. Шадур, В. Шамрай, О. Шаповалов, С. Шевченко, П. Шевчук, О. Шиманова-Стефанишин, Т. Шлемкевич, Н. Шотурма, В. Шульга, О. Юдін, М. Яремчук, В. Ященко, R. Allison, G. Avery, J. Bērziņš, H. Bey, Y. Biliusov, B. Buchanan, F. Cameron, B. Cherniavska, D. Chyzhov, R. Clarke, S. Derevianko, G. Diem, J. Dougherty, H. Dzhahupov, S. Feldstein, A. Friedman, K. Giles, M. Heras, M. van Herpen, F. Hoffman, S. Huntington, S. Janz, O. Jonsson, J. Kalenský, V. Kaletnik, L. Kello, R. Knake, V. Kotsur, J.-F. Kremer, T. Kuprii, M. Libicki,

T. Madryha, R. Maness, K. Martineau, T. Maurer, B. Müller, B. Nimmo, Y. Nykorovych, A. Osaulenko, R. Perelyhina, M. Rasmussen, A. Rathmell, T. Rid, M. Seddon, R. Seely, I. Semenets-Orlova, D. Shlapak, P. Singer, S. Shevchenko, A. Slobodianiuk, H. Tumber, S. Vonsovych, C. Watts, F. Webster та інші. Таким чином, історіографія аналізованої проблематики складається зі значного числа наукових праць, які засвідчують динамічний інтерес дослідників до проблеми інформаційно-безпекової політики загалом (зокрема, детермінації ролі інституційних чинників в процесі актуалізації останньої).

Наукова гіпотеза полягає у самобутності функціонування інституційних чинників інформаційно-безпекової політики щодо феномена українських політичних стратегій, кампаній, практик тощо й репрезентативності останніх до сучасних викликів, російської інформаційної агресії. Першою чергою, вищезазначене продукує імплементацію й адаптацію міжнародного досвіду (стратегій, практик, стандартів та іншого) з динамізацією співпраці із зарубіжними партнерами, підґрунтям чого є потреба у зміцненні української держави. Своєю чергою, ефективна інформаційно-безпекова політика полягає не лише у стримуванні та реагуванні на загрози, а й у проактивному формуванні позитивного інформаційного простору, сприянні медіаграмотності населення та розвитку незалежних медіа.

Натомість розвиток інституційного потенціалу в царині інформаційної безпеки (зокрема, через удосконалення законодавчої бази, професіоналізацію кадрів та впровадження передових технологій) може значно підвищити стійкість України до інформаційного впливу агресора. Відтак, стратегічне планування та координація інформаційно-безпекової політики на національному рівні, забезпечення її гнучкості та адаптивності до змінюваних умов і загроз є ключовими для гарантування інформаційної безпеки країни в довгостроковій перспективі.

Джерельна база. Питомими джерелами наукової роботи є нормативна-правова база: Закони України, укази Президента України, рішення та постанови Кабінету Міністрів, постанови Верховної Ради України,

нормативні-правові документи центральних органів виконавчої влади, а також рішення органів державного управління та місцевої влади.

Наукова новизна отриманих результатів дослідження зумовлена комплексним, ґрунтовним вивченням самобутності генези інституційних чинників інформаційно-безпекової політики України. Остання досліджена у корелятивному зв'язку з низкою викликів в умовах гібридної російсько-української війни. Зокрема, наукова робота заповнює такі лакуни у аналізованій проблематиці:

Уперше:

– комплексно досліджено підходи до розуміння інформаційної безпеки як складника національної безпеки держави й локалізовано роль і місце інституційних чинників у її функціонуванні;

– розроблено та обґрунтовано теоретичну модель інституційної взаємодії в царині інформаційної безпеки, яка враховує специфіку гібридної війни та потребу адаптації національної безпекової стратегії до змінюваних умов внутрішнього і зовнішнього середовища;

– опрацьовано широкий масив історіографії та репрезентативну джерельну базу з аналізованої проблематики задля відстеження генези інституційних чинників інформаційно-безпекової політики України та їх ролі у цьому процесі;

– запропоновано авторське визначення поняття національної безпеки та інформаційно-безпекової політики;

– ідентифіковано види наявних та потенційних загроз, продукованих російською федерацією для України, сформовано рекомендації до адаптації й імплементації практик, стратегій тощо вищезазначеної політики;

– проведено вивчення інформаційно-безпекових практик на основі SWOT-аналізу та методів прогнозування, що дозволило визначити ключові напрями оптимізації державної політики у цій царині.

Уточнено та вдосконалено:

– теоретико-методологічні засади дослідження поняття національної безпеки та її

диджиталізаційний вимір у контексті інституційних чинників інформаційно-безпекової політики;

– категорійно-понятійний апарат такої політики щодо динаміки, специфіки тощо останнього задля виокремлення кореляцій між поняттям національної та інформаційної безпеки;

– особливості побутування системи інформаційного простору з диференціацією останньої щодо функційної параметризації покладених на неї питомих завдань.

Новий рівень отримали положення про:

– самобутню генезу поняття національних інтересів у диджиталізаційному вимірі щодо їх категоризації, структуризації та іншого з вибудовуванням за значущістю щодо зовнішніх/внутрішних складників й кореляцією з впливом законодавчих і нормативних документів на формування інформаційного простору України;

– роль інституційних чинників в процесі формування й реалізації інформаційно-безпекової політики в контексті міжнародного досвіду (інформаційного протистояння під час гібридних й інформаційних воєн) та виокремлення оптимальних моделей взаємодії між різними інституційними суб'єктами (включаючи державні органи, громадські інституції та міжнародні організації);

– ключові принципи та механізми міжнародної кооперації у галузі інформаційної безпеки, що може стати основою для розробки нових міжнародних договорів та угод, а також низки викликів безпеці інформаційного простору в контексті параметризаційних особливостей розгортання гібридної російсько-української війни й інформаційної агресії, яка її супроводжує.

Теоретичне значення дослідження детерміноване можливістю використання матеріалів, висновків, результатів, додатків та іншого у низці подальших гуманітарних студій з політології, соціології, культурології, історії культури, культурній антропології, прикладної лінгвістики, соціолінгвістики

тощо. Також вищезазначені дані репрезентативні щодо вивчення політичних практик, стратегій та іншого у межах інформаційно-безпекової політики (зокрема, генези політичної думки, стратифікованої політичним дискурсом). Окрім того, ідеї, представлені у науковій роботі, унаочнюють трансформаційні зміни сучасних політичних досліджень щодо тенденції до інтеграції гуманітарних наук (зокрема, міжпредменого складника українського модерного державотворення, належного врядування і тому подібного). Щодо останнього, то представлене дисертаційне дослідження репрезентативне в контексті побутування соціокультурного складника розуміння інформаційної безпеки як детермінанти національної безпеки держави й ролі і місця інституційних чинників у її функціонуванні.

Практичне значення роботи полягає у можливості використання її наукових здобутків у навчальному процесі (зокрема, лекційних, семінарських заняттях, контрольних роботах, іспитах тощо у закладах вищої освіти). Поза тим, дані дисертаційного дослідження можуть бути актуалізовані під час розробки навчальних курсів з низки політологічних, соціологічних та інших дисциплін. Зокрема, за такими напрямами підготовки як «Національа безпека», «Політологія», «Міжнародні відносини», «Європейські студії», «Інформаційна безпека» та інші. Окрім того, його результати доцільно використати для створення навчальних підручників, посібників, методичних рекомендацій тощо, а також під час написання кваліфікаційних наукових праць. Також матеріали наукової роботи покликані сприяти подальшому розвитку та безпосередньому внеску в посилення національної безпеки України, формування стійкості інформаційного простору до зовнішніх та внутрішніх викликів, а також у забезпеченні сприятливих умов для розвитку інформаційного суспільства в країні.

Особистий внесок здобувача репрезентований актуалізацією широкого спектра історіографії й джерельної бази, які, своєю чергою, дозволили комплексно дослідити підходи до розуміння інформаційної безпеки як складника національної безпеки держави. Окрім того, вищезазначене стало

підґрунтям для локалізації ролі і місця інституційних чинників у функціонуванні такої політики й формулювання авторського визначення поняття національної безпеки та інформаційно-безпекової політики. Також розроблено та обґрунтовано теоретичну модель інституційної взаємодії в сфері інформаційної безпеки, яка враховує специфіку гібридної війни та потребу адаптації національної безпекової стратегії до змінюваних умов внутрішнього і зовнішнього середовища. Поза тим, актуалізовано нестандартний підхід до формулювання і вирішення дослідницьких завдань, використання інноваційної методології для їх розв'язання, а також висвітлено самобутність генези інституційних чинників інформаційно-безпекової політики. Теоретичні та практичні результати, які виносяться на захист, отримані автором самостійно, є достовірними, об'єктивними й відтворюваними.

Апробація результатів дослідження. Основні положення та результати дисертаційної роботи було обговорено на засіданнях кафедри політичних наук Прикарпатського національного університету імені Василя Стефаника. Вони також представлені в доповідях на таких конференціях: III Всеукраїнській науково-практичній конференції «Політичні процеси сучасності : глобальний та регіональний вимір» (м. Івано-Франківськ, 27–28 травня 2021 р.); Всеукраїнській науково-практичній конференції «Теоретичні та практичні аспекти політичного розвитку в Україні і світі в умовах повномасштабної російсько-української війни (пам'яті Любомири Мандзій)» (м. Львів, 10 травня 2023 р.); IX Міжнародній науково-практичній конференції «Практичні та теоретичні питання розвитку науки та освіти» (м. Львів, 29–30 жовтня 2023 р.); X Міжнародній науково-практичній конференції «Пріоритетні шляхи розвитку науки і освіти» (м. Львів, 29–30 листопада 2023 р.).

Публікації. За темою дисертаційної роботи опубліковано 13 наукових праць, з них – 6 статей у наукових фахових виданнях України, 1 стаття – у науковому фаховому виданні інших держав, включеному до Web of Science, 6

статей, які додатково відображають наукові результати дисертації.

Структура та обсяг дисертації. Дисертація складається зі вступу, трьох розділів, що поділяються на дев’ять підрозділів, висновків, списку використаних джерел та літератури, який налічує 395 позицій, з них 81-на – іноземними мовами і 7-ми додатків. Загальний обсяг дисертації – 254 сторінки, з них основний текст – 179.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ПОНЯТТЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

1.1. Стан наукової розробки проблеми

Поточна геополітична ситуація (інформаційна й гібридна російсько-українська війна) засвідчує особливе місце інформаційно-безпекової політики (далі – ІБП) як складника сучасного соціополітичного дискурсу. Зокрема, така політика є інструментом підтримання національної безпеки (далі – НБ) і набула статусу засобу належного (і не тільки) врядування як інструмента суспільної стабільності тощо. Природно, що успішна реалізація інформаційно-безпекової політики детермінована низкою інституційних чинників, які забезпечують злагодженість, неперервність, накопичувальну природу тощо дій державних інституцій та інших структур заради загальної вищезазначеної мети.

Показовою є роль інституційних чинників (державних органів), які, на нашу думку, доцільно ранжувати на такі гілки влади:

1. *Законодавчу* – забезпечує правову базу у вигляді низки нормативно-правових документів, які покликані уможливити функціонування ініціатив у межах ІБП за умов воєнного стану. До прикладу: мобілізаційні та демобілізаційні заходи, соціальну підтримку військовослужбовців і громадян та ін. Питомою властивістю нормативно-правової бази за таких умов є *адаптивність* і *гнучкість* (дають змогу оперативно усунути поточні ускладнення та забезпечують наступність і сталість, а також стратегічну природу рішень), *прозорість* і *повнота охоплення* (мовиться про наскрізний характер тих чи тих ініціатив щодо всієї низки нормативно-правових документів) тощо. Показовим при цьому є статус системи «Оберіг» та застосунку «Резерв+», які згадуються в одних документах і відсутні в інших, що продукує неоднозначність їх статусу фахівцями з юриспруденції.

2. *Судову* – функційно призначена унеможливити нехтування правами громадян за умов воєнного стану: така параметризаційна природа цієї гілки продукує потребу в незалежній, неупередженій діяльності судів, які покликані захищати громадян від локальних і системних зловживань уповноважених органів і забезпечити справедливий розгляд справ, пов'язаних з інформаційною (і не тільки) безпекою тощо.

3. *Виконавчу*, яка є стрижневою щодо ІБП, оскільки саме вона забезпечує адаптивність, динамічну реакцію тощо таких органів на поточні інформаційні загрози. Окрім того, саме в межах її функціонування відбувається продукування злагодженої роботи державних інституцій (державних органів) та оперативне ухвалення рішень (ідеться передовсім про наявність механізмів такого процесу та динамічну взаємодію з іншими органами).

Діяльність вищезазначених гілок влади детермінована спектром викликів і загроз ІБП, які насамперед лімітують її. Мовиться про *кіберзагрози*, що унаочненні зростанням кібератак, ускладненням їх сценаріїв і широтою ураження. Далі доцільно згадати про низку *інформаційних операцій*, які мають за мету продукування дезінформаційних кампаній та актуалізацію неправдивих даних тощо. Вони покликані дестабілізувати ситуацію в Україні шляхом підриву довіри до державних інституцій і загалом влади. Безпосередньо з вищезазначеними операціями пов'язані *внутрішні виклики*: згадаймо реакцію певних українських блогерів-мільйонників на нещодавню атаку дитячої лікарні «Охматдит». У межах останньої різні люди (О. Волошин, Є. Коршик, В. Роговенко та ін.) просували однакові, сконструйовані російськими технологами, наративи: втомленість від війни, неможливість перемоги, потреба в зупинці смертей тощо.

Прикметно, що ефективність роботи державних органів детермінована двома складниками: а) *інституційною взаємодією* та б) *інституційною стійкістю*, які становлять інтерес у вимірі досліджуваної проблематики. Так, *А* корелює з метою ефективної ІБП, яка потребує кооперації, передовсім гілок виконавчої влади. Серед останніх доцільно згадати такі: *координаційні органи*

(здебільшого органи державної влади (вищезазначені інституції), які покликані узгоджувати діяльність учасників процесу управління в низці питань за умов воєнного стану), *міжвідомчі комісії* (акумулюючі для координації діяльності представників різних гілок влади, що дає змогу прискорювати розв'язання того чи того питання шляхом міжінституційних кореляцій) та *громадські ради* (покликані залучити громадськість до формування ІБП, підвищуючи рівень довіри до органів державної влади).

Натомість *Б* є репрезентативною щодо рівня безпеки тих чи тих державних інституцій у контексті зовнішніх / внутрішніх загроз, що включає низку компонентів, які корелюють зі складниками *А*. Так, доцільно згадати: *захист інституційної інфраструктури* (полягає в надійному убезпеченні політичної комункації та інформаційно-телекомунікаційних систем від інформаційних атак, яке здебільшого матеріалізовані низкою вимог Державної служби спеціального зв'язку та захисту інформації України (далі – Держспецзв'язку)); *підтримку інституційної довіри* (вищезазначено про можливість створення громадських рад, що частково забезпечує таку довіру, проте основною є параметризація діяльності інституції: зокрема, прозорість, зворотний зв'язок, логічність і зрозумілість інформаційних кампаній та ін.); *інституційну адаптивність* (здебільшого ранжована диджиталізаційними трансформаціями управлінських систем: так, державні інституції мають бути адаптивними до соціокультурних видозмін і викликів, що продукує потребу в інноваційному складнику в їх діяльності).

Усе викладене вище підтверджує стрижневу роль інституційних чинників у реалізації ІБП за умов воєнного стану. ІБП детермінована специфікою протидії викликам і загрозам інформаційної безпеки, що полягає в потребі комплексного підходу, динамічної діяльності та взаємодії на зовнішньому (міжнародному) і внутрішньому (національному) рівнях і актуалізації громадськості в її побутуванні. Елементами ІБП є координація роботи державних інституцій, генеза технологічної інфраструктури, розвиток нормативно-правової бази тощо.

Аналіз інституційної системи щодо інформаційної політики як складника протидії гібридній російсько-українській інформаційній війні вміщено в праці В. Гапоненко [343], у якій авторка висвітлює самобутність генези інститутів інформаційної політики, досліджує їх розвиток, ефективність тощо. Учена акцентує увагу на основних загрозах інформаційній безпеці України, серед яких називає лакунізованість і превентивність заходів, недостатню увагу до громадянської освіти тощо. Дослідниця пропонує розширене тлумачення інституційної системи протидії інформаційній війні, включаючи в це поняття державні та громадські інститути декомунізації, культурної пам'яті та ін.

Корелює зі згаданими вище дослідженням праця О. Бабікова та інших науковців («Balancing Interests: Criminal Proceedings & Private Life Interference Under Martial Law in Ukraine» [319]), у якій проаналізовано диференціацію меж допустимого втручання в приватне життя особи в законодавстві України та інших країн. Останню вчені досліджують щодо балансу інтересів учасників кримінального провадження під час проведення негласних заходів для здобуття інформації. Дослідники стверджують, що ними висвітлено шляхи актуалізації низки невирішених питань щодо регулювання кримінального процесуального законодавства, що дає змогу забезпечити баланс інтересів учасників кримінального провадження під час вищезазначених заходів. Натомість використання результатів негласних заходів збору інформації продукує комплексний і системний підхід до вдосконалення законодавства в цій царині за умов воєнного стану або під час проведення антитерористичної діяльності.

Дослідження особливостей організаційно-правового продукування інформаційної безпеки в умовах воєнного стану висвітлено в праці Б. Мельниченко та інших науковців («Organizational and legal principles of information security of enterprises in the conditions of martial law in Ukraine» [374]), у якій автори наголошують на тому, що за умов війниінформаційна безпека підприємств набуває іншого тлумачення, стаючи складником системи

НБ. На думку вчених, особливо значущою є специфіка організаційно-правового забезпечення та побутування стрижневих засад інформаційної безпеки. Дослідники пропонують запровадити спеціальний правовий режим здійснення інформаційної безпеки підприємств за умов воєнного стану з актуалізацією можливостей держави в цій царині. Зокрема, рекомендують використати правовий інструмент обмеження поширення даних про діяльність того чи того підприємства через актуалізацію локальних нормативно-правових документів. Останні мають за мету зміну приналежності таких даних в умовах воєнного стану до категорії таких, доступ до яких обмежено [374].

Стрижневий аспект ІБП, а саме виконання правоохоронцями своїх обов'язків за умовах воєнного стану висвітлено в праці Ю. Голоднюка та інших науковців («Administrative law governing the activities of law enforcement agencies under Martial Law» [315]), у якій вивчено самобутність механізму адміністративно-правового регулювання діяльності правоохоронних органів за умов воєнного стану. Автори зазначають, що під час збройного конфлікту злагодження діяльності вищезазначених органів сприяє встановленню правопорядку та дотриманню прав і свобод громадян.

Самобутність науково-методичного підходу до аналізу нормативно-правової бази, специфіки, форм взаємодії державних інституцій (тут – органів місцевого самоврядування та поліції) щодо створення безпечного середовища за умов воєнного стану висвітлено в праці А. Баска, О. Нестерцової-Собакар, М. Калімана («Interaction between Local Governments and the Police in Ensuring the Vital Functions of the Region and Creating a Secure Environment Under Martial Law: Legal and Economic Aspects» [321]). Автори з'ясували правові, економічні й організаційні засади взаємодії державних інституцій у контексті реалізації вищезазначеної діяльності, вони стверджують, що релевантними напрямами вдосконалення такого процесу на територіях, наближених до зони бойових дій, є: а) створення добровільних громадських формувань для охорони порядку; б) співпраця державних інституцій з органами безпеки підприємств критичної інфраструктури з метою виявлення колаборантів; в) контроль рівня

освітлення об’єктів дорожньої інфраструктури та звернення до відповідних державних інституцій задля його посилення вночі; г) відеонагляд за громадськими місцями та іншими об’єктами життєдіяльності громадян, які не контрольовані поліційними системами відеоспостереження; ґ) розширення кадрового резерву працівників воєнізованих формувань (за рахунок актуалізації співробітників та курсантів відомчих закладів: Міністерства внутрішніх справ (далі – МВС), Служби безпеки України (далі – СБУ), Державного бюро розслідувань (далі – ДБР) та інших); д) удосконалення та розширення фінансування задля врахування балансу між забезпеченням підтримки сталого розвитку регіону й гарантуванням побутування безпечного середовища.

Наступна праця А. Собакара, О. Нестерцової-Собакар [384] («Information Security of the Activities of Law Enforcement Bodies of Ukraine Under the Conditions of the Legal Regime of the Martial State» [384]) містить докладний аналіз наявних підходів до поняття інформації, інформаційної безпеки та інформаційного забезпечення державних інституцій (тут – правоохоронних органів). Зокрема, автори детально характеризують специфіку правового регулювання зазначених понять за умов воєнного стану та надають їх власні визначення, які враховують самобутність ситуації, що склалася. Окрім того, вчені висвітлюють нормативно-правову базу, актуальний стан та стрижневі проблеми інформаційного забезпечення державних інституцій. Дослідники виокремлюють питомі складники інформаційного забезпечення та зосереджуються на правовому статусі тих чи тих об’єктів критичної інфраструктури, підкреслюють стрижневу та координуючу роль вищезазначеної виконавчої влади, яка забезпечує злагоджену інформаційну взаємодію державних інституцій. Значущим є ґрунтовний аналіз міжнародних стандартів, стратегій, практик тощо щодо інформаційної взаємодії державних інституцій задля гарантування публічної безпеки за умов складної безпекової ситуації в Україні.

Натомість правові засади діяльності державних інституцій (тут – правоохоронних органів) за умов воєнного стану стали об'єктом вивчення праці В. Гусарова «Кремль розпочав нову інформаційну операцію проти України» [56]. Автор визначає правові засади з урахуванням модерних соціоекономічних, ідеологічних і безпекових проблем, акцентує увагу на локалізації організаційно-правових принципів, які репрезентативні щодо глибини змін у діяльності правоохоронних органів за умов воєнного стану. Особливу увагу приділено перспективності принципу ситуативного впровадження нових послуг для допомоги населенню. На думку автора, це може бути зведено до надання послуг з розміщення громадян в укриттях, забезпечення вразливих груп усім необхідним (питною водою, продуктами харчування) тощо.

Самобутність продукування державної безпеки в умовах воєнного стану в контексті функцій Національної гвардії України (далі – НГУ) є предметом дослідження О. Батюка, А Пузанова («Objectives and Functions of the National Guard of Ukraine as a Subject of Ensuring State Security Under Martial Law» [322]). Автори підкреслюють, що специфіка діяльності НГУ полягає в особливій організаційно-правовій природі, що корелює з унікальністю її завдань і функцій. Науковців зазначають, що дослідження державних інституцій (тут – правоохоронних органів) має релевантне теоретичне і практичне значення для оцінки суті та змісту діяльності НГУ. Показово, що остання є суб'єктом гарантування державної безпеки за умов воєнного стану: це, на думку авторів, дає підстави постулювати доцільність внесення змін до чинного законодавства України щодо статті 2 Закону України «Про Національну гвардію України».

Специфіку розкриття правового регулювання гарантування НБ в умовах воєнного стану (загрози, можливі взаємодії та перспективи) розкрито в праці А. Носача та інших науковців («Ensuring National Security under Martial Law Conditions: Legal Regulation, Threats, Cooperation and Directions for Improvement» [336]). Автори зазначають, що ІБП є комплексною системою, у

яку входять національні та міжнародні заходи. Учені зосереджують свою увагу на фінансуванні як важливому складнику продукування НБ: на їх думку, фінансова безпека є основою економічного розвитку. Дослідники підкреслюють, що основною загрозою фінансовій безпеці є корупція, яка руйнує генезу військово-промислового комплексу, перешкоджає розгортанню диджиталізаційних ініціатив тощо.

Низка правових проблем і перспектив державної політики в царині зайнятості населення за умов воєнного стану є предметом розгляду статті Д. Швеця та інших науковців («State Policy in the Field of Employment: Legal Problems and Prospects in the conditions of Martial Law» [385]), у якій автори обґрунтовують напрями змін ІБП та акцентують увагу на стратегічній необхідності соціальної спрямованості останньої. Учені встановлюють низку кореляцій воєнного стану й ринку праці, визначають ключові напрями ІБП та її основні завдання. Дослідники підкреслюють, що законодавча нерозмежованість повноважень державних інституцій продукує дисфункцію оперативних заходів у цій царині.

Особливості проходження державної служби за умов воєнного стану в контексті низки безпекових викликів репрезентовано в праці О. Салманової, І. Арістової та ін. («Peculiarities of Public Service Under the Legal Regime of Martial Law» [375]). Автори підкреслюють, що головною особливістю такої служби є диджиталізаційний складник, зокрема оцифрування публічних послуг. Окрім того, вчені виділяють потребу у відновлюваній природі державної служби на деокупованих територіях на тлі обмеженості матеріальних і кадрових ресурсів і відсутності матеріально-технічної бази. Дослідники доходять висновку, що особливості проходження державної служби за умов воєнного стану детерміновані передовсім перебудовою найрелевантніших сфер реалізації державної політики (зокрема, у царині безпеки й оборони).

Обґрунтовує підходи до особливостей (державного та місцевого) управління в умовах порушення безпеки і воєнного стану на території України

В. Воротін [391]. У аналізованому дослідженні автор визначає місце і роль системи антикризового управління в збалансуванні суспільних відносин у публічній сфери та виокремлює механізми координації дій суб'єктів управління, пропонує визначення змісту стрижневих понять антикризового державного управління та розробляє інструментарій розвитку державного управління (методологію його етапів). Пропонована модель спрямована на змістову категоризацію: ранжування доцільності актуалізації тих чи тих механізмів та інструментів антикризового управління як засобу досягнення мети в умовах воєнного стану та післявоєнної відбудови європейської держави. Дослідником розроблено інформаційну схему функціонування інституційного механізму антикризового управління за означених умов.

Своєрідний аналіз політичного інтернет-дискурсу в контексті ресурсного підходу в царині прикладної лінгвістики та цифрових гуманітарних наук висвітлено в праці О. Довганя [334], у якій автор відзначає тенденцію до превалювання в політичному інтернет-дискурсі маніпулятивних стратегій як репрезентанта прагнення до впливу на співбесідника учасників політичної комунікації, яка, на думку вченого, матеріалізована шляхом актуалізації експлікованої й імпліфікованої сугестивності, що превалює над аксіологічним компонентом. Дослідження репрезентативне щодо аналізу низки інформаційних кампаній російської федерації, які мають за мету підрив авторитету української влади, вплив на громадян тощо. Окрім того, перспективним автор вважає вивчення механізмів мовного впливу на адресата, який перебуває в конфліктогенному середовищі російсько-української гібридної війни.

Показовою в контексті аналізованої нами проблематики є інше дослідження О. Довганя [333], де автор зосереджує увагу на самобутності політичної лінгвістики. Науковець репрезентує специфіку текстів політичного інтернет-дискурсу, заломлюючи її в призмі диджиталізаційних змін (зокрема, машинного навчання). Дослідник зазначає, що аналіз текстів такого дискурсу й ІБП нерозривні, оскільки боротьба з продукуванням, побутуванням тощо

низки неправдивих даних у вищезазначеному середовищі (дезінформації, мізінформації, пропаганди) є питомим складником такої діяльності. Автор вбачає перспективним напрямом ІБП диджиталізацію процесів боротьби з такими явищами: зокрема, розвиток алгоритмів машинного навчання, здатних локалізувати наративні джерела. На думку вченого, останні продуктивні в контексті пристосування до плинних смислів політичного інтернет-дискурсу й ґрунтовного аналізу в його межах у всьому різноманітті форм і методів.

Аналіз динаміки розвитку професійної компетентності викладачів закладів вищої освіти (далі – ЗВО) за умов воєнного стану представлено в праці М. Вайнтрауба [390], у якій автор акцентує увагу на значущості та злободенності розвитку професійної компетентності щодо низки специфічних вимог і викликів. Учений виокремлює самобутні складники професійної компетентності педагогічних працівників за умов воєнного стану: безпеку життя, здоров'я та охорони праці; правила та поведінку в надзвичайних ситуаціях (далі – НС) під час війни; адаптацію освітніх програм тощо. Дослідник презентує розроблену модель розвитку професійної компетентності науково-педагогічних працівників ЗВО в умовах воєнного стану у вигляді графа.

Отже, проведений аналіз історіографії з досліджуваної проблематики унаочнив специфіку феномена ІБП, детермінованого низкою інституційних чинників за умов воєнного стану, та виявив лакунізовану природу цієї проблеми. Мовиться насамперед про комплексну, інтегровану, міжпредметну та дискурсивну природу останньої, яка продукує потребу в її ґрунтовному аналізі в контексті сучасних гуманітарних досліджень у диджиталізаційному вимірі. Це, природно, спричиняє спрямованість нашої наукової роботи на заповнення вищезазначених лакун задля: а) комплексного та всебічного вивчення інституційних аспектів формування та реалізації ІБП України; б) виявлення основних проблем і викликів, що стоять перед державою в цій царині в контексті зовнішньої агресії; в) розробки рекомендацій щодо

оптимізації інституційного механізму гарантування інформаційної безпеки на базі найкращих національних та міжнародних практик.

Релевантними стратегіями актуалізації ІБП в умовах воєнного стану є: а) *генеза нормативно-правової бази* (вищезазначені законодавча й судова гілки, які продукують розробку низки нормативно-правових актів, що регулюють діяльність у інтернет-дискурсі (кіберпросторі), захист персональних даних, боротьбу з неправдивими даними тощо); б) *розбудова технологічної структури* (передовсім виконавча влада, представлена діяльністю Держспецзв'язку та низкою ініціатив Міністерства цифрової трансформації України (далі – Мінцифри)); в) *ефективна робота з кадрами* (ідеться про постійне підвищення кваліфікації, професійну освіту та розвиток кадрового резерву: стажування, обмін досвідом тощо); г) *актуальні інформаційні кампанії* (представлені різноманітними заходами з розвитку медіаграмотності населення: до прикладу, функціонування освітніх серіалів на порталі «Дія», у яких доступно та зрозуміло подано інформацію з тих чи тих питань із залученням громадських організацій і експертів); ґ) *динамічна глобалізація* (міжнародне співробітництво, представлене участю в низці міжнародних організацій та ініціатив з профільної проблематики й розвитком партнерських відносин з країнами, що мають високий рівень інформаційної безпеки).

1.2. Категорійно-понятійний апарат дослідження

Вищезазначена низка питань у межах аналізованої в нашій науковій роботі проблематики закономірно дає змогу позиціонувати проблему гарантування безпеки в онтологічному спектрі (цивілізаційному розвитку), у межах якого говоримо про аксіологічну детермінацію соціокультурних явищ, феноменів, яка базована на емпіричному складнику. Так, дві світові війни, припинення «холодної війни» тощо засвідчили гостроту й експоненційну диференційованість нових загроз національній та міжнародній безпеці.

Зокрема, міждержавні конфлікти, низка терористичних актів та гібридна російська-українська війна з постійною загрозою використання ядерної зброї країною-агресором, заявами про знищення The North Atlantic Treaty Organization (далі – НАТО) або України тощо становлять питому небезпеку на сьогодні [34, с. 192–198].

Прикметно, що перелік реальних і потенційних загроз національній та міжнародній безпеці ранжований у диджиталізаційному вимірі, оскільки генеза останніх більшою мірою опосередкована ним. Це, природно, уможливлює позиціонувати забезпечення національних інтересів тієї чи тієї держави комплексом дій. У межах останніх відбувається співвимірне реагування на актуальні виклики та загрози, тобто здійснення ефективної національно-безпекової політики. Насамперед така політика в її широкому витлумаченні позиціонована діяльністю суб'єктів профільних (політичних) відносин щодо гарантування національної та міжнародної безпеки.

Натомість вищезазначена діяльність має дуальну природу функціонування, а саме – внутрішньо- та зовнішньодержавний напрями. Самобутність окресленої ІБП детермінована низкою чинників (спрямованістю, методами її здійснення тощо), які корелюють з розумінням суті стрижневого поняття НБ суб'єктами ухвалення управлінських рішень. Водночас, серед внутрішньодержавних чинників окремо варто виокремити політичну участь як форму реалізації інституційної активності громадянського суспільства, що суттєво впливає на формування та легітимність рішень у сфері інформаційної безпеки. Закономірно, що на сьогодні, на нашу думку, наявна флуктуативність і навіть дифузність визначень НБ, які здебільшого витлумачені дослідниками в ширшому або вужчому ключі. У цьому контексті важливо наголосити, що політична участь є однією з ключових передумов ефективного формування національної безпеки в демократичному суспільстві. Активне залучення громадян до процесу прийняття рішень, виборів, політичного діалогу та громадського контролю забезпечує не лише вищу легітимність державної політики, але й

зміцнює її інформаційно-безпековий потенціал. Участь суспільства в політичному житті є важливим фактором протидії маніпулятивним впливам, дезінформації та зниженню довіри до інститутів влади, що особливо актуально в умовах гібридної війни Відповідно, динаміка категорійно-понятійного апарату (див. 1.2.1) нашого дослідження корелює з трансформаційними змінами цього поняття. Це продукує висвітлення його генези для найкращого розуміння специфіки, самобутності й репрезентативності щодо відповідної політики.

Отже, НБ є захищеністю всіх рівнів побутування громадянина (онтологічного, гносеологічного, аксіологічного тощо), стратифікована специфікою його соціалізації, соціального контракту та іншого, у проспекційних, ретроспекційних і потенційних координатах матеріалізації, які продукують сталість існування (наративного зокрема) тієї чи тієї країни [66]. У певному сенсі НБ може бути позиціонована сукупністю усталених поглядів, форм реалізації (кампаній, практик, стратегій тощо) щодо побутування цілей і державної стратегії в царині продукування безпекового середовища для громадян. Зокрема, мовиться про гарантування екзистенційної тяглості та онтологічної сталості суспільства і держави щодо низки загроз різної природи з урахуванням актуальних ресурсів та можливостей [16].

Також НБ витлумачують здатністю того чи того етносу до задоволення базових потреб, необхідних для самозбереження, самовідтворення і самовдосконалення з мінімізацією втрат компонентів аксіосфери останньої в актуальному стані [166, с. 35]. Окрім того, НБ позиціонується стабільністю, якій притаманна сталість протягом тривалого часу, що означає специфічну динаміку захищеності від найістотніших наявних загроз і небезпек, поєднувану зі здатністю до розпізнавання вищезазначених викликів і превентивних дій для їх нейтралізації.

Поточний стан досліджень з безпекознавства уможливлює виокремити такі складники структури НБ: а) *державну*, що є станом, за якого захищені питомі потреби й інтереси тієї чи тієї держави (тут – політичного інституту),

власне державних інституцій (державних органів): суверенітету, територіальної цілісності та подібного; б) *громадську*, яка полягає в рівні захищеності громадянина і суспільства загалом здебільшого від внутрішніх загроз (до прикладу, карантин COVID-19 та інше); в) *особисту*, що полягає у відсутності загроз для побутування громадянина: до прикладу, наявність фізичних (вода, світло, продукти харчування тощо), соціальних (відсутність ізоляції, реалізація суспільних прав) і духовних (повага, розвиток та ін.) потреб; г) *техногенну*, з функціонуванням якої пов'язують відсутність тих чи тих загроз (тут – аварій, катастроф) на об'єктах і суб'єктах, які можуть становити потенційну небезпеку: на атомних електростанціях, дамбах тощо; г) *екологічну*, яка полягає в забезпеченні гомеостазу середовища задля створення сприятливих умов для розвитку екологічних систем: захист від стихійних лих (зсувів, виверженьвулканів, землетрусів, цунамі й т. ін.); д) *економічну (фінансову)*, до якої відносять продукування стабільного і планомірного економічного зростання, розвитку ринку праці тощо: до прикладу, забезпечення робочими місцями, захист прав працівників тощо за умов воєнного стану; е) *енергетичну* – стан електроенергетики, за якого можливе задоволення поточних і перспектив запитів споживачів, а також вироблення й продаж електричної енергії; є) *інформаційну*, суть якої в тому, що інформаційне середовище тієї чи тієї країни продукує конфіденційність, доступність, цілісність, правдивість тощо даних; ж) *особисту*, що характеризується станом захищеності її життєдіяльності від актуальних, перспективних загроз [167].

Питомі концептуальні положення, покладені в основу сучасного розуміння НБ, сформульовані в Законі «Про національну безпеку США» [370]. На той час (до початку 90-х рр. XX ст.) найбільшу небезпеку становило запекле протистояння Союзу Радянських Соціалістичних Республік (далі – СРСР) і Сполучених Штатів Америки (далі – США), наслідком чого міг стати початок ядерної війни, що спричинило б невиправну шкоду для біоти нашої планети.

Закономірно, що та чи та загроза НБ певної країни продукує нарощування її обороноздатності. До прикладу, російська федерація на тлі низки успішних воєнних кампаній Збройних Сил України (далі – ЗСУ) стала використовувати іранську та корейську зброю. Низка геополітичних змін (розпад СРСР; припинення дії Варшавського договору, у який входили Албанія, Болгарія, Німецька Демократична Республіка, Польська Народна Республіка, Румунія, Радянський Союз, Угорщина й Чехословаччина; низка нерегульованих етнополітичних конфліктів у Західній Європі, Африці та інші) спродукували формування принципово нового підходу до проблеми міжнародної та національної безпеки [303]. Так, на нашу думку, продуктивним є виокремлення трьох основних теоретичних підходів до розуміння сутності НБ:

1. У межах першого основну увагу приділено *аксіологічному складнику (ціннісній парадигмі) суспільства*, серед яких варто назвати політичну автономність, економічне зростання, духовний розвиток тощо. Головними представниками цього підходу є: А. Вольферс (A. Wolfers) (у праці «Національна безпека як двозначне поняття» досліджував концепцію національної безпеки, підкреслюючи її суб'єктивний характер і залежність від сприйняття загроз. Він аналізував, як різні держави визначають та інтерпретують безпеку залежно від власних цінностей та інтересів [395], Дж. Гадді (J. Gaddy) (зосереджувався на вивченні впливу економічних факторів на національну безпеку, досліджував, як економічна політика та ресурси впливають на здатність держави гарантувати свою безпеку та стабільність) [339], Х.Д. Ласвелл (H.D. Laswell) (аналізував політичні процеси та їх вплив на національну безпеку, розглядаючи, як розподіл влади та політичні рішення впливають на здатність держави захищати свої національні інтереси) [354], J. Johnson (Дж. Джонсон) (досліджував етичні та моральні аспекти національної безпеки, зокрема, як моральні цінності й етичні норми впливають на формування політики безпеки та ухвалення рішень у цій сфері) [352], Д. Кауфманн (D. Kaufmann) (вивчав зв'язок між управлінням, корупцією та

національною безпекою, аналізуючи, як якість державного управління та рівень корупції впливають на здатність держави гарантувати безпеку та стабільність) [357], Р. Коен (R. Cohen) (досліджував роль культури та міжкультурної політичної комунікації в контексті національної безпеки, розглядав, як культурні відмінності та непорозуміння можуть призводити до конфліктів та загроз безпеці) [331], М. Міхалак (M. Michalack) (зосереджувався на аналізі міжнародних відносин та їх впливу на національну безпеку, досліджував, як глобальні політичні процеси та взаємодія між державами впливають на безпекову ситуацію окремих країн) [368] та ін. У цьому підході поняття безпеки ототожнюється не лише із захищеністю національних цінностей, культурного спадку та інших надбань, а й з безперешкодним їх поширенням [157, с. 130–135].

До прикладу, американський дослідник Г. Даєм [332] під час аналізу безпекової ситуації в США щодо динаміки генези й поширення ціннісного складника підкреслював самобутність інтеграції і подальшої експлікації західних цінностей. Так, на думку вченого, протягом американського історіогенезу традиційно відбувалося поширення переконань, цінностей і стилю життя, які мають за мету привнесення добробуту питомого для США стилю життя, управління й світогляду іншим людям. Понад те, ці наративи навіть задекларовані у Стратегії національної безпеки США [388], Зокрема, у документі зазначено, що «[…] з метою захисту нашої нації та поваги до наших цінностей, Сполучені Штати прагнуть поширити свободу у всьому світі, очолюючи міжнародні зусилля зі знищення тиранії і підтримки ефективної демократії» [7, с. 69–70].

Обґрунтувати специфічність цих поглядів можна шляхом аналізу думок Ф. Фукуями в його праці «Кінець історії та остання людина» [340] і С. Хантінгтона в дослідженні «Зіткнення цивілізацій» [347]. Так, перший стверджує про те, що ліберальні демократії не становлять загрозу одна одній, а тому війна між питомо демократичними державами фактично неможлива [340]. Щодо другого автора, то він вважає, що лінії розлому між

цивілізаціями (культурами, системами цінностей) і є лініями фронтів у майбутніх війнах [347].

Зауважимо, що такий підхід до продукування НБ через поширення аксіологічної компоненти побутування етносу, навіть за допомогою збройних сил, на нашу думку, має деструктивну природу. Так, український дослідник О. Бодрук [19] щодо цього слушно акцентує увагу на тому, що підґрунтям таких поглядів є усталені процеси розвитку західного суспільства. Серед них науковець виокремлює: ринкову економіку (світоглядна модель національної картини світу), індивідуалізм (узвичаєно актуалізовану в межах особистої безпеки громадян США та їх особистих меж тощо), розвинуту демократію (продукує самобутній підхід до політичної комунікації: зокрема, зворотного зв'язку між виборцями та кандидатами на той чи той пост).

2. Другому підходу притаманна *орієнтованість на вивчення НБ у координатах національних інтересів*. У межах означеного підходу простежуємо розширення понятійної сфери НБ. Так, вона розглядається не виключно в зоні інтересів держави, а саме щодо побутування суб'єкта (особи, громадянина) та певного суспільства загалом. Показово, що вищезазначені тези локалізовано в Законі України «Про основи національної безпеки України» [86], а сам підхід має більш універсальну, сучаснішу природу. Його представниками є низка українських та зарубіжних дослідників: В. Богданович [14], О. Бодрук [19], Г. Браун [329], С. Даниленко [57], М. Каплан[358], Г.Моргентау [369], С. Хоффман [346] та ін.

Зауважимо, що цей підхід суголосний сучасним вимогам, оскільки інтегрує у своїй структурі історичний досвід, культурний спадок та самобутність генези української політичної думки. Продуктивність орієнтованості на вивчення НБ у координатах національних інтересів детермінована деструктивністю зосередження винятково на інтересах держави: специфіці її економічного, військового та інших потенціалів. Результатом такого перекосу стає підпорядкування окресленим цілям

інтересів окремих особистостей, продукування внутрішніх конфліктів тощо, що деструктивно впливає на політичну полісистему.

Зазначені вище особливості, на жаль, досі тією чи тією мірою актуалізовані в політичній практиці, засвідчують побутування проблеми кореляцій, співвідношення інтересів громадянина й держави. Останні часто можуть мати різну функційну параметризацію і, як наслідок, просто парадоксальним чином не збігатися, що, на нашу думку, неприпустимо у демократичній державі. Водночас окреслений перекос у бік держави та її інституцій є закономірним, оскільки саме вона відіграє в системі продукування НБ системоутворюючу роль. Так, саме державні інституції й службовці формують нормативно-правову базу щодо продукування НБ. Ідеться передовсім про ухвалення рішень задля запобігання й нейтралізації загроз, виконання яких має обов'язкову природу. Окрім того, релевантною, на нашу думку, є монополія держави на актуалізацію воєнних потужностей та низки інших передбачених законами заходів примусового плану щодо продукування НБ.

3. Самобутність третього підходу полягає в *актуалізації кореляцій національних цінностей* (аксіологічний, ноосферний компоненти) *та інтересів* (онтологічний, гносеологічний компоненти) у полісистемі НБ. Такий підхід уможливив низці дослідників А. Величко, І. Волощук [22], В. Горбулін [48; 49], А. Качинський [137], В. Ліпкан [170–175], Г. Ситник [274] та ін.) позиціонувати безпеку станом, актуалізація якого передбачає відсутність загроз: зокрема, це дало можливість виокремити станом країни, за якого відсутні / усунені реальні зовнішні / внутрішні загрози її національним інтересам та характеру життя [133].

Отже, продуктивним визначенням НБ є рівень захищеності релевантних інтересів громадян, суспільства та держави від зовнішніх / внутрішніх загроз реального / потенційного плану. Насамперед така безпека диференціюється на низку видів: політичну, економічну, соціальну, демографічну, інформаційну, екологічну та воєнну. Продукування НБ передбачає підтримку відповідного

рівня стабільності соціальної полісистеми, який гарантує її подальшу генезу. Як уже йшлося, головними об'єктами НБ є громадяни (права, свободи), суспільство загалом (духовний і моральний вимір), держава (конституційний устрій, суверенітет і територіальна цілісність).

Відповідно це дає змогу локалізувати такі *чинники НБ*: а) феномен національної незалежності та суверенітету; б) неподільність територіальної цілісності держави; в) динаміку розвитку громадянського суспільства; г) актуалізовані демократичні механізми й практики, а також дієвість нормативно-правової бази щодо захищеності громадян; ґ) економічний потенціал держави, низка її соціополітичних потенцій; д) параметризація стану збройних сил: боєздатність, кількість, видове різноманіття тощо; е) детермінація національної унікальності, самобутності тощо; є) специфіка культурного спадку, світоглядних орієнтирів, виражена в національній та мовній картині світу; ж) особливості актуалізації стратегій, концепцій, програм та іншого національного розвитку, ідеї тощо, наявність загальновизнаної мети; з) відсутність атомізації суспільства: продукування соціокультурного вектора згоди та єдності громадян і територій країни; и) пов'язана з попереднім пунктом внутрішньополітична стабільність, що виявляється в готовності та здатності політичних сил до реалізації загальновизначених цілей.

Відтак НБ є мірою реального рівня прав і свобод членів того чи того співтовариства (тут – громадян), що організовані / підпорядковані певній, співвіднесеній територіально, етнічно та інше державі [277]. Щодо геополітичного фактора такої безпеки, то його продукування є пріоритетним напрямом державної політики НБ. Натомість речова, матеріалізована, конкретна природа зовнішньої політики продукує виокремлення вищезазначених поточних і перспективних загроз та небезпек і формування адекватної системи управління ними. Відзначимо, що геополітична безпека є відносно новим підходом, актуалізованим у сучасній історіографії, у якій цю

царину розглядають у призмі її складників: власне, зовнішньої та внутрішньої політики.

Геополітична безпека в такому контексті є складником НБ і полягає в управлінні її системо. У межах НБ державні та недержавні інституції витворюють умови для контролю, розподілу та іншим над наявними ресурсами (земельними, водними, повітряно-космічними тощо). Показово, що зміст такої (геополітичної) безпеки недостатньо розкритий у історіографії, що й спричинює наше звернення до питомого підґрунтя цього поняття – геополітики. Натомість окреслення самого поняття, джерел, предмета й основних законів геополітики репрезентативне щодо осягнення її категорійної самобутності і, своєю чергою, експлікації останньої до понятійної локалізації геополітичної безпеки.

При цьому необхідно, на нашу думку, усвідомлювати параметризаційні особливості генези політичної полісистеми держави. Зокрема, принципово важливим є формування тієї чи тієї політики з огляду на джерела поточних та перспективних загроз, а не усунення їхніх наслідків. Окрім того, логічно припустити, що внутрішні загрози корелюють із зовнішніми, оскільки є їх наслідками. Так, російська агресія на території України спричинила появу низку колаборантів, які ширять проросійські наративи. Якщо до початку війни це були наративи про «братський народ», то зараз, як уже зазначалося щодо нещодавньої трагедії в «Охматдиті», про «смерті», «поразку» та інше.

Таким чином, зміст геополітичної безпеки насамперед ми вбачаємо в продукуванні зовнішньої безпеки (А) разом з усуненням можливих джерел внутрішньої (Б), спродуковані А. Природно, що релевантним чинником осягнення змісту геополітичного виміру безпекового феномена є соціокультурний зміст світової цивілізації, яка в загальному розумінні є ідеальною структурою, що висвітлює найкращі щаблі інтелектуального, духовного та світоглядного розвитку того чи того етносу. Останній ранжований духовними та світоглядними змінами конкретної нації і є

питомим джерелом для наукового аналізу витоків поточних і потенційних безпекових загроз [104].

Характерно, що така категорійно-понятійна локалізація уможливлює з'ясувати стрижневі чинники, положення, практики, стратегії тощо, власне, продукування НБ, що є комплексом політичних, економічних, соціальних, безпекових (охорона здоров'я), військових і правових заходів. Останні спрямовані на продукування сталої життєдіяльності нації та усунення поточних і наявних загроз, а саме: а) захист державного і б) суспільного ладу; в) забезпечення територіальної цілісності, недоторканості й суверенітету, а також г) політичної та економічної незалежності й ґ) здоров'я нації; д) організація й проведення охорони громадського порядку; е) боротьба зі злочинністю; є) продукування умов для техногенної безпеки та ж) захист від стихійних небезпек (цунамі, землетрусів тощо).

Державними інституціями, які гарантують НБ, є воєнізовані формування: Головне управління розвідки (далі – ГУР), ДБР, ЗСУ, СБУ, правоохоронні та медичні органи [101]. При цьому проблеми НБ у наші дні набувають дедалі більшої актуальності, стаючи центром уваги більшості країн світу, міждержавних утворень і громадських об'єднань. Водночас, політична участь – як інституціоналізована, так і неформальна – виступає індикатором дієвості взаємодії між державою та суспільством у сфері формування безпекової політики, насамперед у контексті протидії інформаційним загрозам. Саме через механізми політичної участі (вибори, петиції, громадські слухання, участь у формуванні стратегій тощо) формується стійка та легітимна інформаційно-безпекова парадигма. Така пильна увага до аналізованої проблематики зумовлена експонентним зростання кількості загроз, небезпек і викликів, що мають типологічну, видову та інтегровану природу і є здебільшого актуалізованими в межах диджиталізаційних змін.

Закономірно, що продукування високорівневої захищеності національних інтересів, у межах актуалізації якого витворюють належні умови для сталого, динамічного й планомірного розвитку особистості, суспільства та

держави, є стрижневим завданням ІБП, умовою продуктивності якої виступає пріоритет несилових шляхів захисту національних інтересів (цінностей, культурної й історичної пам'яті та інших здобутків), які є підґрунтям ІБП. У такому контексті така безпека має розглядатися, на нашу думку, як інтегративне утворення, осередок тощо, у якому акумульовано всі сфери життєдіяльності суспільства, а стрижневою є інформаційна.

1.2.1. Основні підходи до визначення поняття національної безпеки

Вищезазначено складність і неоднозначність проблеми продукування НБ держави, що має стратегічну природу, у контексті актуалізації національних ідей, стратегій, планів, концепцій тощо. Природно, що широта, актуальність та інтегрованість феномена НБ впливає на категорійно-понятійну флуктуативність, дифузність тощо, виражену через спектр її витлумачень, що є основою для створення низки концепцій безпеки, актуалізованих у полісистемах ІБП різних країн. Це визначає стрижневу роль такої безпеки у формуванні тих чи тих політичних стратегій, орієнтованих на виокремлення репрезентативних інтересів нації.

Окрім того, останнє продуктивне щодо побутування (створення, наявності тощо) стратегій для подолання поточних та майбутніх загроз, а також реалізації можливостей їх усунення [57]. Водночас осягнення сутності та аналіз структурних / функційних складників полісистеми продукування НБ релевантне. Зокрема, мовиться про методологічне підґрунтя цього процесу, що, своєю чергою, продуктивне щодо виокремлення корелятивної специфіки теоретико-практичної природи аналізованої проблеми. Так, наявний історіогенез концепції НБ детермінований низкою трансформаційних змін світової політики, міжнародних відносин та диджиталізаційною динамікою. Остання репрезентативна щодо видозмін загроз (типів, видів, природи тощо), які становлять утруднення для тої чи тої країни, та різноманіття підходів до їх усунення.

Виокремимо такі історичні періоди генези НБ, які є релевантними, зокрема:

1. *Рання концепція НБ* (XIX – початок XX ст.), яка полягала у зосередженні на формальних показниках НБ: військовому захисті та територіальної цілісності держави. Таке тлумачення було актуалізоване в контексті побутування великих імперій та самобутності їх колоніальних стратегій, у межах яких превалювали зовнішні військові втручання.

2. *Період Першої та Другої світових воєн*: ці конфлікти видозмінили саме розуміння аналізованого поняття, поглибивши осягнення важливості стратегічного співробітництва, що виявилося в продукуванні низки альянсів, актуалізації промислового потенціалу та пошуку шляхів економічної стабільності як основи безпекової політики.

3. *Холодна війна*, у період якої розуміння НБ набуло комплексної природи (у нього ввійшли не лише військові, а й низка політичних, економічних, ідеологічних та інших аспектів). Визначальними щодо напрямів розвитку такої політики цього періоду закономірно були: перегони озброєнь, ідеологічне протистояння між США та СРСР.

4. *Період після холодної війни*, специфіка якого полягала у видозміні концепції НБ, яка зазнала низки змін через появу нових загроз (тероризму, регіональних конфліктів, економічних криз і викликів тощо).

5. *Період глобалізації та диджиталізаційного розвитку* суттєво трансформував розуміння сучасних викликів і загроз, екстраполювавши їх у площину інформаційних технологій (далі – ІТ): кібербезпека, гібридні війни, інформаційна безпека тощо стали стрижневими аспектами НБ [149, с. 20].

6. С*учасний період*, найпоказовішим у якому вважаємо безпекову ситуацію в нашій країни, якому притаманне нове концептуальне осмислення. Ідеться передовсім про протидію низці зовнішніх загроз, продукування внутрішньої стабільності та реформування складників безпекової політики [100].

Зазначені періоди історичного розвитку аналізованої нами концепції репрезентативніші щодо якнайкращого усвідомлення змін поглядів на поняття безпеки та розуміння детермінант, які впливали на цей процес. Насамперед тут вважаємо доцільним згадати низку теоретичних підходів, які є підґрунтям для аналізу самобутності міжнародних відносин та специфіки безпекової політики. Власне, основні теоретичні школи (реалізму, лібералізму та конструктивізму) містили різне розуміння поняття «безпека» у контексті держави. Розгляньмо їх докладніше:

а) *реалізм* – підхід, у межах якого НБ розуміють у призмі військової міці та балансу сил: так, представники цього напряму (Дж. Міршаймер [367], Г. Моргентау [369], К. Уолц [392] та ін.) позиціонували міжнародну систему анархічним осередком, що продукує збільшення вищезазначених детермінант як елементів стримування й попередження потенційних загроз [361] (до прикладу, теорія неореалізму (К. Уолц [392]) та теорія «офензивного реалізму» (Дж. Міршаймер [367]) та ін.);

б) *лібералізм*, у межах якого головне вирішення питання НБ вбачалося в міжнародному співробітництві, демократичних інститутах та економічній взаємозалежності, що позиціонувалися інструментами її продукування: прибічники цього напряму (І. Кант [356], Р. Кеохейн [360], Дж. Най [372] та ін.) вірили в можливість зменшення конфліктів і забезпечення стабільності за допомогою діяльності міжнародних організацій, правових угод та економічної інтеграції (до прикладу, ідея «вічного миру» (І. Кант [356]), теорія комплексної взаємозалежності (Р. Кеохейн [360] та Дж. Най [372]), теорія «м'якої сили» тощо);

в) *конструктивізм* – підхід, що унаочнює роль ідей, ідентичностей та норм у продукуванні НБ, який базується на суб'єктивності цього поняття (А. Вендт [394], К. Вердерлоу [172, с. 210], П. Каценштейн [359] та ін.): так, питомо воно не є об'єктивним станом, а має природу конструкта, сформованого на перетині соціальних взаємодій та дискурсів (до прикладу,

концепція ідентичності в міжнародних відносинах А. Вендт [394], К. Вердерлоу [172, с. 210], П. Каценштейн [359]).

Показово, що в контексті безпекової ситуації в нашій країні ці підходи можуть бути застосовані для вивчення різноманітних аспектів НБ. Передовсім ідеться про відповіді на виклики зовнішньої загрози, гібридної війни, кібербезпеки, внутрішньої політичної стабільності (інформаційні кампанії, пропаганда, дезінформація, мізінформація тощо рф). Характерно, що НБ є складною, когезійною тощо полісистемою, яка перебуває в постійному розвитку. Природа такої полісистеми інтегрована, оскільки в неї входять різні підсистеми та релевантні взаємозв'язки (усередині і ззовні останньої), що утворюють самобутнє мереживо цього конструкта. Питомими параметризаційними особливостями окресленої полісистеми є відповідна структурна цілісність, системна єдність, які мають функційну спрямованість. При цьому кожен її елемент має відносну атомізованість, що «продуковане виконання ним необхідних функцій щодо її онтологічної протяжності загалом» [164, с. 206].

Ці характеристики спричиняють формування й розвиток НБ як динамічної, відкритої, адаптивної тощо полісистеми. Водночас кореляції між складниками такої полісистеми, самобутність її побутування в певному соціокультурному середовищі продукують новий рівень якості. Це дає змогу такому утворенню ефективно розв'язувати завдання продукування НБ: відповідна структурна, композиційна, функційна його природа спричиняє набуття цілісності, що необхідно для ефективного функціонування полісистеми загалом. Прикметно, що така полісистема має атомізованість, яка призводить до функційної продуктивності загальних завдань усієї структури: це стрижнева детермінанта забезпечення її сталого функціонування та високої ефективності [389].

Зокрема, у праці О. Гончаренка, Є. Лисицина[46] відстежено трансформаційні зміни поняття НБ: за словами авторів, первинно воно мало абстраговану природу, набувши практичного витлумачення в сучасних

адміністративних практиках. Також на сьогодні актуалізовано кількісні методики її стану, за якими НБ оцінюють тією чи тією чисельною величиною. Водночас вона належить відрізку від 0 (найнижчий / найгірший рівень її стану) до 1 (відповідно, найвищий / найкращий), це суголосно розгляду концепції НБ у вимірювальному ключі ступенем (мірою, рівнем тощо). Наслідком такого підходу є захищеність життєво важливих інтересів, прав, свобод та іншого громадянина, суспільства і держави від низки внутрішніх / зовнішніх загроз) та її стратифікація в спектральному вимірі: оцінка відповідності правам, свободам, інтересам, цінностям громадян, суспільства і держави [275].

Праця С. Даниленка [57] унаочнює інший погляд на аналізоване поняття, витлумачуючи його станом захищеності життєво важливих інтересів особистості, суспільства і держави та людства загалом від зовнішніх / внутрішніх загроз. Прикметно, що саме таке визначення вважають класичним, адже саме воно було актуалізовано в нормативно-правовій базі України, а саме – Законі України «Про основи національної безпеки України» [95]. Зауважмо, що проведений автором аналіз історіографії уможливив нам локалізувати генезу підходів до визначення поняття НБ.

Так, концепція «стану захищеності», актуалізована в процесі витлумачення поняття «національна безпека», набула значного поширення. Дедалі більше дослідників акцентують увагу на тому, що таке визначення є застарілим. Це пов’язано з тим, що воно детерміноване часом, коли «безпеку» пов’язували з протяжністю існування (наявністю) низки показників та градацією їх стану. При цьому такий стан здобував чітке визначення й здебільшого був незмінним, натомість будь-яке відхилення продукувало новий сталий стан.

Ми погоджуємося з думкою згаданих науковців: адже таке тлумачення репрезентує безпекову парадигму, що була актуалізована в радянські часи, коли пріоритет надавали захисту, а не попередженню тих чи тих загроз. Окрім того, на сьогодні локалізований розгляд певного аспекту (у цьому випадку – захисту) позиціонують неповним, що аргументовано таким важливим

складником аналізованого поняття, як превентивні заходи (звуження, послаблення, усунення та попередження небезпек і загроз), що було висвітлено в праці В. Ярочкіним [211, с. 304].

Прикметно, що нещодавно загрози позиціонувалися атрибутом онтології будь-якого предмета (об'єкта), проте розуміння їх параметризаційних особливостей розвивалося. Наслідком цього процесу стало те, що сучасна безпекова концепція полягає у випереджувальній діяльності щодо тих чи тих загроз. Наслідком цього стає мінімізація негативного впливу на функціонування та життєдіяльність об'єктів продукування безпеки. Це дало змогу низці вчених (до прикладу, В. Ліпкан [174]) вийти за межі споглядання загроз як іманентних небезпек, акцентувавши увагу на їх творчо-конструктивній ролі в розвитку об'єкта.

Такий підхід співзвучний із сучасним розумінням безпекознавства як інтегрованої, міжпредметної тощо науки, що репрезентовано розмаїттям її підходів до різноманітних проблем НБ. Останнє увиразнено низкою підходів до її визначення, яскраво представлене в праці О. Корнієвського [154], де автор глибоко аналізує поняття «національна безпека». Науковець витлумачує його здатністю країни до збереження цілісності (неподільності), суверенітету, політичних, економічних, соціальних та інших основ суспільного життя. Дослідник визначає країну як самостійний суб'єкт міжнародних відносин, підкреслюючи необхідність збереження цього стрижневого підґрунтя.

Доповнене розуміння аналізованого поняття в праці О. Сосніна [278], у якій автор надає три релевантні визначення поняттю НБ, під яким він розуміє безпеку а) етносу (нації), так і космополітичного (багатонаціонального) загалу; б) суспільства, у межах якого відбувається об'єднання людей, що проживають на одній території під впливом соціокультурних чинників; в) держави, що є організаційно-правовою формою об'єднання народів і націй для спільних справ.

Кожне з визначень поняття НБ додає семантичних відтінків для його універсалізованого осягнення: мовиться про самобутні аспекти розуміння НБ.

Так, показовим вважаємо політологічний контекст, пропонований у праці В. Храмова, де НБ позиціоновано якісним станом кореляції громадян, суспільства, держави і природи. Продуктивність наведеного визначення, на нашу думку, в акцентуванні на гармонійному зворотному зв'язку та оптимальних умовах існування цієї системи. Такий підхід дозволяє не лише оцінити безпеку як стан захищеності, а й як динамічний процес взаємодії між різними елементами соціуму й середовища. У цьому контексті національна безпека постає не лише результатом владних рішень чи інституційних стратегій, а й відображенням збалансованості між правами громадян, інтересами держави та викликами зовнішнього середовища. Таким чином, її сутність значно глибша за формальні механізми захисту — вона полягає у забезпеченні умов сталого розвитку, внутрішньої стабільності та соціальної довіри, які разом формують основу для успішного функціонування держави у мінливому глобальному контексті[107, с. 176–178].

Продуктивним і значущим також вважаємо трактування аналізованого поняття В. Храмова [107], який виокремлює дві групи детермінант, що визначають стан національної безпеки: а) *воєнні* (готовність збройних сил та їх поточний стан; потенційні зони військових конфліктів; наявність резервів і здатність до мобілізації (стан мобілізаційного ресурсу); участь у військово-політичних об'єднаннях (альянсах, організаціях тощо, союзах); професіоналізм особового складу; витрати на оборону та вміст воєнної доктрини); б) *природні* та *економічні* (геополітичне положення і геостратегічна інфраструктура; соціальні аспекти, зокрема й економічний рівень населення; демографічні та етнічні характеристики; рівень суспільної дисципліни, правопорядку та стійкості; стан інформаційної безпеки країни; людський потенціал).

Такий підхід продуктивний щодо розгляду НБ як комплексного об'єкта, що актуалізує не тільки воєнний складник змісту, а й різноманітні соціальні й економічні складники. Отже, аналіз окреслених аспектів гармонізує інтереси громадян, суспільства та держави в контексті НБ [107], яка є багаторівневим

поняттям, що охоплює різні детермінанти, кожна з яких є репрезентативною щодо продукування стабільності та добробуту держави.

Ключовими вимірами НБ є: а) *військова* (включає здатність держави захищати свою територію та суверенітет від зовнішніх та внутрішніх загроз, підтримувати ефективні та добре оснащені збройні сили, а також стримувати потенційних агресорів); б) *політична* (пов'язана зі сталістю політичної системи, захисту від внутрішніх та зовнішніх загроз, а також ефективним управлінням країною: демократичні інституції, правова держава та прозорість урядування є ключовими елементами політичної безпеки); в) *економічна* (детермінована продукуванням економічної стабільності, зростання та розвитку, також включає захист від економічних криз, забезпечення енергетичної незалежності та розробку стратегій для протидії глобальним економічним викликам); г) *соціальна* (знаменує продукування соціальної стабільності, рівності та справедливості, до неї входить охорона здоров'я, освіта, соціальний захист тощо); ґ) *екологічна* (здатність захищати своє природне середовище, управляти природними ресурсами та протидіяти екологічним загрозам); д) *інформаційна* (у неї входить захист від кібератак, боротьба з мізінформацією, дезінформацією, захист ІС) (див. Рис. 1):

Рис. 1 Виміри НБ [218]

Відзначимо, що ці виміри корелюють один з одним (оскільки взаємопов'язані, взаємозалежні), що спричиняє потребу в їх комплексному розумінні для випрацювання ґрунтовної стратегії НБ будь-якої держави. Показовим у цьому плані є визначення, уміщене у «Політичній енциклопедії», де «НБ позиціонується здатністю країни підтримувати свою цілісність, суверенітет, а також зберігати стабільність у політичній, економічній, соціальній сферах та інших аспектах громадського життя, дозволяючи їй виступати як незалежний учасник міжнародних відносин» [226].

Це визначення не є вичерпним і єдиним: існує чимало різних підходів до тлумачення поняття НБ, яка, до всього, є юридичною категорією, що продукує фіксацію такого визначення в нормативно-правовій базі (конституції, законах,

указах, постановах, рішеннях тощо) нашої та інших країн і міжнародних організацій. У цьому контексті стрижневим вважаємо Закон України «Про національну безпеку України» [98], який визначає НБ як захищеність життєво важливих інтересів особи, суспільства та держави від внутрішніх / зовнішніх загроз. Цей нормативно-правовий документ охоплює різні сфери, включаючи воєнну, економічну, політичну, соціальну, екологічну, інформаційну та кібербезпеку.

Визначальною також є Конституція України [150], яка містить низку положень, що стосуються НБ (зокрема, гарантування прав і свобод громадян, забезпечення суверенітету та територіальної цілісності країни). Окрім того, доцільно згадати низку стратегічних документів (зокрема, Стратегію національної безпеки [244] тощо), які репрезентативні щодо основних напрямів безпекової політики, актуалізованих у контексті сучасних викликів та загроз. Також вагомими в контексті нашого дослідження є Закони України: «Про оборону» [100], «Про Службу безпеки України», «Про боротьбу з тероризмом» [246], «Про основні засади забезпечення кібербезпеки України» [240] тощо.

Ця нормативно-правова база є підґрунтям для діяльності державних органів у царині НБ, що пов’язано з їх визначальною щодо повноважень таких органів роллю, а також актуалізацією механізмів реагування на різноманітні загрози. Окрім того, зазначені документи акумулюють у своїй структурі низку принципів, завдань і механізмів продукування НБ, ураховуючи наявні здобутки в цій царині [160, с. 83–90].

Легіслативний підхід до феномена НБ в Україні має своїм підґрунтям Декларацію про державний суверенітет України [58]. Зауважмо, що остання була першим документом, у якому закріплювалися базові принципи окресленої галузі, після неї доцільно згадати Закон України «Про національну безпеку» [58], у якому докладно прописано НБ. Зокрема, у нормативно-правовому документі її позиціонують як гарантування державного суверенітету, збереження територіальної цілісності, захист демократичного

конституційного устрою країни, а також інших релевантних національних інтересів від будь-яких реальних чи потенційних загроз.

Тут підкреслимо важливість аналізу нормативно-правових документів України щодо НБ, що засвідчує потребу в комплексному вивченні цього феномена. При цьому особливу увагу доцільно звернути на структурні кореляції аналізованого поняття, зокрема взаємозв'язок між його зовнішніми / внутрішніми аспектами, висвітлений у нормативно-правовій базі. Це продукує висновок про те, що Закони України щодо НБ не лише визначальні щодо її структури й принципів діяльності відповідних органів влади, а й акцентують увагу на потребі адаптування до змінюваних глобальних / регіональних умов.

Окрім того, необхідно врахувати самобутність реагування України на низку сучасних викликів (кіберзагрози, гібридну та інформаційну війну). У контексті динаміки якого висновуємо, що НБ не обмежується лише традиційними воєнними чи політичними аспектами, а охоплює інші важливі царини (згадані кібер- та інформаційну безпеку). Це дає підстави стверджувати відповідність динаміки розвитку НБ в Україні експоненційному розвитку викликів сучасного світу (зокрема диджиталізаційної природи), що увиразнює специфіку (стратегічність, прогностичність, адаптивність, гнучкість тощо) української державної політики у безпековій сфері.

Сучасна українська історіографія засвідчує зростання інтересу до феномена НБ та її складників. На нашу думку, цей інтерес почав експоненційно зростати після ухвалення та затвердження стрижневих нормативно-правових документів і започаткування нових наукових установ. Такий інтерес можна пояснити певними детермінантами, як-от:

а) посиленням академічного фокусу на феномені НБ на тлі *змінності геополітичних умов* (зокрема, подій, що сталися в нашій країни протягом останнього десятиліття: анексія Криму, російсько-українська війна тощо);

б) *потребами в розробці інноваційних теоретико-практичних підходів і стратегій* тощо, які були б дієвими за сучасних умов: учені аналізують і

пропонують рішення для широкого спектра загроз (зокрема, кібербезпеки, інформаційної та гібридної війни, економічних і соціальних викликів);

в) глобалізаційними та євроінтеграційними тенденціями сучасної української науки, що продукують *генерування низки міждисциплінарних досліджень у інноваційних наукових установах та дослідницьких центрах* (такі організації не лише здійснюють ґрунтовні дослідження, а й провадять аналітичну діяльність, спрямовану на підтримку розробки політики та стратегічного планування);

г) такий інтерес до НБ у науковій спільноті репрезентативний щодо *глобальної тенденції до інтегрованості безпекових питань у парадигму сучасних досліджень* (зокрема, політології, міжнародних відносин, соціальних наук тощо), які є продуктивні щодо розробки фундаментальних, ефективних і наукоємних стратегій НБ, що враховують різноманітність форм, типів тощо загроз і викликів [141, с. 45–51].

Зростання інтересу до феномена НБ в Україні закономірно стимульоване потребою в продукуванні нового покоління експертів, аналітиків та фахівців у цій галузі. Так, ЗВО та дослідні інститути (до прикладу, НАН України) формують спеціалізовані програми та курси, основна мета яких – деталізоване вивчення детермінант НБ та міжнародної безпеки (далі – МБ). Це зумовлює появу фахівців, здатних аналізувати поточну ситуацію в її динаміці, прогнозувати та пропонувати варіанти реакцій на змінні геополітичні події та безпекові виклики.

Окрім того, простежуємо посилення зворотного зв’язку, динамізацію співпраці між державним (державні інституції) і науковим (навчальні, наукові, науково-дослідні установи) секторами. Природно, що окреслена взаємодія продукує краще розуміння практичних потреб у царині НБ та інтенсифікацію випрацювання ефективних політичних рішень. Водночас така співпраця спричиняє виформовування механізму взаємодії між державними інституціями й представниками наукової спільноти, даючи змогу науковцям впливати на формування різноманітних політичних рішень.

Серед важливих детермінант назвемо міжнародне співробітництво в царині дослідження НБ: так, українські дослідники, експерти та інші фахівці співпрацюють із зарубіжними колегами. При цьому українські вчені беруть активну участь у низці міжнародних заходів (конференцій, круглих столів, симпозіумів тощо) та обмінюються досвідом і знаннями з колегами. Це продукує екстраполяцію українських досліджень у ширший (міжнародний) контекст, роблячи їх актуальними, суголосними часу: у них використовують найкращі світові практики аналізу й розвитку тих чи тих стратегій, кампаній та ін. Водночас це доводить, що наукові розвідки у сфері НБ України набувають дедалі більшої значущості й ваги, що висвітлено в кількісному (і якісному) зростанні українських досліджень.

При цьому саме поняття НБ має, як уже зазначалося, інтегровану, диференційовану й поліпредметну природу, що, закономірно, формально представлено в його багатовимірності й поліаспектності. Різниця між останніми, своєю чергою, не лише змістова, а й галузева (мовиться про предметну приналежність того чи того виміру та продуктивність дослідження і ньому). Відтак фундаментальне дослідження феномена НБ включає в себе спектр можливих (інколи суперечливих відносно одна одної) точок зору, які, корелюючи одна з одною, продукують комплексне розуміння побутування поняття НБ [221].

Отже, ґрунтуючись на актуалізованих визначеннях та історично-концептуальних підходах до поняття НБ, вважаємо доцільним подати власну дефініцію цього стрижневого для нашої роботи поняття. На нашу думку, НБ є багаторівневим концептом, що охоплює комплекс життєво важливих інтересів громадянина, суспільства та держави від внутрішніх / зовнішніх загроз. При цьому НБ є комплексною полісистемою, функціонування якої вимагає скоординованого підходу у вищезазначених царинах, а також гнучкого, оперативного, динамічного тощо реагування на поточні реалії, виклики та загрози. До цієї полісистеми входить не лише реагування на наявні загрози й виклики, а й стратегічне планування, метою якого є випередження таких

проблем і превентивне їх подолання. Це має спродукувати тривалу стабільність, добробут та гармонію існування держави.

1.2.2. Співвідношення понять національної та інформаційної безпеки

Вищезазначене закономірно підводить нас до такої проблеми категорійно-понятійного апарату дослідження, як співвідношення понять НБ та інформаційної безпеки (далі – ІФ), суть якої полягає в тому, що низка дослідників Д. Біленець, В. Веселий, В. Марчук, С. Дерев'янко та ін. виокремлюють чимало складників, що є стрижневими щодо дефініції НБ. Так, у колективній монографії «Національна безпека України в реаліях масштабної військової агресії» за авторства Д. Біленець, В. Веселого, К. Возняковської, О. Волощук, Т. Демчук, Т. Латковської, В. Марчука, І. Глиняного та І. Факаса [11] докладно проаналізовано сучасні виклики, що постали перед Україною в умовах масштабної військової агресії. У праці розглянуто питання зміцнення обороноздатності, гарантування інформаційної безпеки, економічної стійкості та міжнародної співпраці. Автори пропонують комплексні підходи та рекомендації щодо посилення національної безпеки України, ураховуючи реалії та загрози, з якими стикається держава. Характерно, що стрижневим складником НБ є інформаційний, який, своєю чергою, продукує дискусії щодо його приналежності до НБ. Зважаючи на її неподільність, цілісність та кореляційність, постає питання можливості атомізації такого її складника, як самостійної / залежної детермінанти НБ.

На нашу думку, відповідь доцільно узвичаєно шукати в окресленій нормативно-правовій базі: у ст. 17 Конституції України [150] зазначено, що захист суверенітету та територіальної цілісності України, гарантування її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу. У Законі України «Про основи

національної безпеки України» [100] окреслено основні сфери НБ, серед яких виокремлюється й інформаційна.

У концептуальному плані вважається, що НБ є цілісним екзистенційним феноменом, а відтак не може бути репрезентована сукупністю корелятивних складників (економічного, інформаційного, політичного та ін.). Водночас НБ доцільно аналізувати крізь призму її системної параметризації (властивостей), що дає підстави говорити про неї в інформаційній, екологічній тощо царині. Продуктивність оперування цими підкатегоріями полягає у відсутності впливу на цілісну полісистему НБ: поява вищезазначених «складників» ніяк не вплине на її суть.

У випадку дослідження НБ у різних сферах життєдіяльності їх використання буде мати позитивну динаміку, оскільки вони допоможуть деталізувати, фундаменталізувати аналіз, що проводиться. При цьому сама полісистема лише виявиться через низку нових форм, що репрезентують її локальні прояви або властивості. Таке параметризаційне різноманіття тільки покращить її вивчення, даючи змогу вибудувати мереживо внутрішніх (логічних та інших) взаємозв'язків [9, с. 7–9].

Отже, питома сутність окреслених елементів, актуалізованих у межах націобезпекового дискурсу (середовища), виявиться через їхній корелятивний зв'язок, що, власне, і витворює полісистему НБ. Вважаємо: саме у цій особливості й полягає хибність вектора сучасної історіографії. Мовиться про те, що більшість наукових досліджень феномена НБ не актуалізують евристичний потенціал націобезпекового підходу. Його ми викладемо в стрижневих тезах нашого бачення цієї проблеми та продуктивності його використання:

1. Національні інтереси (далі – НІ), загрози для них, а також управління такими загрозами в усій полісистемі НБ матеріалізовані за посередництва концептів інформації та інформаційної царини.

2. Громадянин і його права, інформація (дані) та інформаційні системи й права на них є основними детермінантами не лише НБ в інформаційній сфері, а й ключовими складниками всіх безпекових об’єктів будь-якої сфери.

3. Розв’язання завдання НБ детерміноване динамікою актуалізації інформаційного підходу як стрижневого складника науково-практичного методу.

4. Феномен НБ має яскраво виражене інформаційне підґрунтя, що пов’язано з її зумовленістю специфікою побутування даних у політичному (і не тільки) дискурсі.

5. Нерівномірний розвиток вищезазначених вимірів НБ (зокрема, інформаційного) спричиняє неможливість продукування ІБ.

6. Інформаційний складник є питомим для людської онтології: відповідно він притаманний будь-якій сфері життєдіяльності громадян, суспільства й держави [16; 74; 48].

Відтак ІБ є одним з найрелевантніших понять наукової та інших парадигм людської діяльності. Це, зокрема, пов’язано з її зумовленістю аксіологічним спектром (ідеться про її ціннісну природу щодо явищ довільної природи). Сутність, комплексна й багаторівнева природа ІБ виявляється через особливу динаміку функціонування сучасного інформаційного суспільства. Аналіз низки підходів до визначення ІБ уможливлює стверджувати про потенційну відкритість його категорійно-понятійної природи. Так, у межах сучасного розвитку політологічного вчення доцільно розглядати інформаційне суспільство фундаментальніше й системніше, акумулюючи нові дані про його побутування, не обмежуючи категорійною локалізацією.

Вищезазначене позначене актуалізацією визначення ІБ у межах інтегрального підходу, за якого вона визначатиметься за допомогою локалізації її найрелевантніших сутнісних ознак. Вони актуалізовані з урахуванням сталої динаміки інформаційних систем і трансформаційних змін не лише інформаційного суспільства, а й інформаційного, антропологічно зумовленого культурного цивілізаційного спадку. Такий підхід, продукований

у межах сучасної гуманітарної парадигми, дає підстави стверджувати про неможливість аналізу ІБ атомізовано – як перехідного або відокремленого стану НБ, оскільки він зумовлений соціополігенезом політичних стратегій тощо.

Такий особливий стан інформаційного складника (даних) є питомою параметризаційною специфікою (властивістю, атрибутом) сучасного інформаційного суспільства, яке розгортається в контексті діяльності громадян і її результату, спрямованого на забезпечення того чи того рівня безпеки в інформаційній царині. При цьому ІБ є зумовленою не лише минулим і поточним, а й майбутнім (генезою, можливими виявами тощо) станом побутування даних, що дає змогу говорити про її процесуальну природу. Відтак її доцільно розглядати в контексті особливого роду поєднання певних ознак: стану, властивостей, а також управління загрозами і небезпеками. Для останнього властивим є забезпечення обрання оптимального шляху їх усунення і мінімізації впливу негативних наслідків. Це, зрештою, за своїм змістом і становить діяльність зі створення сприятливих умов для реалізації інтересів об’єкта [52, с. 9–18].

Таким чином, ІБ за своєю суттю є ширшою, ніж захист інформації, певний концепт тощо, оскільки це контекстуальне утворення. ІБ є багаторівневою, поліінтерпретаційною цариною діяльності, усвідомлення суті якої можливе за умови використання системно-комплексного підходу [162, с. 425]. Її дослідження має виходити із засад філософії науки, ноосфери та низки інших філософських наук, що продуковане сутністю як внутрішнього змісту предмета, що репрезентований за посередництва сталої єдності всієї низки багатошарових, змінних, суперечливих тощо форм онтології. При цьому базовою характеристикою ІБ варто позиціонувати ймовірність появи підвищеного ризику реалізації тієї чи тієї загрози / виклику / небезпеки для громадянина, суспільства та держави.

Прикметно, що стрижневим критерієм ефективного її продукування є високий ступінь безпеки з мінімумом витрат [294], що, своєю чергою,

уможливлює стверджувати про самобутність структури поняття ІБ. Так, її релевантними складниками виступають життєво важливі потреби (інтереси) представників тієї чи тієї соціальної полісистеми, які мають бути співвідносні із зовнішніми чинникам (інтересами наднаціональних, національно-державних тощо структур) у межах міжнародного співробітництва. Характерно, що зсередини національно-державного утворення його вищезазначені інтереси активно взаємодіють з інтересами складників останнього. Такими складниками є соціальні групи, еліта, організації, партії, кандидати, релігійні й етнічні утворення, рухи тощо. Натомість сукупність внутрішніх і зовнішніх інформаційних загроз виформовує передумови для порушення безпечного функціонування системи державного управління [153, с. 384].

У такому сенсі ІБ є характеристикою стійкого стану системи державного управління, яка під впливом зовнішніх / внутрішніх загроз, викликів або небезпек зберігає релевантні параметризаційні особливості для власного існування. Отже, вона, будучи характеристикою сталого розвитку, виступає базовою цінністю держави, водночас низка ціннісних орієнтацій, базованих на певних уявленнях представників соціальних груп та іншого, зазвичай не тотожні. Саме в цій рисі ми вбачаємо безпосередній репрезентант впливу держави як актора, що за допомогою різноманітної методології матеріалізує аксіосферу (громадян, суспільства) в інформаційній царині [214, с. 65–68]. До прикладу, у випадку з рф ми говоримо про маніпулятивні стратегії такої реалізації, які виформовані урядом у населення й несуть ідею «руського міра».

Повертаючись безпосередньо до співвідношення понять НБ та ІБ, зазначаємо, що *перша* (НБ) актуалізує широкий спектр заходів і стратегій. Метою ІБ є продукування стабільності, цілісності, наступності розвитку держави. Окрім того, до НБ входить оборона від воєнних загроз (вторгнення, тероризму), продукування економічної сталості та інші зазначені вище віхи. Також у її межах актуалізовано низку аспектів, пов’язаних із зовнішньою

політикою, оборонною стратегією і внутрішньою сталістю і (як наслідком) добробутом.

Натомість *друга* (ІБ) зосереджена на захисті інформаційного середовища держави. У нього входить не тільки технічний (апаратний) захист, удосконалення інформаційно-телекомунікаційних систем тощо, а й протистояння інформаційним кампаніям, мізінформації, дезінформації, пропаганді [333], що в цьому контексті є формами, типами, видами гібридної й інформаційної війни, а метою – підрив державного суверенітету, маніпулювання свідомістю тощо. До ІБ входить також політична полісистема, механізми захисту персональних даних громадян і гарантування їх конфіденційності в цифровому світі.

Отже, співвідношення НБ та ІБ детерміноване корелятивною природою їх побутування. Так, продукування ІБ є невід'ємним елементом НБ, оскільки захист національних інтересів у наші дні більшою мірою формується політикою щодо інформаційних небезпек / загроз / викликів. Такий пріоритет пов'язаний з тим, що вони мають співвимірні руйнівні наслідки для національної цілісності, суверенітету та іншого, підриваючи економічну, безпекову, соціальну стабільності всередині країни, що уможливлює прирівняти їх результати до узвичаєних терористичних чи воєнних атак [99; 269, с. 68–72].

Під цим кутом показовими є низка кореляцій між НБ та ІБ, які стратифіковано в таких стрижневих аспектах як-от:

а) *сутність інформації як концепту*: мовиться про ту важливу роль, яку дані відіграють на сьогодні, що закономірно продукує потребу їх захисту як репрезентанту безпекової політики щодо національних інтересів (ідеться про злами, кібератаки, а також цілеспрямовані дезінформаційні та інші кампанії, що підривають довіру до державних інституцій, впливають на політичні рішення, завдають шкоди економіці тощо);

б) *безпосередній вплив інформаційних загроз на оборону країни:* ідеться про те, що кібератаки на воєнні об'єкти або об'єкти критичної інфраструктури

продукують значне ураження здатності держави відповідати на зовнішні / внутрішні загрози;

в) *релевантна роль ІБ у добробуті країни* (зокрема, захисті персональних даних, забезпеченні їх конфіденційності тощо): базова категорія в контексті підтримки довіри громадян до державних інституцій та надання їм цифрових послуг [185] (до прикладу, у межах актуалізованої нашим урядом концепції «Держава у смартфоні»).

Відтак ІБ є стратегічним складником НБ, продукуючи стабільність побутування, неперервність державного управління, повноту надання цифрових послуг тощо. Зазначені віхи зумовлюють комплексний підхід, у який входять не лише технічні заходи безпеки, низка законодавчих ініціатив, а й широкий спектр міжнародної співпраці. У процесі зіставлення поняття ІБ та НБ підкреслимо стрижневу роль інформаційних загроз, вид, тип та інше яких виформовують специфіку побудови НБ у конкретній країні. Так, спрямовані на державні інституції (СБУ, ДБР тощо), фінансові установи (ОщадБанк, ПриватБанк та інші), об’єкти критичної інфраструктури тощо кібер- та інші атаки можуть завдати значної шкоди: збитків, порушити надання життєво важливих послуг, спричинюючи таким чином хаос і паніку.

Не менш впливовими є мізінформація, дезінформація та пропаганда [333], що є потужними інструментами, використовуваними для маніпулювання громадською думкою, актуалізацією недовіри до влади тощо. Такі інструменти є особливо продуктивними в контексті впливу на виборчі процеси й активно використовуються рф у нашій країні задля спричинення внутрішнього розколу українського суспільства. Зокрема, мовиться про кібершпигунство, що включає збирання конфіденційної інформації з політичною, воєнною та іншою метою. Це може загрожувати НБ та ІБ, продукуючи здатність впливу зовнішніх акторів на державне управління та низку інших стратегічних процесів України.

Небезпечними для нашої країни в цьому контексті є й численні інформаційні кампанії рф, спрямовані на поширення неправдивих даних, що

дестабілізують ситуацію в Україні, створюють соціальне напруження й підривають авторитет влади [75]. Таким чином, окреслений тип загроз потребує комплексного, фундаментального та інших підходу до його розв'язання із застосуванням диджиталізаційного складника. Окрім того, корелює з успіхом згаданих деструктивних напрямів рівень медіаграмотності українського населення, який дає змогу протидіяти мізінформаційним, дезінформаційним і пропагандистським впливам ворога.

Це закономірно підводить нас до думки про релевантність захисту інформаційної сфери як важливого елемента НБ. Позаяк інформаційні (зокрема телекомунікаційні) системи, мережі та інше стали невід'ємною частиною сучасної військової та оборонної інфраструктури, що виокремлюється в низці складників: *захисті критичної інфраструктури*: енергетичних мереж, транспортних систем, фінансових установ тощо (до прикладу, мережа Центрів надання адміністративних послуг (далі – ЦНАП) належить до критичної інфраструктури, оскільки збирає для надання тих чи тих послуг дані про громадян і є місцем скупчення людей); *захисті урядових систем політичної комунікації*: мовиться про інформаційно-телекомунікаційні системи державних інституцій (до прикладу, центральних органів виконавчої влади (далі – ЦОВВ)[306]; *захисті цілісності й непорушності державних даних*: ідеться про забезпечення стабільного побутування даних, що можуть мати стратегічну або управлінську значущість (до прикладу, Реєстр державних сертифікатів (далі – РДС) на володіння державною мовою Національної комісії зі стандартів державної мови (далі – НКСДМ) є таким типом даних, оскільки наявність відповідного сертифіката є стрижневою умовою здобуття посад державної служби); *захисті воєнної ІБ*: передовсім мовиться про мережу воєнних та політичних комунікацій, систем управління, баз даних тощо (до прикладу, система «Оберіг», яка містить особисту інформацію про всіх військовозобов'язаних громадян України, є стратегічним об'єктом); *захисті від неправдивих даних* (мізінформації, дезінформації пропаганди рф [334]): ідеться про попередження, вилучення,

спростування та інше такого типу даних (до прикладу, Центр протидії дезінформації (далі – ЦПД), що здійснює фактчекінгові операції й виконує вищезазначені функції) [20].

Відтак інформаційна царина є пріоритетною в контексті НБ, оскільки вона включає не лише важливі ресурсоємні потужності, а й забезпечує інтенсифікацію обороноздатності країни. Таким чином, продукування, актуалізація, реформування тощо комплексних стратегій ІБ є релевантною щодо функціонування й розвитку національного оборонного комплексу [111; 296]. Натомість роль державних інституцій і чинників, що впливають на визначення національної доктрини НБ та стратегії продукування ІБ, є визначальною та вирішальною, охоплює такі аспекти: а) *розробка політичних стратегій, кампаній, механізмів тощо та вдосконалення* ІБ і генеза її нормативно-правової бази (визначення стандартів захисту даних, правил кібербезпеки і механізмів реагування на інформаційні загрози); б) *контроль дотримання вищезазначеного курсу, нагляд над функціонуванням нормативно-правової бази* (моніторинг та оцінка ефективності актуалізованих урядовими структурами, приватним сектором і громадськістю заходів безпеки); в) *координація дій акторів, що відповідають за НБ та ІБ*, що продукує єдину, цілісну, продуману й актуальну політику реакцій на поточні та можливі загрози / виклики / небезпеки, а також сприяє обміну досвідом, даними і ресурсами); г) *розвиток міжнародної співпраці*: ідеться про активну підтримку урядом глобалізаційних безпекових ініціатив (міжнародні угоди, організації, партнерства тощо, які мають за мету обопільну підтримку й обмін знаннями і досвідом); ґ) *продукування низки освітніх і просвітницьких ініціатив*: уже згадані освітні серіали на порталі «Дія» покликані поглибити навички медіаграмотності співвітчизників (інформаційні кампанії, навчальні програми та інші ініціативи, спрямовані на зміцнення суспільної усвідомленості щодо цифрових загроз / викликів / небезпек та алгоритмів їхній протидії) [139].

Роль уряду, його змістових засадах, регулюванні й виконанні політики ІБ є стрижневою щодо продукування НБ. Це зазвичай відбувається шляхом імплементації вищезазначених заходів у загальну стратегію НБ, яка гарантує стійкість країни до низки різноманітних інформаційних загроз. Зокрема, міжнародний вимір НБ та ІБ України, особливо в контексті російсько-української війни, набуває неабиякої значущості. Мовиться передовсім про взаємодію з міжнародним співтовариством, яка відіграє ключову роль у продукуванні безпеки та стабільності, а також у протидії зовнішнім / внутрішнім загрозам.

Участь у таких міжнародних ініціативах (наша країна активно бере участь у таких заходах, спрямованих на зміцнення кібербезпеки та боротьбу з мізінформацією, дезінформацією і пропагандою) включає взаємодію у межах програм НАТО, Європейського Союзу (далі – ЄС), Організації з безпеки і співробітництва у Європі (далі – ОБСЄ) та інших міжнародних утворень, організацій, платформ тощо. Окрім того, такі ініціативи передбачають ратифікацію нормативно-правових документів: угод, договорів і под. Україна ратифікувала низку міжнародних документів (Європейська конвенція про кіберзлочинність (Будапештська конвенція); угода про співпрацю у сфері кібербезпеки між Україною та НАТО; стратегія кібербезпеки України; стратегія інформаційної безпеки України; план реалізації стратегії кібербезпеки України), які стосуються кібербезпеки та захисту інформаційної інфраструктури.

Отже, цей інформаційний вектор безпекової політики України сприяє синхронізації її нормативно-правової бази з міжнародними стандартами та забезпечує підтримку в боротьбі з транснаціональними кіберзагрозами. Прикметно, що інтенсивна співпраця із зарубіжними країнами (зокрема, білатеральні та мультилатеральні відносини) продукують обмін інформацією, розвідувальними даними та досвідом у царині кібербезпеки. Також міжнародне співробітництво інтенсифікує випрацювання спільних стратегій протидії вищезазначеним загрозам / викликам / небезпекам та підтримку

безпекових ініціатив, що в контексті російсько-української війни є критично важливо, адже зазвичай включає технічну допомогу (озброєння), навчання (згадаймо навчання українських захисників у Англії), фінансову підтримку (кошти) та політичне й дипломатичне сприяння.

Міжнародне співробітництво продукує вдосконалення норм міжнародного права (зокрема й в Україні, яка удосконалює цей напрям у царині кібербезпеки та інформаційної війни). Така робота природно включає ініціативи щодо розробки та актуалізації нових міжнародних норм, стандартів та ін. Натомість інтеграція в глобальні системи безпеки дає змогу нашій країни ефективніше протистояти низці інформаційних загроз сьогодення, підвищувати рівень НБ і зміцнюючи міжнародний правопорядок та стабільність [121; 186, с. 20].

Це уможливлює стверджувати про кореляцію між НБ та ІБ, яка, на нашу думку, є фундаментальною щодо сучасних глобальних і національних викликів. Взаємопов’язаність цих понять продукована передовсім детермінацією стабільності і безпеки держави від захисту її інформаційного простору та диджиталізаційної інфраструктури. Сучасна безпекова реальність демонструє, що ІБ є невід’ємним складником НБ. Це пов’язано з тим, що захист інформаційного простору та систем є критично важливим для збереження суверенітету, економічної стабільності, політичної незалежності й добробуту країни. Відмінність між окресленими поняттями криється також і у їхній природі: НБ є станом, у якому держава здатна захистити низку формальних показників (суверенітет, цілісність територій тощо) свого побутування. Натомість ІБ сконцентрована навколо інформаційного дискурсу (апаратного, програмного, віртуального тощо) і його захисту від несанкціонованого доступу, актуалізації, змін та ін.

Отже, базуючись на окресленій категорійно-понятійній базі дослідження. вважаємо за доцільне сформулювати власне визначення ІБП.

ІБП є комплексом заходів, правил і стратегій, розроблених та імплементованих державою або організацією для захисту своїх інформаційних

активів від різноманітних загроз (несанкціонованого доступу, використання, розголошення, переривання, зміни, знищення тощо даних). Така політика, природно, включає в себе удосконалення, розвиток і розробку нормативно-правової бази, створення рівнів захисту інфраструктурних об'єктів через використання апаратних і програмних засобів. Окрім того, вона включає розробку, удосконалення тощо протоколів (скриптів) реагування на різноманітні інциденти, пов'язані зі спектром проблем ІБ. У такому сенсі ІБП дотична до окремих аспектів організаційної культури та поведінки, у які входять відповідна робота з кадрами (навчання, підвищення кваліфікації, перепідготовка) і розробка етичних норм (стандартів, принципів тощо) управління інформацією. Її основною метою є не лише технічних захист інформації, а й продукування стійкості та відповідального ставлення до інформаційних ресурсів з-поміж громадян і державних службовців [295].

У такому контексті релевантною, на нашу думку, є така властивість ІБП, як адаптивність, що полягає в інтенсифікації трансформаційних змін щодо змінюваних диджиталізаційних умов, які представлені дедалі новими видами загроз / викликів / небезпек у межах гібридної й інформаційної російсько-української війни. Це вимагає специфічного підходу, зосередженого на протидії різноманітним інформаційним загрозам, які становить агресивна політика росії. ІБП включає комплекс заходів, правил і стратегій, спрямованих на захист інформаційного простору країни від кібератак, мізінформації, дезінформації, пропаганди кібершпигунства й інших форм інформаційного втручання.

1.3 Види інформаційної безпеки та їх дискурсивна природа

На нашу думку, тут логічно звернутись до питомого розуміння поняття ІБ, яке, зазвичай, розуміється дослідниками у доволі спрощеному, відірваному від контексту, тобто дискурсу, плані. Таке звернення виглядає достатньо логічним, оскільки саме на його підґрунті можна виокремити складники ІБ, до

яких належить: а) відсутність єдиного підходу до категорійно-понятійного апарата (див. 1.2); б) недостатня семантична актуалізація поняття «загроза», його родова і видова невизначеність, що продукує дифузність меж від інших, споріднених термінів («небезпека», «виклик», «ризик» тощо), яка, своєю чергою, спричиняє нечітку кореляцію з, власне, ІБ, а також категорійним ланцюгом «інформаційна війна», «інформаційне протиборство», «інформаційний тероризм» та іншими; в) наявність невирішеної проблеми формування категорійно-понятійного апарату теорії ІБ; г) відповідно, неможливість на підґрунті теоретичних розробок цього апарата сформувати фундаментальну полісистему моніторингу та управління загрозами і небезпеками в інформаційній царині [125].

Відповідно, стрижневе поняття нашого дослідження, – загрози інформаційним ресурсам (далі – ІР), – доцільно ранжувати у контексті потенційно-можливих випадків екологічної, технічної або антропологічної природи. Вищезазначені загрози об’єднує їх потенційний небажаний вплив на інформаційні системи (дані загалом), які містяться на таких ресурсах. Натомість джерело актуалізації певних подій у загрозливих, небезпечних та інших обставинах детерміноване вразливістю їх природи. Таким чином, наявність цієї риси (вразливості) корелює з процесом активізації загроз, небезпек та іншого: так, за теорією множин вони є невичерпними, а відтак не можуть бути категоризовані й анотовані повною мірою. Отже, інтегруючи різноманітні підходи та інше щодо розв’язання цього питання виокремимо такі види загроз (див. рис. 2) [197, с. 176]:

Рис 2. Види загроз.

Однак найчастотнішим і найнебезпечнішим є людський фактор у роботі інформаційних систем: помилки користувачів, операторів, системних адміністраторів та інших фахівців, які їх обслуговують. Часом вищезазначені помилки становлять загрозу (неправильно введені дані, помилка програмного коду тощо), викликаючи системний збій або колапс, створюючи лакуни у безпекових системах тощо, або питомо є такими небезпеками. До прикладу, показовим є випадок уведення неправильних даних швейцарським авіаоператором, що спричнило зіткнення двох літаків, на одному з яких летіли діти.

Загалом понад 65% завданої ІР шкоди припадає на ненавмисні помилки: натомість природні катастрофи (пожежи, землетруси та інше) трапляються не так часто [40, с. 153–158]. Відтак, значущим є акцентування на диджиталізації царини ІБ, яка, своєю чергою, дозволить зменшити вплив людського фактора. Зокрема, плідним вважаємо програму Національного інституту стратегічних

досліджень «Електронна Україна» [249.]. Також виділимо такий вид небезпеки для ІБ як крадіжки, суб'єктами вчинення яких переважно є штатні спеціалісти, добре обізнані з роботою інформаційної системи та заходами її убезпечення. Мовиться також про незадоволених фахівців або тих, що не поділяють цінностей організації, установи та іншого, де вони працюють. До прикладу, показовими є дії колишнього генерала СБУ, одного з керівників ГУР України В. Кравченко, який 18 лютого 2004 року передав матеріали з обмеженим доступом журналістам «Дойче Веле» [308, с. 91–92].

Окрім того, доцільно згадати означені загрози, небезпеки та інше природного плану, яким притаманний великий спектр і видове різноманіття. Так, згадаємо інфраструктурні порушення (аварії електроживлення, відсутність зв'язку, перебої з водопостачанням тощо – власне, все те, що громадяни України пережили внаслідок ракетних атак та атак дронами) й стихійні лиха (землетруси, повені, смерчі та тому подібне). Наостанок відмітимо кількість інформаційних загроз (далі – ІЗ) природного характеру, яка становить приблизно 14% від загального числа [393]. Розглянемо інші класифікації викликів, загроз, небезпек та іншого (див. табл.1.1):

Таблиця 1

Класифікація викликів, загроз, небезпек

Категоризована властивість	**Характеристика**
За структурою впливу	
Системні	Релевантні для всього спектра складників суб'єкта захисту НБ, при цьому такий вплив є ґрунтовним, продукується одночасно у кількох вразливих і релевантних для всієї структури місцях. Безпосередньо для суб'єкта захисту НБ така атака здебільшого спрямована на дискредитацію фахівців, які працюють у ньому, через медіа, інтернет-дискурс (зокрема, політичний інтернет-дискурс). До прикладу**:** у 2014 році Російська Федерація здійснила масштабну кібернетичну атаку на Україну, яка вплинула на весь спектр державних інститутів, зокрема на енергетичну інфраструктуру,

	Продовження таблиці 1 фінансові установи та засоби масової інформації. Одним із важливих аспектів цієї атаки була дискредитація українських фахівців, використовуючи політичний інтернет-дискурс для поширення пропаганди та фальшивої інформації через медіа.
Структурні	У їх межах здійснюють вплив на атомізовані складники системи (державних інституцій або їх елементів). До прикладу, під час порушень процедури виборів міста Мукачево весною 2004 року відбулося дискредитування гілок влади: нижньої – місцевої влади, середньої – МВС.
Елементні	впливають на складники системи продукування ІБ (далі – СПІБ), вони мають постійну природу і можуть становити загрозу лише у випадках неефективного моніторингу або його відсутності. До прикладу, наприкінці 60-х років XX століття в Італії діяли так звані «Червоні бригади», які влада не сприймала достатньо серйозно. Наслідком цього стало те, що терористи спочатку погрожували, а згодом розпочали фізичну ліквідацію суддів, які виносили їм вирок [179, с. 127–131].
За природою актуалізації	
Реальні	Активізація алгоритмів дестабілізації, які не мають просторових і часових обмежень. До прикладу: ракетні удари та авіаудари, що були здійснені під час військових конфліктів (наприклад, вторгнення Росії в Україну в 2022 році), є реальними викликами для національної безпеки. Ці загрози не обмежуються часом чи простором і активно реалізуються у практичній реальності.
Потенційні	Задіяння алгоритмів відбувається лише за певних умов стану державної інституції. Приклад: Існує загроза потенційних кібератак, спрямованих на державні інституції або критичну інфраструктуру, якщо буде досягнута певна політична чи економічна криза. Наприклад, країни, що мають нестабільну економічну ситуацію, можуть стати мішенями для атак з боку кіберзлочинців або державних акторів.
Здійснені	Втілені у онтологічній реальності. Приклад: здійснена загроза у вигляді терористичних атак 11 вересня 2001 року в США. Атаки, що були втілені в реальність, призвели до глобальних змін в політиці безпеки та нових стратегій боротьби з тероризмом.

	Продовження таблиці 1
Потенційні	Фальшива активізація показово подібних до алгоритмів дестабілізації елементів, або задіяння таких алгоритмів, які схожі на вищезазначені, проте вони ними не є. Приклад: поширення фальшивих новин або маніпуляцій через соціальні мережі, які можуть виглядати як частина інформаційної атаки, але насправді вони не є частиною організованої дестабілізаційної кампанії. Наприклад, фальшиві повідомлення про наступ чи масові заворушення, які можуть бути використані для впливу на громадську думку або політичну ситуацію в країні, але насправді є лише частиною інформаційної маніпуляції.
За модальністю (ставленням)	
Об’єктивні	Декларовані сукупністю обставин і фактів, що достовірно характеризують навколишнє середовище. При цьому ставлення до них суб’єкта управління не відіграє вирішальної ролі через те, що об’єктивні загрози існують незалежно від його волі та свідомості. До прикладу, у Законі України «Про основи національної безпеки України» не визначено пріоритетність захисту від ІЗ, проте їх значущість є вагомою, що продукує деструктивність акцентування уваги на інших загрозах [238;239].
Суб’єктивні	Сукупність складників онтологічної реальності, яка вважається суб’єктом управління системою безпеки: у цьому випадку стрижневу роль у ідентифікації тих чи інших обставин та чинників відіграє воля вищезазначеного суб’єкта, який, власне, і приймає безпосереднє рішення про надання статусу або локалізації тих чи тих у безпековому вимірі.
За об’єктом впливу	
Громадянин	Суспільство / Держава
За формами актуалізації	
Нормативні	Визнані нормативно-правовими документами країни: зокрема, в Україні такі загрози визначені в Законі України «Про основи національної безпеки України» [100].
Ненормативні	Існують об’єктивно, проте не є усвідомленими вищим політичним керівництвом держави і не знайшли адекватного віддзеркалення у нормативно-правовій базі [222].

У вищезазначеній Таб. 1.1 висвітлено поліінтерпретаційність, різноманітність тощо підходів до класифікації викликів, загроз, небезпек та іншого ІБ. Диференційованість підходів природно корелює з генезою інформаційної зброї та продукує виникнення інформаційних воєн, середовищем яких буде ІПр. Натомість засобами окреслених бойових дій стане інформаційний інструментарій, покликаний продукувати досягнення низки стратегічних, політичних, економічних тощо цілей. Зокрема, щодо інформаційної й гібридної російсько-української війни доцільно говорити ппро такі види ІЗ, які набули особливої значущості:

1. *Кібервійна/кібератаки*: російська федерація динамічно використовує інтернет-дискурс задля ведення активних бойових дій проти України. Здебільшого атаки у ньому спрямовані на критичні об’єкти інформаційної інфраструктури (енергетичні мережі, фінансові установи та урядові системи). Метою таких заходів є завдання шкоди НБ, викликання хаос та підрив довіри громадян до уряду загалом (зокрема, державних інституцій). До прикладу, кібератака на урядові системи та критичну інфраструктуру України під час вторгнення в лютому 2022 року. Основною метою цих кібератак було завдання шкоди національній безпеці України, зокрема шляхом підриву довіри до уряду, порушення координації та захисту критичних об'єктів. Атаки на інфраструктуру мали на меті створити додаткове навантаження на систему, відволікаючи ресурси від бойових дій на фронті. Це показує, як Росія активно використовує кіберзброю в рамках своєї агресії проти України, де кібернапади не тільки підтримують військові операції, але й активно сприяють інформаційній дестабілізації, одночасно послаблюючи національну безпеку країни в декількох аспектах.

2. *Мізінформація, дезінформація* та *пропаганда*: виявляються у актуалізації низки неправдивих даних у вищезазначених дискурсах [334], метою яких є введення в оману громадян, маніпулювання громадською думкою як всередині нашої країни, так ззовні – на міжнародній арені. До прикладу, поширення неправдивих новин, створення фейкових соціальних

мереж, застосунків-копій офіційних та інтенсивне залучення тролів для поширення проросійських наративів.

3. *Кібершпигунство*: має на меті збирання конфіденційних даних наших співгромадян, які можуть бути використані для політичного тиску, воєнних цілей та іншого. До прикладу, злам офіційної та особистої електронної пошти, сторінок у соціальних мережах та тому подібного чиновників і таке інше.

4. *Вплив на медіа, онлайн-платформи, соціальні мережі тощо*: виявляється у вищезазначених у пункті 2 спробах маніпулювання громадською думкою, проте вже таргетованіше. До прикладу, використання ботів, фейкових акаунтів тощо у Facebook, Tik Tok та інших для створення враження великої кількості невдоволених українською владою користувачів. Згадаймо, тренд з піснею «Ухилянт» у Tik Tok, що сама по собі є вірусною і ставала тлом для висловлення невдоволення або критики дій нашого уряду.

5. *Психологічні операції*: унаочнені впливом на моральних дух, переконання та поведінку населення й позначені акумуляцією здобутків пунктів 1–4. До прикладу, актуалізація пропагандистських матеріалів, неправдивих даних та інших методів, покликаних посіяти паніку та атомізувати українське суспільство.

6. *Використання технологічних (першою чергою, апаратних) вразливостей*: мовиться про розробку, інтеграцію, імплементацію та експансію диджиталізаційних здобутків, які, разом з тим, продукують появу певних вразливостей [176, с. 16–20]. До прикладу, проблема із захистом того чи того застосунку, бази даних та інших, що мають стратегічне значення може спродукувати можливість знищення даних, які у ній знаходяться. Так, вищезазначений РДС НКСДМ, у випадку порушення його безпеки може призвести до хаосу і зриву конкурсів на обіймання посад державної служби. Останнє пов’язане з тим, що такий сертифікат чинний в електронному, а не паперовому вигляді, тому при наборі спеціаліст відділу кадрів перевіряє його наявність безпосередньо у вищезазначеному РДС, відсутність зв’язку з яким можу призвести до вкрай негативних наслідків.

Отже, інформаційні війни є реальністю диджиталізаційного світу, у якому ми живему, а тому відсутність розробленої концепції НБ, доктрини ІБ, а також стратегії інформаційної боротьби є критичними. Тим не менш, Україною розроблено і впроваджено низку нормативно-правових документів тощо щодо ІБ. Окрім того, наша держава ратифікувала ряд міжнарожних угод, договорів та іншого, які впливають на ІБ: останні суголосні сучасним диджиталізаційним трендам, викликам, небезпекам, загрозам і тому подібному. Відзначимо також динамічний розвиток ефективних українських механізмів для впровадження вищезазначених ініціатив та контролю їх трансформаційних змін.

Разом з тим державні інституції, повноваження яких стосуються ІБ (СБУ, Міністерство оборони України (далі – Міноборони), МВС та інші) відіграють стрижневу роль у продукування захисту інформаційної інфраструктури нашої країни [17, с. 29–32; 87; 117; 66]. При цьому питомим підґрунтям СПІБ є міжнародна співпраця, що забезпечує додаткову підтримку та обмін досвідом. Характерно, що інтенсивні зміни у глобальному та регіональному геополітичних дискурсах продукують потребу у постійному перегляді та вдосконаленні української законодавчої та нормативно-правової бази задля ефективного регування на нові виклики, загрози, небезпеки глобалізованого світу.

Отже, у представленому розділі наукової роботи проаналізовано теоретико-методологічні засади дослідження НБ: подано стан наукової розробки проблеми, виокремлено її категорійно-понятійний апарат (зокрема, основні підходи до визначення НБ та розкрито самобутність співвідношення НІД у інформаційній царині). Так, проведений аналіз історіографії засвідчив специфіку феномена ІБП та локалізував його співвіднесеність з низкою інституційних чинників в умовах воєнного стану, виявивши лакунізовану природу цієї проблематики. Мовиться про інтегровану, дискурсивну та інші особливості природи останньої, що, закономірно продукує потребу у її фундаментальному аналізі в контексті сучасних політологічних досліджень.

Натомість продукування високорівневої захищеності, питомої для національних інтересів, виформовує належні умови для сталого, динамічного й планомірного розвитку громадянина, суспільства та держави, що є стрижневим завданням ІБП. Прикметно, що головною умовою побутування останньої виступає пріоритет несилових шляхів захисту національних інтересів (цінностей, культурної й історичної пам'яті та інших здобутків), які є її підґрунтям. У такому контексті безпеку доцільно розглядати інтегративним утворенням, концептом, у якому акумульовано всі сфери життєдіяльності суспільства, де стрижневою є інформаційна.

Подана низка визначень та історично-концептуальних підходів до поняття НБ природно спричинила потребу у репрезентації універсалізованої авторської дефініції. У межах останньої НБ позиціонуємо багатошаровим концептом, що охоплює комплекс життєво важливих інтересів громадянина, суспільства та держави від внутрішніх/зовнішніх загроз. При цьому НБ є комплексною полісистемою, функціонування якої вимагає скоординованого підходу у вищезазначених царинах, а також гнучкого, оперативного, динамічного тощо реагування на поточні реалії, виклики та загрози. До цієї полісистеми входить не лише поточне реагування на наявні загрози й викликий, а й стратегічне планування, метою якого є випередження таких проблем й превентивне їх подолання.

Своєю чергою, інформаційні війни є актуальною проблемою сучасного світу, що продукує потребу у низці змін нормативно-правової бази, виконавчих механізмах та іншому. Зокрема, першою чергою, доцільно виструнчити концепцію НБ, доктрину ІБ, а також стратегію інформаційної боротьби. Водночас, Україна інтенсивно розробляє і впроваджує передовий досвід зарубіжних партнерів, продуктивно адаптуючи його (досвід) на своєму підґрунті: розробляючи і впроваджуючи нормативно-правові, соціальні та інші ініціативи, пов'язані з ІБ. Також відзначимо бурхливу міжнародну діяльність українського уряду: укладення низки угод, договорів та іншого, які впливають на ІБ. Вищезазначені документи суголосні диджиталізаційним

трендам, викликам, небезпекам та іншому, які стоять перед сучасною демократичною державою, якою є Україна.

Також заслуговує на увагу бурхливий розвиток ефективних, сучасних та інноваційних механізмів впровадження окреслених ініціатив та контроль їх трансформаційних змін. При цьому важливу роль, природно, відіграють інституційні чинники (державні інституції): СБУ, Міністерство оборони України (далі – Міноборони), МВС та інші, повноваження яких дотичні до питань ІБ. Прикметно, що динамічні зміни у глобальному та регіональному геополітичних дискурсах продукують потребу у постійному перегляді та вдосконаленні української законодавчої та нормативно-правової бази задля ефективного реагування на нові виклики, загрози, небезпеки ІБ глобалізованого світу.

РОЗДІЛ 2. ПОБУТУВАННЯ ІНФОРМАЦІЙНОГО ПРОСТОРУ ЩОДО ДЕРЖАВНО-ПРАВОВОГО МЕХАНІЗМУ БЕЗПЕКИ

2.1. Інформаційний простір України в контексті побутування інституційних чинників

Вищезазначені трансформаційні зміни розуміння ключових понять цієї наукової роботи засвідчили їх інтегративну природу, що, закономірно, продукує розгляд інформаційного простору (ІПр) як складника соціального простору. У такому контексті під цим поняттям доцільно розуміти страти суспільного життя, репрезентативні щодо ролі інформаційних комунікацій (далі – ІК) у них. Окреслене поняття набуває стрижневої ролі щодо побутування інституційних чинників (державних інституцій): така його динаміка детермінована переходом нашої країни до нового типу суспільства (економіки знань)[306]. У межах останнього релевантною цінністю стає інформація, що задекларовано формуванням Мінцифри (зокрема, актуалізацією концепції «Держава у смартфоні» тощо), яка, до всього, набула властивостей соціального ресурсу [41].

На жаль, гібридна й інформаційна російська-українська війна суттєво вплинула на становище нашої країни в ІПр, який репрезентативний щодо особливостей побутування й специфіки доступу, що, своєю чергою, виформовує платформу для розвитку і функціонування демократії. Так, на сьогодні, помітною є наявність у пересічних громадян гострого відчуття неможливості впливати на політичний курс уряду й місцевої влади, що активно використовується в інформаційних кампаніях ворога [262]. Останні заперечують цивілізаційний вектор розвитку Україні, у межах якого відбувається інтенсифікація міжнародних відносин (зокрема, перебирання досвіду ЄС і динамічна глобалізація інтегративного розвитку всіх сфер діяльності). Зокрема, у праці С. Дерев'янка «Гібридна війна: інформаційно-безпековий вимір» [61] ідеться про основоположну роль інформаційних

технологій і медіа в сучасних конфліктах і війнах у теперішньому світі, що впливають на національну безпеку держави загалом, України зокрема та її приналежні сектори.

Прикметно, що експонентний розвиток ІТ у нашій країні дійшов до такого рівня взаємодії, за якого швидкість, якість, доступність і актуальність інформації (даних) стають релевантними. Зокрема, мовиться про затребуваність останніх усіма учасниками ІБП, яка є визначальною щодо ефективності їх трансформаційних змін. Показово, що в сучасній економічній практиці наявний досвід створення єдиного ІПр, проте на рівні підприємства, холдингу, міста або навіть на рівні суб'єктів одного уряду. Однак проблема ІК у царині, що акумулює декілька країн, досі не знайшла своє розв'язання повною мірою [256].

При цьому доцільно врахувати специфіку пострадянського простору, у межах якого не кожна країна здатна інтегрувати свої інформаційні ресурси (далі – ІР) на сьогодні, оскільки такий простір можливий лише приблизно за одного рівня розвитку. До прикладу, рф, на сьогодні через санкції ЄС та ідеологічне підґрунтя актуалізує зворотний процес, дедалі більше прагнучи до атомізації свого ІПр, що засвідчує регресивність панівних у російському суспільстві наративів.

Утім, досвід ЄС у плані продукування ІПр (зокрема, побутування інституційних чинників (державних інституцій)) є показовим, що пов'язано з наявністю певного корпусу даних зі створення таких осередків, який за теоретичної обробки репрезентативний щодо генези на українському підґрунті. Відтак вивчення інституційних чинників (державних інституцій) щодо побутування ІБП за умов воєнного стану може бути продуктивним щодо низки економічних складників (зокрема, економічних відносин) [113].

Вищезазначена специфіка категорійно-понятійного апарату (див. 1.2) закономірно продукує паралельну актуалізацію терміна ІПр поряд з такими поняттями, як «інформаційне середовище», «інформаційне поле» та іншими з періодичним заміщенням останніми. Таким чином, підходи до ІПр відрізняють

або за метричною параметризацією (з урахуванням процесів, що відбуваються у його межах), або за концепціями (останні випрацювані в окресленому категорійно-понятійному апараті (насамперед природничих наук)).

Так, у цих науках ІПр позиціонований інформаційно-пошуковою системою (далі – ІПС), тобто впорядкованою сукупністю інформаційних одиниць (далі – ІО), що в подальшому піддаються обробці (пошуку й розшифровці). ІПр можна позиціонувати сукупністю інформаційних процесів, математичною моделлю, що має певні функційні параметри. ІПр інтерпретований, до прикладу, системою детермінант, що забезпечують перебіг певних інформаційних операцій [79].

Така поліінтерпретаційність досліджуваної нами категорії спричиняє потребу конкретизації із урахуванням європейських реалій та інноваційних світополітичних тенденцій. У межах останніх такий простір є сукупністю об’єктів (предметів, явищ, процесів) онтологічної реальності, матеріалізованих (ідеться про формальні вияви їх побутування: вимірність тощо) стосовно одне одного: тяглість, форма, відстань, орієнтація, взаємодія, перетин та інше.

Відповідно в межах соціального підходу доцільним вважаємо декларування сфери стосунків між людьми й спільнотами з метою обміну даними. У цьому випадку ІПр можна визначити своєрідним осередком певних утворень (структур: організацій, індивідів або їх груп), які взаємодіють у межах інформаційних відносин, тобто збирання, продукування, поширення і споживання інформації. При цьому категорійно-понятійна локалізація детермінована: а) *описом й аналізом ІТ* на соціально-політичну царину в синхронії й діахронії; б) *їх роллю в динаміці, природі тощо трансформаційних змін соціальних екосистем* (зокрема, соціальних технологій): власне, мовиться про викреслення того чи того вектора таких операцій; в) *виробництвом (за допомогою ІТ) нових соціальних і політичних технологій* із паралельною девальвацією наявних [196].

Отже, окреслена категорійно-понятійна категоризація репрезентативна щодо виокремлення єдиного ІПр – віртуального / матеріального конструкта, якому притаманна внутрішня ідентичність, спільні цілі й завдання тощо. Останні мають бути доступними для всіх учасників спільноти (тут – країни і, відповідно, громадяни) задля набуття, обміну й актуалізації ІР. У цьому контексті виокремимо критерії ІПр: 1. *Інформаційна цілісність* (одноманітність), що забезпечується високим ступенем медіаграмотності суспільства, де дані доступні для розуміння, пошуку й використання. 2. *Єдність цілей*, у межах яких суб'єкти, що взаємодіють (тут – громадяни) у просторі, мають спільну мету і вектор реалізації певних ідей. 3. *Доступність*, реалізована прозорістю тих чи тих практик щодо набуття, використання тощо даних [112].

Характерно, що інтеграційна взаємодія щодо ІБП потребує насамперед ретельного вивчення європейського досвіду, який засвідчує значущість розуміння трансформаційних змін усередині ЄС, що уможливлює вибудувати оптимальний вектор взаємодії, розвитку та виформувати адекватну стратегію. Отже, доцільно зосередитися на діахронічному аспекті формування ЄС: так, вищезазначений процес розпочався після Другої світової війни, основними причинами якого стало продукування захисту від посилення впливу СРСР й американської соціокультурної та економічної експансії.

Стимулом, підґрунтям тощо для міжнародної інтеграції стала інтернаціоналізація виробництва, яка спродукувала потребу у важелях і механізмах поглиблення взаємодії національних господарств: Євразійський економічний союз (далі – ЄАЕС), Європейська система центральних банків (далі – ЄСЦБ) тощо. У цих установах розроблювалися проєкти, що визначали функції й існування ЄС, історія створення якого, своєю чергою, має свою етапність, яка не репрезентативна щодо досліджуваної нами проблематики. Однак показовими вважаємо етапи формування єдиного ІПр, які розгорталися у тісному взаємозв'язку [216]:

1. *Зона вільної торгівлі* (1958–1968 рр.). Наприкінці цього етапу відбулося усвідомлення потреби у створенні нової інформаційної структури на міждержавному рівні.

2. *Митний союз* (1968–1986 рр.). На цьому етапі важливу роль у створенні організацій і установ регулювання та розвитку інформаційного середовища відіграли наднаціональні структури європейський агентств: останні використовувались для координації й управління інформаційними потоками. Так, наднаціональні інституції доповнювали механізм європейської інтеграції у цілісну полісистему, наслідком чого стало удосконалення інституційної системи.

3. *Загальний ринок* (1986–1992 рр.). Важливою віхою цього періоду в контексті нашої наукової роботи є поширення автоматизованих систем управління (1970 р.) і поява інтернету, що вийшли на міжнародний рівень. Окрім того, показовим стало створення Європейської мережі бізнес- та інноваційних центрів, що мала самобутню інфраструктуру (складалася з національних мереж) і стала підґрунтям для інтегрованої європейської інноваційної й інформаційної системи. Важливим складником цієї мережі є European Patent Office (далі – EPO), інформаційне забезпечення якого здійснюють спеціальні служби мережі «Інтернет». Основною метою функціонування цього проєкту є надання даних на регіональному та державному рівні з орієнтацією на малий і середній бізнес. Інформаційний супровід розвитку інноваційної діяльності забезпечується декількома IP вільного доступу, фінансованих ЄС [79].

Базою цієї мережі є система Community Research and Development Information Service (далі – CORDIS), що підтримується програмою Competiveness of Small and Medium Enterprises (далі – COSME). Ця програма забезпечує вільний доступ до інформації про наукові дослідження і розробки, реалізовані в країнах ЄС. Вона також корисна для пошуку джерел фінансування в наукових дослідженнях, пошуку партнерів, трансфера технологій. Ця система включає і розв’язання питань інтелектуальної

власності за посередництва контактів з різними установами, організаціями, інституціями тощо [195]. Таким чином, формування єдиного ІПр на цьому етапі ще не передбачало розвинутої організаційної структури, проте вже поставлено питання щодо пошуку, добору та репрезентації даних, їх достовірності й безпеки. Паралельно набула розвитку система соціальних мереж, що вплинула на інформаційні потоки як усередині, так і ззовні ЄС.

4. *Економічний і валютний союз* (з 1993 і до досі). Детермінований уходженням європейського співтовариства на шлях постіндустріального розвитку, що спродукувало поліпшення рівня життя населення, з-поміж наслідків чого – щораз більші темпи диджиталізаційних змін: набули поширення новітні комп'ютерні й телекомунікаційні пристрої, що, своєю чергою, актуалізувало питання контролю інформації.

Була створена низка агентств ЄС, які можна розділити за спрямуванням: економічні (внутрішній ринок тощо), моніторингові (охорона природи, права людини тощо), комунікаційні (освітні, соціальні, безпекові щодо здоров'я, наукові тощо), стратегічні (репрезентативні щодо роботи ЄС та особливостей її функціонування), політичні (власне безпекові, геополітичні питання тощо). У контексті цього дослідження виокремлюємо моніторингові (пов'язані зі збиранням, обробкою та поширення даних із дотриманням вільного доступу до них: European Environment Agency (далі – EEA), European Union Fundamental Rights Agency (далі – FRA) тощо) та політичні (спільної зовнішньої політики та ІБП: European Defence Agency (далі – EDA), European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (далі – FRONTEX) тощо) [108].

Характерно, що на початкових етапах такі інституції були лише накопичувачами інформації: водночас були сформовані загальні канали й розроблені регламенти доступу до даних, проте атомізовані для кожної установи. Лише з введенням євро і формуванням Валютного союзу наднаціональний механізм у ЄС почав функціонувати розгорнутою системою

в повному обсязі. Створення економічного й валютного союзу ЄС уможливило сформулювати стрижневі положення системи мережевих платежів [41].

2000 р. у ЄС ухвалено до розробки й реалізації проєкт «Електронна Європа» (Electronic Europe) (далі – eEurope), який засвідчив акцентування на досягненні соціальної єдності націй союзу і європейської спільноти загалом. Останніми багато уваги приділено проблемі ІПр у соціальних і культурних вимірах людської діяльності, збереження культури й розвитку освіти. Проєкт «Електронна Європа» має за мету посилення зв'язку між урядом і громадянами за посередництва ІТ. На думку розробників, це продукуватиме зростання ефективності й виконання нормативно-правових документів, розвиток державних служб, взаєморозуміння між державними інституціями і громадянами [262].

Основна мета проєкту суголосна з курсом української Мінцифри: доступність усіх послуг, надаваних владою, через мережу «Інтернет». Водночас це уможливлює говорити про необхідність формування єдиного ІПр на базі простої інформації й вільного доступу до неї. Тут доцільно згадати дванадцятирічний досвід співпраці Мінцифри з Естонською академією електронного урядування: зокрема, проєкти EGOV4UKRAINE, EU4DigitalUA та «Підтримка ЄС у зміцненні кібербезпеки України». Показовим тут є найновіший на сьогодні проєкт ЄС «Цифрова трансформація для України» (DT4UA) [86], мета якого – підвищення ефективності та безпеки надання державних послуг і доступу до них для громадян і бізнесу.

Він розпочався з листопада 2022 року (рік початку російсько-української війни) та триватиме до квітня 2025 року, основною метою є реалізація питомої вимоги єдиного ІПр в Україні. Зокрема – розвиток механізмів, підвищення ефективності та безпеки надання / отримання державних послуг щодо покращення доступу до них громадян і бізнесу в Україні відповідно до вимог ЄС. Ці послуги є базовими для демократичної країни: вони є необхідними під час війни і стануть у нагоді після її закінчення (як база для відновлення країни) [256].

Релевантними в реалізації проєкту «Цифрова трансформація для України» є чотири стрижневі напрями: а) розвиток цифрових послуг та середовища надання послуг «Дія»; б) оптимізація процесів обміну даними між реєстрами, надавачами та кінцевими користувачами (громадянами) таких послуг; в) генеза інфраструктури електронної ідентифікації відповідно до electronic IDentification, Authentication and trust Services (далі – eIDAS); г) трансформаційні зміни системи електронного управління справами, що продукуватиме ефективніший та прозоріший розгляд кримінальних справ [103].

У цьому контексті вагомим є внесок Мінцифри, що має за мету інтенсифікацію диджиталізаційних процесів в Україні. Так, за три роки міністерством цифровізовано найпопулярніші та наймасовіші державні сервіси, що потрібні громадянам у побутовому житті. Така пильна увага уряду до диджиталізаційних процесів пов'язана зі специфікою ІПр України щодо формування та реалізації державної політики. Ідеться насамперед про забезпечення процесу комунікації між державними інституціями (усередині і ззовні – з громадянами) та поширення інформації, релевантної для ухвалення управлінських рішень [216].

За сучасних умов стрімкої диджиталізаційної генези державі необхідно адаптувати свої інституційні механізми для ефективного управління ІПр. Серед стрижневих інституцій, які є складниками цього процесу щодо регулювання ІПр, назвемо: а) *ГУР* (здійснює видобування, обробку, надання розвідувальних даних (у межах Закону України «Про розвідку», проводить низку заходів задля сприяння реалізації національних інтересів, бере участь у формуванні державної політики тощо) [246]; б) *ДБР* (встановлює справедливість у суспільстві через проведення незалежних, фундаментальних і всебічних розслідувань злочинів з метою притягнення винних до відповідальності, безвідносно до їх посад, зв'язків та ресурсів) [64]; в) *Державний комітет телебачення і радіомовлення України* (далі – *ДКТРУ*) (формує державну інформаційну політику, регулює діяльність медіа, ліцензує

телерадіокомпанії та контролює дотримання законодавства України у сфері інформації) [65] та г) *Національна рада України з питань телебачення і радіомовлення* (далі – *НРУПТіР*) (контролює дотримання стандартів мовлення, опікується виданням ліцензій і діяльністю телерадіокомпаній) [207]; г) *Мінцифри* (розвиває ІТ: зокрема, виформовує електронне урядування, диджиталізує державні послуги, розвиває ШІ та інше) [202] та д) *Держспецзв'язку* (питомий складник полісистеми кібербезпеки нашої країни, у межах відповідальності якого – стабільна, неперервна та безпечна робота державних ІР та об'єктів критичної структури тощо) [62]; е) *НКДСМУ* (сприяє розвитку української мови як державної, продукуючи її логічну, цілеспрямовану й науково обґрунтовану стандартизацію) [205] і є) *Уповноважений із захисту державної мови* (його діяльність спрямована на захист української мови як державної, а також сприяння права громадян нашої країни на отримання інформаційних та інших послуг безпосередньо державною мовою) [291]; ж) *СБУ* (стрижневою місією інституції є безпека України та захист її громадян, що репрезентовано в напрямах її діяльності: контррозвідці, участі в бойових і спеціальних операціях на фронті, захисті національної державності, боротьбі з тероризмом, захистом ІБ та охороною державної таємниці) [276]; з) *ЦПД* (здійснює заходи, покликані протидіяти наявним / потенційним загрозам НБ та національним інтересам (далі – НІ) в інформаційній царині, продукує ІБ, шляхом виявлення мізінформації, дезінформації та пропаганди) [300] тощо.

Водночас вважаємо доцільним ураховувати низку інституційних викликів і можливостей, існування яких детермінує розвиток ІБП, зокрема: 1. *Політичний гомеостаз і незалежність медіа* як стрижневий виклик поточної ситуації в Україні: ідеться передовсім про убезпечення медіа від політичних акторів, що продукуватиме зміцнення довіри до влади й уможливить уникнути маніпуляцій різного роду, натомість сформувати систему неупередженого інформування громадян та актуалізувати демократичні процеси. 2. *Протидія мізінформації, дезінформації та*

пропаганді: пов’язана з тим, що ІПр України на сьогодні є релевантним об’єктом інформаційних атак, метою яких є підрив авторитету влади, продукування внутрішнього напруження та загальна дестабілізація безпекової ситуації. 3. *Розвиток медіаграмотності населення* через формування умінь громадян критично оцінювати достовірність різноманітних даних, на підґрунті низки складників (стилю, джерела, змісту та іншого) таких даних [79].

Оскільки ІПр безпосередньо корелює з вищезазначеним політичним гомеостазом, то релевантним є вільний доступ до інформації з об’єктивним висвітленням дій уряду. Насамперед це продукує стабільне політичне середовище й формує довіру до уряду з експонентним зменшенням ризику виникнення тієї чи тієї кризи. Така політика сприяє поширенню демократичних цінностей, питомими складниками динаміки процесу якої є зміцнення громадянського суспільства, генеза політичної культури й трансформаційні зміни урядування [256].

Таким чином, на перший план функціонування ІПр України щодо побутування інституційних чинників (державних інституцій) виходять стратегічні комунікації уряду, які є важливим інструментом державної інформаційної політики (зокрема, ІБП), оскільки вони сприяють продукуванню позитивного іміджу країни на міжнародній арені й стабілізації політичного становища всередині неї. У такі комунікації входять інформаційні проєкти, спрямовані передовсім на ззовні (інформація про події в Україні, сфальсифіковані відео та текстові дані тощо). Частиною такої комунікації є також взаємодія з діаспорою як важливим ресурсом для просування НІ України у світі. Мовиться про активну взаємодію державних інституцій з представниками діаспори, залучення їх до інформаційних проєктів та підтримки низки урядових кампаній та ініціатив[306].

ІПр України є диференційованою, інтегрованою та динамічною полісистемою, яка детермінована побутуванням інституційних чинників (державних інституцій). Їх діяльність корелює з динамікою адаптації до нових викликів (зокрема, у межах гібридної та інформаційної російсько-української

війни). Відтак інституційні чинники відіграють стрижневу роль щодо продукування ефективного функціонування ІБП, насамперед формуючи нормативно-правову базу та надаючи державні послуги, а також актуалізуючи свій питомий функціонал (регулюючи діяльність медіа, інтегруючи ІТ тощо), що корелює із загальною державною концепцією, стратегією щодо цього вектора [41].

Тільки за комплексного підходу й активної взаємодії між інституційними чинниками (державними інституціями) можливий сталий, поступовий, логічний розвиток ІПр України, який є стрижневим складником НБ та розвитку, що зумовлює потребу в його постійній генезі, диджиталізації тощо. Для забезпечення ефективного функціонування ІПр необхідно актуалізувати комплекс заходів, метою яких є розвиток нормативно-правової бази, експонентне підвищення рівня міжінституційної координації та інтегрування інноваційних ІТ.

Головними детермінанти належного побутування ІПр є: інноваційні технології (ШІ, блокчейн, BD тощо), які продукують підвищення ефективності управління інформаційними потоками та захисту даних; міжнародна співпраця, що забезпечить актуалізацію передового досвіду в царині НБ та ІБ, а також регулювання ІПр загалом; стратегічне планування: мовиться про розробку та реалізацію довгострокових стратегій розвитку ІПр, у яких враховано не лише глобальні тенденції та специфіку розгортання, а й самобутність трансформаційних змін української держави в контексті поточної безпекової ситуації – гібридної й інформаційної російсько-української війни.

2.2. Система забезпечення інформаційного простору та специфіка її роботи щодо безпекових стратегій

Як уже йшлося, ІБ є стрижневим та інтегрованим поняттям у науковому дискурсі, яке детерміноване сутністю, ґрунтовністю та іншим сучасного

інформаційного суспільства. Проведений у попередньому розділі (див. 1.2) аналіз категорійно-понятійного апарату дослідження дав змогу розглядати ІБ як конструкт, у межах якого актуалізована органічна єдність ознак (стану, властивостей тощо). Окрім того, виокремимо таку властивість, як управління загрозами і небезпеками, що продукує обрання оптимального шляху х усунення через мінімізацію впливу негативних наслідків. Власне, це і є змістовним осередком діяльності зі створення сприятливих умов для реалізації інтересів громадян [151, с. 17–22].

ІБ сутнісно є ширшою, ніж захист інформації, оскільки вона, як ми з'ясували вище, є інтегрованим напрямом діяльності, який доречно досліджувати в межах системно-комплексного підходу. При цьому специфіка категорійно-понятійного апарату дослідження унаочнює потребу такого диференційованого підходу, який адаптивний щодо спектра багатоманітних і суперечливих онтологічних форм. Водночас стрижневою характеристикою ІБ доцільно позиціонувати ймовірність тої чи тої події онтологічної реальності. У цьому випадку мовиться про вірогідність появи загрози вищого ступеня або певної небезпеки для громадянина, суспільства та держави. Характерно, що критерійним показником ефективності продукування ІБ можна вважати її високий рівень за умови мінімуму витрат.

Таким чином, варто окреслити структуру цього інтегрованого, багаторівневого й поліінтерпретаційного поняття: так, його основним елементом є актуальні релевантні запити тої чи тої соціальної системи. Останні корелюють із зовнішніми чинниками – інтересами наднаціональних та інших національно-державних установ у контексті міжнародного співтовариства [15]. При цьому цей компонент такого національно-державного утворення, як його життєво важливі інтереси, корелює з подібними компонентами (інтересами) складників, що функціонують у його межах. Ними, природно, є соціальні групи, еліта, установи (організації), угрупування (партії), релігійні та етнічні утворення, різноманітні рухи тощо. Натомість сукупність внутрішніх і зовнішніх інформаційних загроз (далі – ІЗ)

виформовують передумови для низки похибок у функціонуванні системи державного управління (зокрема, щодо безпеки цього процесу).

При цьому значущість інформаційно-комунікаційних процесів (далі – ІКС) у сучасному світі дає підстави декларувати продукування ІБ глобальним та пріоритетним завданням інституційних чинників (державних інституцій, органів державного управління). Релевантність цього завдання продукує підпорядкованість його вирішенню політичної, економічної, воєнної, культурної та інших видів діяльності вищезазначених інституцій [158, с. 220–237]. Водночас інфраструктурна лакунізованість системи продукування ІБ унеможливлює стале, експонентне, фундаментальне тощо досягнення її цілей у межах глобальнішого дискурсу НБ в окресленій царині. Відтак стає неможливим досягнення питомої функції полісистеми, яка полягає в продукуванні збалансованого задоволення потреб громадян, суспільства та держави.

Відповідно СПІБ України виформовується та набуває трансформаційних змін у межах Конституції нашої держави [150], інших нормативно-правових документів (див. 1.2–1.3). Конституція є базовим нормативно-правовим державним документом, що, поряд з іншими актами, регулює суспільні відносини в інформаційній царині. У підр. 2.1 ми згадали інституційні чинники (державні інституції), які є підґрунтям вищезазначеної системи. Такі складники, закономірно, актуалізують у своїй діяльності низку нормативно-правових, інформаційно-аналітичних, організаційно-управлінських та інших заходів, спрямованих на продукування належного, сталого функціонування системи державного управління [305].

Формування СПІБ відбувається паралельно з усвідомленням потреби у функціонуванні механізму балансу інтересів усієї системи державного управління в інформаційній царині [187]. Зазначимо самобутність історіогенезу України в аналізованій площині: так, за роки незалежності сформовано підґрунтя для функціонування системи продукування ІБ. Зокрема, напрацьовано великий корпус документів (переважно нормативно-правові:

закони, постанови, укази, концепції, стратегії та інше), у яких визначено стрижневі повноваження державних інституцій у цій царині.

Показово, що Президентом України проведено фундаментальну роботу щодо вдосконалення системи управління вищезазначеною цариною. Так, вагомими в політико-правовій площині вважаємо такі Укази Президента України: «Про деякі заходи щодо захисту держави в інформаційній сфері» [292]; «Про вдосконалення державного управління інформаційною сферою» [290]; «Про вдосконалення інформаційно-аналітичного забезпечення Президента України та органів державної влади» [96]; «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Internet та забезпечення широкого доступу до цієї мережі» [276]; «Про додаткові заходи щодо безперешкодної діяльності засобів масової інформації, дальшого утвердження свободи слова в Україні» [100] тощо.

Побутування СПІБ не обмежується нормативно-правовими документами: тут наявна низка лакун, неточностей, внутрішніх неузгоджень. Зокрема, мовиться також про флуктуативність національної політики, а відтак і ІБ, яка передовсім продукує дифузність доктрини останньої. Відповідно відсутня необхідна для належного й неперервного функціонування Концепції НБ база, якої, на жаль, немає в нашій країні. Це спричиняє потенційну відкритість, невизначеність, адаптивність тощо процесу формування стрижневих складників СПІБ [287, с. 123–127].

Показовим у цьому плані вважаємо Закон України «Про основи національної безпеки України» [100], у якому задекларовано дев’ять стрижневих напрямів державної політики щодо НБ у різних сферах життєдіяльності. Однією з них названо інформаційну, що дає змогу позиціонувати її значущою й долучати до НБ. Водночас постулюємо неузгодженість цього документа щодо місця інформаційної царини (поставлена на останнє місце). На нашу думку, така недбалість авторів засвідчує їх необізнаність, неусвідомлення та інше щодо значущості, ролі такої безпеки у формуванні, побутуванні й розвитку держави як такої.

У найзагальнішому розумінні СПІБ є системою інформаційно-аналітичних, теоретико-методологічних, адміністративно-правових, організаційно-управлінських, спеціальних та інших заходів, що мають за мету продукування сталого розвитку об’єктів ІБ, а також інфраструктури забезпечення останніх [113, с. 423]. Категорійно-понятійна невизначеність зумовлює наукові дискусії щодо вищезазначеного формулювання, проте їх змістовність корелює із локалізацією генези і, власне, функціонування СПІБ.

Зокрема, базовими складниками окресленої системи є: а) *ґрунтовна генеза категорійно-понятійного апарату*, яка полягає в комплексному й інтегрованому визначенні поняття ІБ та її складників, а також світоглядній і концептуальній (логічній, належній тощо) репрезентації останнього в нормативно-правових документах (концепціях, стратегіях, доктринах, програмах тощо, що регулюють його побутування); б) *продукуванні і експлуатуванні оптимальної структури СПІБ*, яка базується на аналізі функціонування її детермінант задля оптимізації механізмів міжінституційної взаємодії в межах актуалізації такої системи; в) *методологічної єдності*, яка реалізована через випрацювання та ухвалення єдиного комплексного підходу до нормативно-правових документів без внутрішніх неузгодженостей і правових колізій щодо питань ІБ; г) *формування прозорого, логічного й органічного для українського законодавства механізму*, метою якого має стати координування діяльності складників СПІБ на всіх рівнях державного управління; ґ) *підготовка і забезпечення кадровим ресурсом усіх рівнів екосистеми ІБ* задля системної, наступної й прозорої діяльності останніх, що продукуватиме підвищення довіри до органів влади і стабілізуватиме додатково безпекову ситуацію в країні за умов війни і майбутнього миру [166, с. 166–168].

Відповідно до самобутності формування СПІБ доцільним вважаємо локалізувати її стрижневі функції (див. табл. 2.1) [106, с. 5–9]:

Таблиця 2

Функції СПІБ України

<table>
<tr><td colspan="3">1. Створення та забезпечення діяльності державних та недержавних органів і організацій – елементів вищезазначеної системи</td></tr>
<tr><td colspan="2">розробка адміністративно-правових засад для побудови та функціонування СПІБ: доктрини ІБ, організаційної та функційної структури системи</td><td>належне, наступне, системне тощо забезпечення елементів СПІБ: інформаційне, аналітичне, адміністративно-правове, матеріально-технічне, кадрове, ресурсне тощо забезпечення усієї системи державного управління</td></tr>
<tr><td colspan="3">2. Управління системою ІБ: здійснення свідомого цілеспрямованого впливу державних інституцій (суб’єкта управління) на загрози та небезпеки, внутрішні та зовнішні чинники, які корелюють зі станом ІБ</td></tr>
<tr><td>розробка на підґрунті вищезазначеної доктрини конкретних планів та технологій її забезпечення суголосно потребам кожного рівня державного управління</td><td>прогнозування, планування, організація, регулювання та контроль усієї СПІБ, а також її окремих елементів</td><td>оцінка результативності дій, витрат на проведення заходів щодо продукування ІБ</td></tr>
<tr><td colspan="3">3. Здійснення планової та оперативної діяльності щодо продукування ІБ</td></tr>
<tr><td colspan="2">визначення інтересів органів державного управління в інформаційній царині та їх пріоритетності щодо державної та інформаційної політики</td><td>виявлення, категоризація та інше загроз та небезпек, локалізація джерел їх виникнення й прогнозування можливих наслідків зі здійсненням низки превентивних заходів</td></tr>
<tr><td colspan="3">4. Міжнародне співробітництво в сфері ІБ</td></tr>
<tr><td>розробка нормативно-правової бази, яка регулює інформаційні відносини між державами та їх взаємодію в царині ІБ</td><td>інтеграція у наявні та утворення нових двосторонніх і багатосторонніх установ (організацій), діяльність яких спрямована на розв’язання проблем ІБ з урахуванням національних інтересів (далі – НІ)</td><td>участь у роботі керівних, виконавчих та забезпечувальних підрозділів вищезазначених установ (організацій), спільне проведення планових та оперативних заходів</td></tr>
</table>

Таким чином, метою продукування ІБ є формування належних умов для діяльності конкретної державної інституції (органу державного управління). Окрім того, проведення моніторингу її стану уможливлює розробити оптимальну модель функціонування СПІБ. Прикметно, що вищезазначеним інституційним чинникам (суб'єктам окресленої системи) необхідно тісно взаємодіяти між собою. При цьому ними має бути актуалізована паралельна спеціалізація задля розв'язання конкретних завдань у її (спеціалізації) межах з вжиттям для цього відповідних, визначених законом, адміністративно-правових форм та методів [166].

Наслідком цього є взаємодоповнення діяльності інституційних чинників, що продукує формування стрункої організаційно-функційної системи. Для неї характерною є самобутня когезія, базована на низці владно-розпорядчих повноважень, а також особливий функційний спектр актуалізацій щодо продукування ІБ. Своєю чергою, це дає змогу позиціонувати складниками СПІБ України: а) інтереси інституційних чинників в інформаційній царині; б) полісистеми таких чинників, а також компетентних осіб і стосунки між ними (ідеться про соціокультурний дискурс, що супроводжує побутування цієї царини).

Умовою функціонування СПІБ є належна організація її побутування, тобто створення економічних, соціокультурних та інших умов. Мовиться про формування, розвиток і забезпечення оптимальної актуалізації інформаційних ресурсів (далі – ІР) у всіх сферах життя і діяльності громадян, суспільства та держави [159]. Стрижневим завданням продукування ІБ є формування умов для організації належного, наступного та іншого управління СПІБ. До основних завдань СПІБ належать:

1. Створення умов для забезпечення інформаційного суверенітету (далі – ІС), що досягається за рахунок участі в генезі державного регулювання розвитку інформаційної царини. Продуковане шляхом виформовування нормативно-правових, економічних, соціокультурних та інших передумов для

розвитку національної інфраструктури та ресурсів, упровадження інноваційних технологій.

2. Наповнення ІПр України достовірними даними та іншого й забезпечення дотримання норм права громадян на свободу слова, доступу до інформації тощо. Продукування, проведення й ужиття комплексних заходів щодо захисту вищезазначеного простору та протидії монополізації інформаційної царини України: гарантування ІБ усіх детермінант системи державного управління та плекання інформаційно-аналітичного потенціалу країни шляхом реалізації ІБП [156, с. 127–129].

3. Залучення медіа до боротьби з корупцією, різноманітними зловживаннями службовим становищем та подібними явищами, що становлять загрозу для НБ України. Окрім того, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування та посадових осіб з вищезазначених органів у діяльність медіа та профілактика таких потенційній протиправних тощо дій цих суб'єктів СПІБ.

4. Відслідковування, локалізація, попередження й перешкоджання вчиненню терористичних дій та іншої протиправної діяльності. Остання є спрямованою на дискредитацію органів влади, пошкодження об'єктів критичної інфраструктури та різного роду перешкоджання функціонуванню системи державного управління загалом. Така діяльність державних інституцій виявляється у: а) моніторингу (спостереженні, оцінці, прогнозуванні тощо) стану ІБ у зв'язку з впливом загроз і небезпек як зсередини, так ззовні системи державного управління; б) забезпечення збереження державної таємниці; в) залучення громадськості шляхом організації демократичного цивільного контролю за функціонуванням вищезазначеної системи управління тощо [103, с. 46–55].

5. Ведення інтенсивної розвідувальної, контррозвідувальної і оперативно-розшукової діяльності, яка має на меті продукування ІБ задля моделювання процесів, механізмів та іншого, ухвалення стратегічних, тактичних і оперативних рішень у сфері державного управління ІБ. Окрім

того, ідеться про створення низки механізмів, практик, стратегій щодо вироблення, реалізації таких рішень. Релевантним також вважаємо безпосередньо протидію апаратному, програмному зламу інформаційно-телекомунікаційних систем ЦОВВ з метою вчинення злочинів (до прикладу, диверсійної діяльності).

Отже, функційна широта спектра СПІБ України локалізована нами в такому категорійно-понятійному конструкті: здійснення суб'єктами СПІБ продукування ІБ за рахунок створення умов для її оптимального функціонування. Такий підхід, на нашу думку, є найпродуктивнішим, незважаючи на наявність цілої низки тлумачень такої параметризації СПІБ. Зокрема, Є. Кравець [159; 160] серед стрижневих функцій СПІБ за умов надзвичайних ситуацій (далі – НС) виокремлює: а) локалізацію, опрацювання та прогнозування загроз і небезпек життєво важливим інтересам громадян, суспільства, держави (об'єктам ІБ), а також здійснення заходів для їх нейтралізації; б) організацію, забезпечення тощо ресурсного резерву для продукування ІБ; в) здійснення низки заходів задля реалізації зазначеної у пункті (б) мети задля нормального функціонування об'єктів ІБ на територіях, які постраждали внаслідок виникнення НС; г) участь у заходах, метою яких є продукування ІБ за межами нашої країни за умовами міжнародних нормативно-правових документів (договорів, угод та іншого), укладених і визнаних Україною [159; 160]. Певну схожість підходу простежуємо в В. Богдановича [14], що дає підстави нам виокремити такі складники за вченим:

1. Розробка й ухваленням політичних рішень, законодавчих і нормативно-правових документів щодо забезпечення СПІБ інформаційними ресурсами (далі – ІР) і нагляд за дотримання норм права в царині побутування таких ресурсів і здійснення правосуддя у сфері інформаційних відносин (далі – ІВ).

2. Визначення та здійснення повноважень системою інституційних чинників (органами державного управління) щодо низки дій (володіння,

розпорядження й користування) у сфері ІР, зокрема фінансово-економічних засад регулювання їхнього використання.

3. Реалізація низки заходів (організаційних, виконавчих, дорадчих та інших) і нормативно-методичний супровід відомчих і регіональних установ у царині формування та актуалізації ІР, контроль за їх формуванням, розвитком і використанням. Також формування (технологічно й методологічно) єдиних засад їх побутування за результатами діяльності державних інституцій (крім ІР, зміст яких становить державну таємницю або дані з обмеженим доступом).

4. Проведення державної реєстрації ІР, забезпечення повноти, комплексності тощо їх створення (первинних і вторинних) на засадах актуалізації даних, що виникає (створюється) у процесі діяльності органів державного управління.

Схарактеризована параметризаційна самобутність СПІБ України закономірно виформовує потребу в репрезентації її методологічної та структурної специфіки [195, с. 74–84]. Зокрема, діяльність, пов'язана з функціонуванням СПІБ, позначена використанням цілої низки способів, засобів, прийомів, механізмів, практик та іншого, які, власне, сукупно і становлять її методологічний каркас. Такі методи диференційовані (оскільки корелюють з інтегративною природою аналізованої проблематики): так, наявна залежність від типу діяльності (сфери застосування), специфіки бажаного результату та оптимальності локальним завдання і місії державної інституції. Відповідно релевантними методами аналізу стану СПІБ є *метод опису та класифікації*, що пов'язано зі специфікою досліджуваної проблеми.

З огляду на це виникає потреба в анотуванні (власне, описі) досліджуваного матеріалу, далі – його категоризації: до прикладу, видів загроз і небезпек, ризиків та викликів тощо і, відповідно, формулювання системи заходів задля подальшого управління ними [199, с. 176]. Окрім того, згадаймо *методи дослідження причинових зв'язків*, за допомогою яких локалізують корелятивні ланцюги між раніше згадуваними об'єктами небезпечної природи. Також вони репрезентативні щодо пошуку причин, появи або

актуалізації тих чи тих небезпечних детермінант та розробки низки заходів з метою нейтралізації таких складників. Серед окреслених методів, що корелюють з функціонуванням логічних, причиново-наслідкових зв'язків, назвемо: *метод схожості, метод відмінності, метод змін, метод залишків* та ін.

Вибір інструментарію сучасного наукового дослідження СПІБ детермінований рівнем і цариною організації захисту, її історіогенезом та поточним станом. Зокрема, залежно від типу, виду, специфіки та іншого загрози конкретизують особливості диференціації, локалізації, інтеграції та глобалізаційний контекст не лише загроз, а й спектра варіацій реакції на них – захисту. Щодо царини ІБ, то зазвичай у її межах виокремлюють: фізичний, програмно-технічний, управлінський, технологічний рівні, рівень користувача, мережний, процедурний [209] і багато ін.

Виокремимо низку типів методів продукування ІБ: а) *однорівневі*: вибудовують на підґрунті адміністрування ІБ і детерміновані особливостями цього процесу; б) *багаторівневі*: базовані на кількох принципах управління ІБ, кожен з яких атомізовано вирішує підзавдання загального процесу й спрямований на виконання конкретних функцій; в) *комплексні*: за своєю суттю є багаторівневою технологією, однак об'єднаною навколо спільної мети за допомогою координуючих функцій, що, своєю чергою, діють за результатами аналізу низки складників небезпеки, які мають спільний осередок; г) *інтегровані*: так само мають за підґрунтя багаторівневі методи, проте модифіковані інструментально (взято за зразок потужні автоматизовані інтелектуальні засоби (далі – АІЗ) з організаційним управлінням) [73, с. 61–70]. Стрижневою рисою самобутньої методології в СПІБ є активне використання *загальнонаукових методів*, які актуалізовані практично на будь-якій стадії управління прогнозами (див. рис. 3).

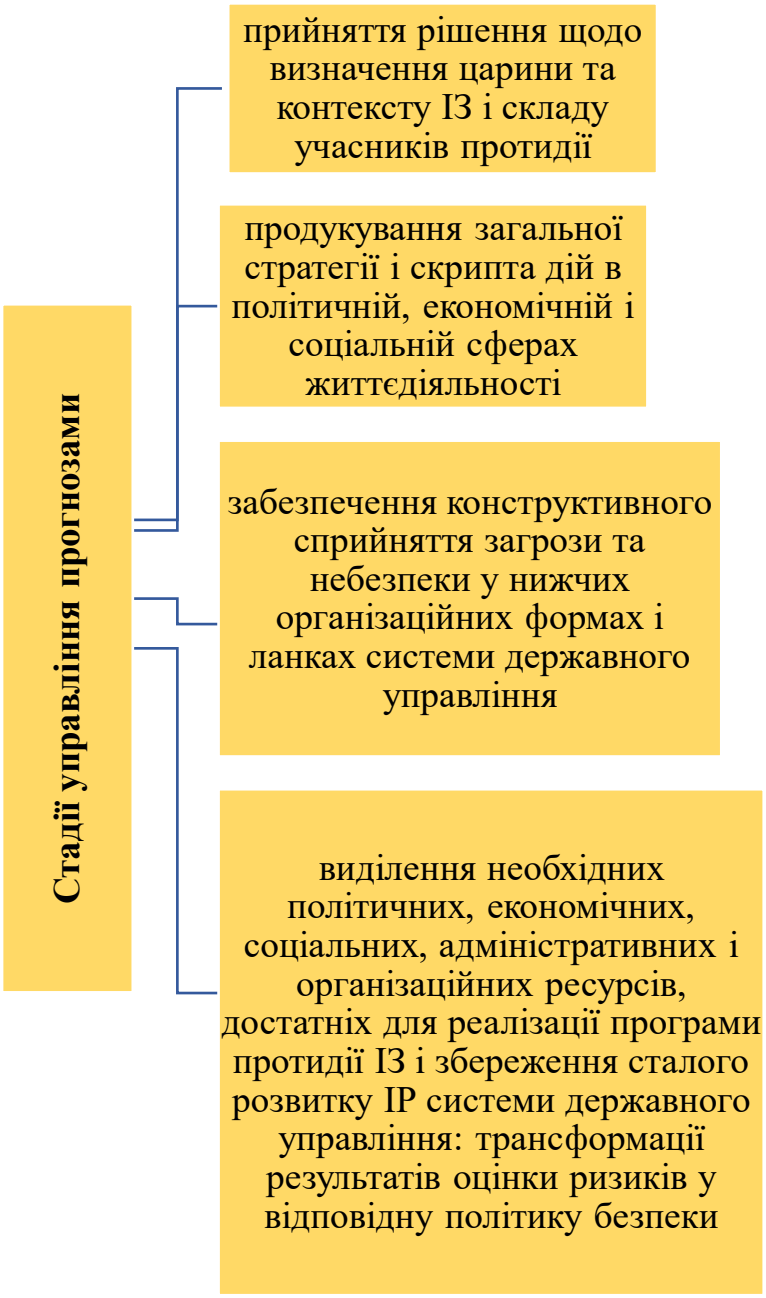


Рис 3. Стадії управління прогнозами.

Характерно, що параметризація використовуваних методів переважно корелює зі специфікою об’єкта впливу (органів державної влади, державних інституцій, ЦОВВ) та поставлених цілей. Мовиться про те, що методи діяльності громадянина детерміновані обмеженістю його впливу на поточну безпекову ситуацію та здебільшого можуть бути зведені до джерела загрози, апелювання до суспільної думки та держави, яка і має вжити рішучих заходів для його убезпечення. До прикладу, у випадку ракетної атаки, атаки дронами

тощо громадянин може піти в заздалегідь підготовлене укриття й перечекати таку атаку, якщо, звичайно, він не військовослужбовець. Навіть у останньому випадку дії такого громадянина обмежені статутом, наказами командира тощо, тобто маємо ту саму залежність від зовнішніх обставин, що і в цивільного.

На нашу думку, у контексті гібридної та інформаційної російсько-української війни помітною є тенденція, за якою суспільство актуалізує у своєму побутуванні методи соціального врегулювання. Метою останніх є надання допомоги його членам, спільнотам та іншим, які зазнали шкоди внаслідок певної загрози [283, с. 29–31]. Так, для демобілізованих громадян існують реабілітаційні осередки, соціальна підтримка та інше, натомість цивільне населення може скористатися гарячими лінія різного роду допомоги. Якщо майно громадянина України зазнало шкоди внаслідок російської атаки, то він має право на отримання відшкодування. Таким чином, релевантною умовою продукування ІБ є не лише обмеження доступу до даних (державна таємниця тощо), а й їх доступність, цілісність, фактчекінг (валідація, перевірка), які, своєю чергою, продукують захист від наявних загроз (мізінформації, дезінфорації, пропаганди тощо).

Іншим складником функціонування ІБ в актуальних умовах України є гарантування сталості інформації під час її зберігання, передачі, актуалізації тощо, тобто дотримання цілісності, неушкодженості тих чи тих даних. До прикладу, система «Оберіг» містить конфіденційну інформацію про всіх військовозобов’язаних нашої держави, яка є стратегічною, тому уряд подбав про захист цих та інших даних. Зокрема, конфіденційність такої інформації забезпечують криптографічні (шифрувальні) методи, проте вони не є стрижневою вимогою систем захисту інформації державного управління. Це пов’язано з тим, що виконання цього шифрування й розшифрування може уповільнити передачу таких даних, зменшуючи пропускну спроможність їх опрацювання. Відповідно фахівець, який працює в державній інституції, буде неспроможний своєчасно та швидко отримати доступ до потрібних даних.

Саме тому забезпечення конфіденційності має корелювати з потенційними можливостями доступу до неї. Відтак управління в царині ІБ базується на балансі між використовуваним інструментарієм щодо захисту даних і часом і складністю його актуалізації. Таким чином, СПІБ насамперед передбачає використання доступних засобів з достатнім ступенем захисту (за потреби) [209, с. 97–100]. При цьому цей захист даних не обмежений винятково апаратними й програмними методами, що засвідчено низкою дослідників.

Ефективне продукування ІБ базоване на різноманітних моделях і методах оцінки загроз, небезпек тощо, яким властива варіативність, детермінована: а) рівнем розвитку конкретної країни; б) соціокультурними детермінантами; в) корпусами аналізованих даних, диференційованих за ступенями й рівнями можливих небезпек, загроз та іншого; г) використовуваним для такого процесу алгоритмом обліку коефіцієнту ймовірності настання та розміру негативних наслідків тощо. Відтак специфіка природи, категоризації конкретних даних із цієї проблематики дає змогу доволі точно визначити ступінь потенційного впливу інформаційної зброї, рівня загроз і небезпек.

Отже, стрижневим методом аналізу інформаційних ризиків є кількісний та якісний, факторний аналіз та ін. Натомість метою якісної оцінки ризиків є критеріальне ранжування інформаційних загроз (далі – ІЗ) та небезпек, що дає можливість сформувати ефективну системи впливу на них. Окрім того, релевантним вважаємо метод критичних сценаріїв, де аналізують ситуації, у межах яких уявний супротивник паралізує систему державного управління, знижуючи її здатність до протистояння можливим небезпекам. Прикметно, що такий аналіз репрезентативний щодо самобутності розгортання інформаційних воєн, які стають органічною частиною політики НБ багатьох розвинених країн.

Згадаймо також *метод моделювання*, продуктивний для навчань з ІБ, що підтверджено позитивним досвідом США. Його суть – у проведенні таких

навчань на підґрунті однієї з відомих корпорацій, де постійно проводилися оперативно-дослідницькі тренінги. Під час останніх відбувалося моделювання різних форм інформаційних атак (далі – ІА) протягом перебігу гібридної та інформаційної війни.

Окрім того, важливу роль у дослідженні продукування ІБ посідає *метод дихотомії*, за допомогою якого можна проаналізувати актуалізовані для протидії загрозам ІБ заходи щодо здійснення відповідного впливу на них (загрози) та укріплення безпекового об'єкта. Доцільно виокремити дві віхи протидії загрозам ІБ: перша продукована сукупністю джерел загроз, друга – осередком заходів із продукування ІБ державної інституції [382].

При цьому методи впливу на галузеву інфраструктуру можна розділити на профільні (власне інформаційні) і непрофільні (неінформаційні). Показово, що профільні (інформаційні) покликані працювати з апаратними порушеннями (пошкодження інформаційно-телекомунікаційних систем, мереж зв'язку, диджиталізаційних засобів управління, систем автоматизованої обробки даних). Тобто на попередження нанесення фізичного пошкодження об'єктів і суб'єктів суспільних відносин, які перебувають під захистом. Натомість непрофільні орієнтовані на роботу із загрозами, детермінованими здебільшого інтернет-дискурсом, а відтак їх об'єктам є кіберзагрози та інші. Таким чином, ідеться про роботу із захисту даних вищезазначених реєстрів, які належать до інформації з обмеженим доступом, державної таємниці тощо.

Вибір цілей і методів протидії тим чи тим загрозам, небезпекам та іншому ІБ є важливою проблемою і складником актуалізації стрижневих напрямів профільної державної політики. У межах аналізованої проблематики доцільно виокремити варіативність дій державних інституцій (органів державної влади). Останні продуковані потребою в аналізі економічного, соціального, політичного та інших станів громадян, суспільства та держави, а також спектра можливих наслідків вибору тих чи тих варіантів здійснення такої діяльності [210; 309; 335; 342; 382].

Отже, СПІБ має інтегровану, міжвідомчу та ієрархічну природу: її структура, організація корелює з відповідними елементами державного управління із чіткою координацією дій складників СПІБ. Відповідна ефективність такої системи детермінована оптимальністю, продуманістю, наступністю та ефективністю централізованого управління з низкою локалізованих відомчо-розпорядницьких функцій, що дає змогу здійснювати моніторинг і контроль над усіма складниками національного ІПр. Натомість стрижневою особливістю СПІБ є її гомеостаз, що полягає в здатності до збереження питомих параметрів її функціонування за будь-яких ситуацій онтологічної реальності.

2.3. Державно-правовий механізм інформаційної безпеки як питомий складник сучасних політичних концепцій

Вищезазначене закономірно продукує наше звернення до питомих політологічних категорій: зокрема, поняття «політика», під яким здебільшого розуміють організаційну, регулятивну й контролюючу суспільну царину, у межах якої відбувається здійснення соціальної діяльності, спрямованої здебільшого на низку трансформаційних змін (досягнення, утримання, реалізацію та ін.) щодо влади громадян, спільнот задля вдоволення низки релевантних інтересів і потреб останніх. В. Горбатенко та Г. Лебединська [1, с. 91–96] слушно зазначають про такий складник природи політологічного категорійно-понятійного апарату, як дифузність, суть якої – у наявності широкого кола визначень стрижневих понять.

Така поліінпретаційність закономірно детермінована інтегрованістю, адаптивністю окресленого концепту, у межах якого політика репрезентована: а) однією зі сфер життєдіяльності українського суспільства; б) полісистемою, що акумулює суспільні відносини, класову взаємодію та інше; в) сукупністю дій, заходів, установ, інституцій тощо, за допомогою діяльності яких відбувається когезія інтересів різних верств населення тощо [226].

Характерно, що при цьому політика держави та інформація – взаємопов'язані, проте не тотожні явища, які перебувають у діалектичній взаємодії під час функціонування державно-правових інституцій.

Так, І. Арістова [3] акцентує увагу на тому, що «якість інформації та її доступність, сучасні інформаційні технології, що радикально збільшують обсяг і швидкість поширення інформації, викликають глибокі зміни в політиці конкретної держави, чинять суттєвий вплив на характер і системи владарювання (точна інформація підвищує ефективність влади, дозволяє вчасно скоригувати обраний напрямок дій, відреагувати на обставини, що знову з'явилися). Водночас і політичні структури впливають на інформацію, ступінь її відкритості, процеси доставки, характер передачі споживачу. Одна з найважливіших соціальних функцій влади – дозування інформації та її «пакування». На цьому засновується механізм маніпулювання громадською думкою. Найвідомішою і простою формою владного контролю над інформаційними процесами виступає цензура, коли держава за допомогою спеціально призначених та відповідальних перед нею чиновників "керує" змістом друкарських та інших інформаційних матеріалів» [2 с.12; 110].

Продуктивним способом адміністрування вищезазначеного зв'язку є система загальнообов'язкових, гарантованих державних норм, які покликані унаочнити волю уряду, виконуючи регуляторну щодо суспільних відносин функцію. Прикметно, що диджиталізаційна генеза, репрезентована глобальною інформаційною революцією, трансформувала питому мету державної влади в розробку та реалізацію концептуальних основ відповідної політики. Це передовсім відбувається шляхом ухвалення низки відповідних нормативно-правових документів з подальшим удосконаленням інформаційних відносин за участю державних інституцій. Своєю чергою, Б. Кормич [152] вважає продукування ІБ виваженою і збалансованою політикою держави в інформаційній царині, що має триєдину природу: а) захист інформаційних прав та свобод громадян; б) захист НБ в інформаційній сфері; в) захист національного інформаційного ринку,

економічних інтересів в інформаційній царині, національних виробників відповідної продукції.

Репрезентативність та продуктивність вищезазначеної структури засвідчує досвід провідних країн світу, в інформаційній політиці яких велику роль приділено узгодженій діяльності відповідного державно-правового механізму (далі – ДПМ). Ідеться про системну діяльність державних інституцій, які доповнюють одна одну у виробленні та реалізації сукупності норм і принципів права, покликаних урегульовувати й актуалізувати суспільні відносини в цій сфері [31]. Таким чином, під ДПМ ІБ доцільно позиціонувати систему взаємопов'язаних, взаємоузгоджених державних інституцій, головним завданням яких є створення умов для успішної реалізації інформаційної політики. За Б. Кормич [153], ефективність такого механізму детермінована продуктивністю кожного складника ДПМ, який має таку триєдину структуру (див. рис. 4):

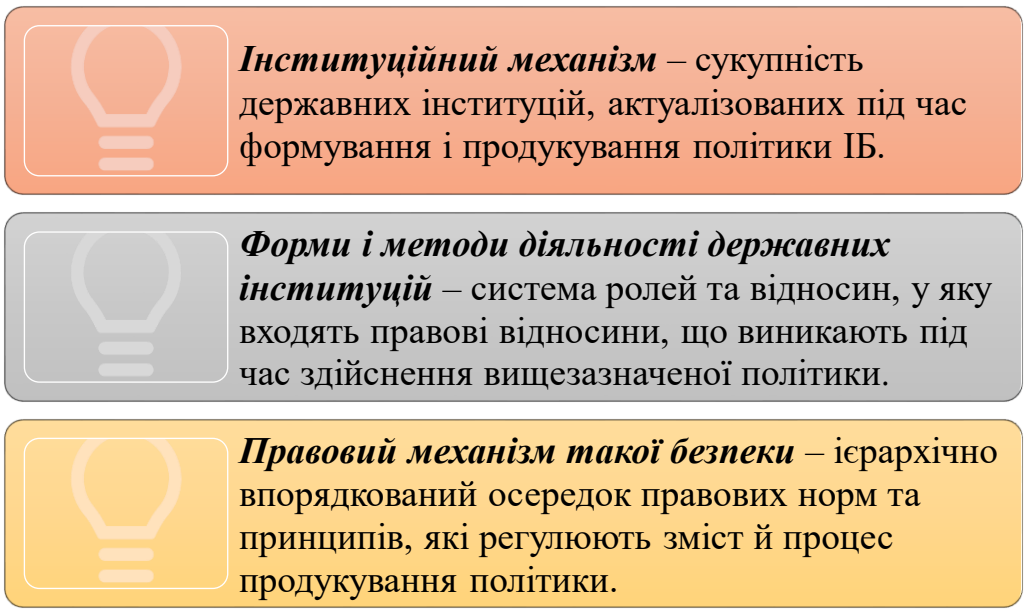


Рис. 4 Складники ДПМ (за Б. Кормич) [153].

Самобутність розвитку політики початку 90-х рр. XX ст. в інформаційній сфері була позначена насамперед розбудовою, розвитком власне технічної (апаратної) інфраструктури. Цей рух задекларований розробкою стрижневих засад щодо реалізації інформаційних прав і свобод

людини й громадянина [12, с. 289]. Водночас це засвідчує поступову зміну вектора: так, відбулася трансформація політики інформатизації на інформаційну політику. Державна інформаційна політика (далі – ДІП) є діяльністю держави у відповідній царині, спрямованою на задоволення галузевих потреб громадянина шляхом формування відкритого інформаційного суспільства.

Підґрунтям формування відкритого інформаційного суспільства є розвиток ІПр, цілісної держави та інтеграція ІПр у світовий інформаційний із урахуванням національної специфіки (особливостей, інтересів, реалій, лакун та ін.) у процесі продукування ІБ на всіх (внутрішньодержавному й міжнародному) рівнях. Відтак ІБ є інструментарієм для втілення інформаційної політики (далі – ІП), що дає підстави стверджувати, що державна політика ІБ є складником останньої. Саме тому закономірна значущість вивчення релевантних напрямів ІП щодо вироблення чітких методологічних підходів до формування СПІБ. Характерно, що структура цієї системи опосередкована напрямами державної політики щодо ІБ, а тому її (системи) детермінантою і корелянтою є ДІП, а не низка потенційних чи наявних загроз ІБ [30; 31; 32; 235; 273].

Для осягнення глибини, низки кореляцій та іншого необхідно локалізувати їх сутність та роль у структурі феномена безпеки. Отже, інституційні механізми є системою установ, правил і процесів, які виформовують сталість, неперервність тощо, безпекову стабільність у ІПр. Самобутність ролі таких механізмів в ІПр України уможливлює виокремити кілька стрижневих аспектів їх побутування (див. 5).

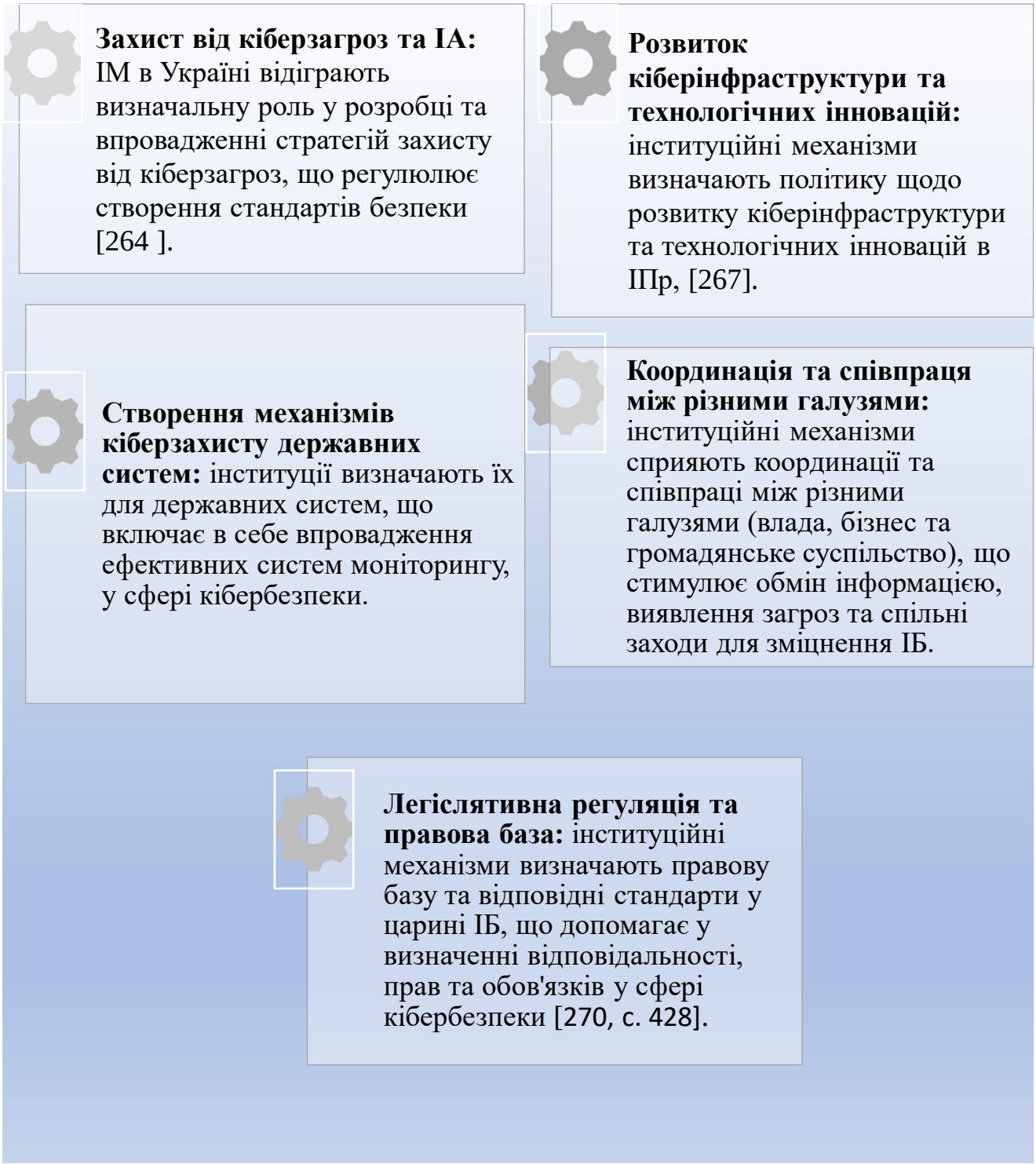


Рис. 5 Аспекти побутування інституційних механізмів.

Таким чином, задля підвищення ефективності інституційних механізмів України в продукуванні ІБ в умовах російської агресії доцільно дотримуватися низки політичних і державно-управлінських заходів у комплексі для успішної протидії загрозам і викликам, які стоять перед нашою державою. Зокрема, це: а) зміцнення співпраці між різними інституціями та секторами; б) створення

механізмів для обміну інформацією та координації заходів; в) активна взаємодія з міжнародними партнерами, обмін досвідом та ресурсами для виявлення та протидії кіберзагрозам; г) заснування високорівневого національного органу, який би координував усі аспекти кібербезпеки в країні, з визначеними повноваженнями та ресурсами; ґ) розробка та впровадження системи інформаційного управління для ефективн моніторингу й адміністрування кіберзаходів, утворення спеціальних груп для захисту критично важливих об'єктів за умов воєнного стану і війни [35].

Цим напрямам і заходам, що мають за мету сприяти функціонуванню комплексної, належної СПІБ України в умовах російського вторгнення, притаманне практично-прикладне спрямування, актуалізоване в інституційному та громадянському рівнях реалізації. У цьому контексті показовою є думка О. Волкова [72, с. 20], дослідника в царині ІБ, який вивчає правові детермінанти кібербезпеки в нашій країні, акцентуючи увагу на її правовому регулюванні. Також згадаємо М. Літинську [134, с. 296], яка досліджує проблеми ІБ та кіберправа: правовий аналіз кібербезпеки, відповідальність за кіберзлочини та інше. Натомість юридичне унормування кібербезпеки та кіберзахисту досліджено Р. Кларком [330], вплив ІПр на владу, виокремлення ролі кібербезпеки в міжнародних відносинах висвітлено Дж. Нує [372], а історію створення та впливу комп'ютерних вірусів висвітлено К. Зеттер [362]. Згадані науковці зробили значний внесок у осягнення самобутності, генези та іншого у сфері ІБ, сприяючи трансформаційним змінам стратегій, концепцій тощо захисту від кіберзагроз [382].

У контексті наявних геополітичних турбулентностей концепція ІБ набуває особливої значущості, стаючи релевантною для продукування стабільності та суверенітету тієї чи тієї країни. На сьогодні українська держава опинилася під впливом російської агресії, яка, своєю чергою, мала непередбачувані наслідки. Зокрема, відчутного впливу зазнала наукова та освітня сфери: ослаблені карантинними заходами наукові й освітні установи

продовжують страждати від тривалих вимкнень світла, ракетних атак і атак дронами.

Саме тому аналіз ДПМ ІБ є значущим на сьогодні: випрацювання категорійно-понятійного апарату є наріжним каменем репрезентації суті такого механізму й ІБ за умов інформаційної і гібридної війни. Останній визначається нами системою законів, інституцій, установ тощо, діяльність яких спрямована на забезпечення функціонування держави та захист її інтересів. Натомість поняття ІБ охоплює комплекс заходів, які мають за мету захист ІПр від потенційних та наявних небезпек, загроз та іншого, а також агресії.

У процесі аналізу такого механізму ІБ релевантними передовсім є стрижневі нормативно-правові документи та інституції, повноваження яких дотичні до їх побутування. Такий підхід є системним і репрезентативним щодо функціонування та захисту ІПр України, у межах якого гарантованою є ІБ в умовах соціальних змін (внутрішніх і зовнішніх загроз). У цьому контексті виокремлюємо такі репрезентативні нормативно-правові документи та установу (див. рис. 6):

Рис. 6 Нормативно-правові складники, релевантні для ДПМ ІБ.

Для актуалізації ДПМ ІБ України релевантною є координація заходів, визначення стратегічних напрямів, а також локалізація та передбачення потенційних загроз, небезпек та ін. Так, діяльність Держспецзв’язку є вагомою у СПІБ: зокрема, розробка й інтеграція заходів з кіберзахисту, контроль дотримання безпекових стандартів в інформаційно-телекомунікаційних системах (далі – ІТС), розслідування низки інцидентів щодо ІБ тощо. Стосовно останнього інтегрованого напряму, то тут діяльність Держспецзв’язку межує

з повноваженнями МВС, яке, своєю чергою, відіграє релевантну роль у протидії кіберзлочинності, провадячи розслідування, здійснюючи превентивні заходи для попередження кібер- та інших загроз, небезпек тощо.

Також згадаємо Раду національної безпеки та оборони (далі – РНБО) України, яка, будучи стратегічним вищим органом управління в безпековій царині, визначає пріоритетні напрями її розвитку, які вибудовують з урахуванням загально- та внутрішньодержавних інтересів, викликів тощо, які корелюють з парадигмою панівних геополітичних і технологічних тенденцій. Релевантною є і діяльність Комітету з питань НБ та оборони (далі – КПНБО) Верховної Ради України (далі – ВРУ), що є законодавчим органом, який формує та удосконалює нормативно-правову базу у сфері ІБ. Саме тому взаємодія зазначених органів покликана забезпечити суверенітет країни в ІПр та інтегрувати ефективні засоби задля досягнення окресленої мети [301, с. 8].

Диджиталізаційний вимір історіогенезу на сучасному етапі, глобалізаційні та інші процеси підкреслюють значущість протистояння російській агресії, яка є особливого роду явищем, що становить загрозу в низці соціокультурних, політичних та інших вимірів, дестабілізуючи загальну безпекову ситуацію у світі. З огляду на це ми вважаємо за доцільне локалізувати такі виміри (напрями), відстеживши самобутність їх параметризаційних особливостей в ІПр (див. табл. 2.2):

Таблиця 3

Виміри (напрями) російської агресії [118, с. 251].

Напрям	*Системна дезінформація та пропаганда*	*Кібератаки та кібершпигунство*	*Маніпулювання громадською думкою*	*Порушення кібергігієни та кіберзагрози громадянам*

Продовження таблиці 3

Параметризація	спрямована на спотворення образу України в глобальному ІПр: створення та поширення фейкових новин, які націлені на дискредитацію та продукування міжнаціональних конфліктів	інтенсивні кібератаки та кібершпигунство, спрямовані на різні об'єкти (державні інституції, критичну інфраструктуру та приватні компанії), що мають за мету отримання конфіденційних даних та порушення нормальної роботи ключових систем і функцій	використання соціальних мереж та інших онлайн-платформ для впливу громадську думку	вплив на кібергігієну громадян для отримання доступу до їх особистої інформації (фішингові атаки, тренди у соціальних мережах, які покликані локалізувати українців тощо)

Під час аналізу конкретних випадків порушення ІБ через російський вплив зауважимо продуктивність використання інтернет-дискурсу (зокрема, політичного інтернет-дискурсу) та медіа загалом. Ідеться про численні випадки актуалізації російськими агентами медіа для поширення неправдивих даних щодо мобілізації, тарифів, урядових ініціатив та ін. Так, заслуговує на увагу спроба російської влади зібрати дані про українських військовозобов’язаних шляхом створення фейкової версії застосунку «Резерв+»: цей крок розрахований на громадян із низькою медіаграмотністю.

Окрім того, постулюємо наявність впливів на політичні процеси через використання вищезазначених соціальних мереж та іншого: ці та інші спроби впливу ворога на нашу країну, природно, зазнають невдачі. Частково це пов’язано з неперервним вдосконалення українським урядом ДПМ продукування безпеки, зокрема й інформаційної: так, наявна ціла низка успішних ініціатив влади, які засвідчують високий рівень адаптивності СПІБ

України на виклики, небезпеки та ін. Зокрема, назвемо їх у хронологічній послідовності:

1. Ухвалення Закону України «Про засудження комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів в Україні та заборону пропаганди їхньої символіки» (2015 р.) [233], який забороняє публічне поширення символіки комуністичного та націонал-соціалістичного тоталітарних режимів, що має на меті убезпечення від маніпуляцій і спроб видозміни тлумачення тих чи тих історичних подій у певному ключі (пропаганди).

2. Закон України «Про основні засади забезпечення кібербезпеки України» (2017 р.) [240], який локалізує правила та заходи для захисту кіберпростору, встановлює обов'язки суб'єктів критичної інфраструктури і регулює взаємодію в цій царині.

3. Створення Національного координаційного центру кібербезпеки (далі – НЦК) (2018 р.) [237], до повноважень якого входить аналіз, координація та реагування на цей вид загроз, небезпек як стрижневий складник СПІБ (зокрема, протидії кібератакам).

4. Створення громадського проєкту «Стоп Фейк» (2018 р.), який активно виявляє та розкриває фейкові дані, уможливлює громадянам України отримувати валідовану інформацію, та ЦПД (2021 р.) [300], що продовжив цю ініціативу.

5. Активна робота в інтернет-дискурсі (зокрема, політичному інтернет-дискурсі), у межах якої наша країна актуалізує свою інформаційну присутність для протидії агресивній пропаганді (до прикладу, діяльність англійськомовного медіацентра «Ukraine: Media Center» (2021 р.)) [112, с. 15–19].

Наведені приклади репрезентативні щодо актуалізації урядом України на державному, правовому та громадському рівнях інноваційних, комплексних і ґрунтовних заходів для протидії інформаційній агресії рф. Природно, що реалізація таких ініціатив детермінована потребою у взаємодії

різних шарів, секторів, спільнот суспільства й глибокому розумінні підґрунтя медіаграмотності (суті наявних і потенційних інформаційних викликів). Саме тому аналіз фідбеку українських громадян, суспільства та уряду на інформаційну агресію корелює з використанням комплексного, інтегрованого підходу.

Реакція уряду України на інформаційну агресію є фундаментальною у плані організації захисту НБ: НЦК аналізує та продукує реакцію на кіберзагрози. Натомість розвиток нормативно-правової бази виформовує правовий фільтр для боротьби з інформаційними кампаніями (мізінформацією, дезінформацією, пропагандою та іншим) ворога. Також прикметним є активне включення громадськості, яка актуалізована в процесі виявлення таких даних та протидії їм. Зокрема, фактчекінгові ініціативи громадян (створення онлайн-платформ з відповідним функціоналом тощо) є засадничими у формуванні цілісної культури медіагромотності українського суспільства [108].

Відтак співпраця є обопільною рисою українського суспільства та уряду, проте не менш важливим складником у СПІБ є міжнародна взаємодія. Так, у царині ІБ така співпраця покликана інтенсифікувати засвоєння нових безпекових стратегій, опанування ефективного інструментарію протидії глобальним інформаційним викликам. Важливим складником є також діяльність українських медіа, які акцентують увагу на дотриманні етичних стандартів, професійної доброчесності, неупереджено надаючи громадян якісні та достовірні дані [326, с. 108–127].

Актуалізація такого інтегрованого, комплексного підходу засвідчує готовність суспільства нашої держави та його лідерів до оперативного, ефективного, ґрунтовного реагування на поточні і потенційні виклики інформаційної природи. Зокрема, ідеться про широту охоплення аспектів ІР, яка засвідчує здатність українського уряду до збереження високого рівня ІБ та відповідальності перед громадянами. Механізм державно-правого інформаційного захисту України є вдумливою полісистемою, що складається

із законодавчих та урядових ініціатив, заходів, кампаній, спрямованих укріпити національну інформаційну сферу за умов поточних і потенційних небезпек, загроз тощо. При цьому питомою метою є підвищення стійкості країни до загроз різної природи, забезпечення конфіденційності та цілісності інформації, а також розвитку інформаційної оборони як релевантного складника НБ.

Водночас аналіз ДПМ ІБ України щодо гібридної та інформаційної російсько-української війни засвідчує значущість комплексного, ґрунтовного і фундаментального підходу до безпеки в диджиталізаційному вимірі. Мовиться про такі урядові ініціативи, як утворення НЦК та ухвалення низки нормативно-правових документів, що регулюють окреслену царину та інші, які підтверджують готовність українського уряду до оперативного реагування на зазначені небезпеки, загрози та виклики.

2.3.1. Особливості національних інтересів в інформаційній царині

Самобутній розвиток сучасного суспільства позначений превалюванням ролі інформаційної царини у людському житті, що, своєю чергою, дозволяє стверджувати провідну роль інформаційної діяльності щодо диджиталізаційних змін. Головною особливістю цієї царини ми вбачаємо у її дуальній природі: з одного боку, вона є відносно самостійною, а з іншого – вторинною (допоміжною) щодо інших видів діяльності. З приводу її допоміжної специфіки, то тут мовиться про те, що окреслена царина обслуговує практично всі аспекти суспільного життя (економіку, політику, державне управління, науку, культуру тощо), тобто має підлеглий стан.

Ми вже згадували у попередньому підрозділі (див. 1.2.2) про те, що стрижневою особливістю співвідношення НБ та ІБ є продукування та дотримання національних інтересів держави (зокрема, в інформаційній царині). Таким чином, національні інтереси держави (далі – НІД) потребують окремого витлумачення, а тому ми подамо їх визначення. Так, під цими

інтересами розуміємо визначальні потреби громадянина, суспільства і держави у інформаційній царині. При тому, їх реалізація гарантує інформаційний суверенітет України, а також прав та свобод людини в вищезазначеній царині.

Це, своєю чергою, дозволяє локалізувати тріаду НІД, складниками якої стають інтереси громадянина, суспільства і держави. Саме ця триєдність лежить в основі системи таких інтересів як її покладені складники, що перебувають, до всього, у постійному русі і зв'язку одне з одним. Останнє засвідчене їх репрезентативністю як детермінант інтегрованої природи й консолідованих властивостей, що перебувають в тісному діалектичному взаємозв'язку та взаємодії. Відтак, НІД є інтегрованим виразом консолідованих інтересів громадян, суспільства і держави, ранжованих у низці трансформаційних змін (здебільшого соціокультурної природи).

Характерно, що диференціація НІД відносно об'єкта (громадянина, суспільства, держави) є доволі умовною, оскільки вона детермінована негативним впливом (роллю) загроз, які розповсюджуються одночасно на декілька чи значну кількість таких одиниць [29]. При цьому в межах цього наукового дослідження НІД становлять інтерес саме в контексті ІБ, оскільки вони репрезентативні щодо неї, водночас не всі інтереси у цій царині дотичні до її продукування.

Зокрема, аналіз Конституції України [150] узвичаєно засвідчує основні права та свободи людини в інформаційній царині: так, у ст. 15 мовиться про те, що суспільне життя в Україні ґрунтується на засадах політичної, економічної та ідеологічної багатоманітності. При цьому жодна ідеологія не може визнаватися державою як обов'язкова, а цензура заборонена. Натомість ст. 31 засвідчує гарантованість таємниці листування, телефонних розмов, телеграфної та іншої кореспонденції.

Ст. 32 унаочнює неможливість збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах НБ, економічного добробуту та прав

людини. Тим не менш, кожний громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе , які не є державною або іншою захищеною законом таємницею. Своєю чергою, ст. 34 вищезазначеного документа містить гарантію прав на свободу думки і слова, на вільне вираження своїх поглядів і переконань. Таким чином, кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір [150].

Показовим в контексті цієї наукової роботи є вищезазначений Закон України «Про основи національної безпеки України» [100], у якому доцільно виокремити, основні НІ в інформаційній царині, а саме:

1. *Для громадянина* – реалізація прав і свобод щодо одержання, використання, поширення, зберігання інформації; забезпечення права на захист від маніпуляцій індивідуальною свідомістю; право інтелектуальної власності; захист енергоінформаційної безпеки людини тощо.

2. *Для суспільства* – побудова інформаційного суспільства; забезпечення плюралізму масмедіа; захист від маніпуляції масовою свідомістю; розвиток духовності, моральних засад, інтелектуального потенціалу Українського народу, зміцнення психічного здоров’я нації.

3. *Для держави* – забезпечення інформаційного суверенітету; унеможливлення монополізації інформаційного простору іноземними компаніями або транснаціональними корпораціями; створення конкурентоспроможних інформаційних технологій та технологій зв’язку; збереження та зміцнення науково-технологічного потенціалу; інтеграція України в європейський інформаційний простір (далі – ІП); боротьба з інформаційною злочинністю [240].

Отже, вищезазначене увиразнює самобутність функціонування НІД у інформаційній царині, засвідчивши доцільність їх розгляду у призмі категорійного ряду: національний ідеал – національна мета – національна ідея

– національні інформаційні потреби – національні інформаційні цінності – НІ в інформаційній царині – національна ідеологія [29].

Своєю чергою, це дозволяє нам виокремити НІД в інформаційній царині, зокрема: а) *інформаційну стабільність* – репрезентовану стійкістю державних інституцій до внутрішніх/зовнішніх впливів; б) *інформаційну збалансованість*, яка виступає виміром ступеня інтегрованості тих чи тих інтересів груп населення країни; в) *інформаційний суверенітет*, що виявляється у недопущенні втручання засобами інформаційного протиборства у внутрішні справи України; г) *генеза України як інформаційної держави*, матеріалізована у функціонуванні останньої як повноправного суб'єкта інформаційного суспільства та інформаційної цивілізації, яка створює умови для реалізації національних інтересів в інформаційній царині у будь-якій точці земної кулі; г) *інформаційний добробут*, що виявляється у повноті задоволення інформаційних потреб населення, здатності до ефективного інформаційного розвитку; д) *забезпечення функціонування української мови як державної* (базується на положеннях однойменного Закону України [232]); е) ефективне *функціонування системи НБ в інформаційній царині*; є) *розбудова армії* з сучасною зброєю і технологіями; ж) *збереження культурних традицій народу*, його укладу життя, історичної спадщини; з) *пріоритетність загальнолюдських демократичних принципів у розбудові держави*, національна злагода та свідомість народу; и) *гарантування конституційних прав і свобод громадянина* в царині інформації; і) *підтримка інформаційно-здорового середовища*; ї) *розвиток духовності, моральних засад, інтелектуального потенціалу українського народу*, зміцнення фізичного здоров'я нації тощо через створення умов для розширеного відтворення населення; й) *інтеграція України у загальносвітовий інформаційний простір*; к) *розвиток рівноправних взаємовигідних відносин з іншими державами світу в інтересах України*; л) *формування національної доктрини ІБ на підґрунті стратегії стійкого розвитку і концепції НБ*, яка включатиме вищезазначений категорій ряд; м) *утвердження нашої країни в*

якості регіонального лідера; н) *формування позитивного міжнародного, першою чергою, гуманітарного іміджу України* [273, с. 3–9].

Отже, НІД у інформаційній царині є результатом усвідомлення цінності інформаційних потреб, усвідомленого вибору у національному масштабі, детермінованих ідеалами, метою, ідеєю тощо. Таким чином, вони формують умови, водночас надаючи засоби задоволення останніх і намічають шляхи їх реалізації. У такому контексті вищезазначені інтереси охоплюють комплекс аспектів, які мають стрижневе значення щодо функціонування громадян, суспільства та держави в інформаційному дискурсі (зокрема політичному інтернет-дискурсі [334]). Натомість їх визначення репрезентативне щодо стратегічних пріоритетів і цілей, які держава прагне досягти у царині ІБ. Зокрема, основні аспекти вищезазначених інтересів у цьому контексті включають:

– *захист державних та приватних інформаційних систем* від несанкціонованого доступу, кібератак, витоків даних та інших загроз ІБ (мовиться про захист державних даних, важливих інфраструктурних об'єктів, а також інформаційних ресурсів приватного сектора);

– *забезпечення свободи слова та преси*, що є одним зі складників демократичного суспільства (гарантування права на вільне вираження думок та доступ до об’єктивної та незалежної інформації є надзвичайно важливим для підтримки зворотного зв’язку державних інституцій з населенням, налагодження суспільного діалогу та критичного мислення);

– *захист від мізінформації, дезінформації, пропаганди тощо як вияву інформаційної війни* (розвиток механізмів виявлення та протидії дезінформації, а також сприяння інформаційній обізнаності населення [105, с. 86–96].

Відтак, національні інтереси у інформаційній царині є підґрунтям для розробки та реалізації національної політики ІБ, при цьому їх категорійна невизначеність продукує принципову відкритість розуміння цього феномена. Водночас певні категорійні обмеження (зокрема, онтологічна визначальність)

продукують формування чіткої, ефективної тощо ІБП, базою якої стають низка викликів/загроз/небезпек. Останні пов'язані з ІБ, продукуючи при цьому захист прав та свобод громадян, які у контексті сучасного інформаційного простору стають складниками національних інтересів та ІБ держави. Серед головних загроз національним інтересам у контексті ІБ доцільно згадати вищезазначені: а) кібератаки та кіберзлочинність; б) мізінформацію, дезінформацію та пропаганду; в) зловживання персональними даними (збір, продаж та інше); г) інформаційну війну [102, с. 20–26].

Отже, осягнення вищезазначених викликів/загроз/небезпек корелює з розробкою стратегій їх вияву та протидії, які, своєю чергою, є стрижневими щодо продукування ІБ та захисту національних інтересів. Характерно, що регулярна оцінка ризиків та вдосконалення заходів ІБ є необхідними для підтримки стабільності та безпеки держави у інформаційному середовищі. Натомість для захисту національних інтересів держави може бути задіяно чимало соціокультурних, управлінських та інших механізмів: що чітко регламентовано розвинутою нормативно-правовою базою України.

Отже, у цьому розділі нами висвітлено самобутність побутування ІПр щодо державно-правового механізму безпеки: проаналізовано такий простір в контексті побутування інституційних чинників, представлено його СПІБ та специфіку її роботи в контексті безпекових стратегій, а також подано особливості цього механізму як складника сучасних політичних концепцій й репрезентовано НІ в інформаційній царині. Своєю чергою, це дозволило стверджувати нагальність комплексного, фундаментального та ґрунтовного підходу й злагодженої, інтенсивної взаємодії діяльності інституційних чинників (державних інституцій).

Разом з тим згаданий ІПр позиціоновано нами стрижневим складником НБ (зокрема, розвитку ІБ), що продукує його відкритість як полісистеми, готової до змін (постійної генези, інтенсивної диджиталізації) задля зменшення впливу людського фактора на побутування інформаційних та телекомунікаційних систем. При цьому підкреслено вагу комплексу

безпекових заходів задля планомірного, поступового й логічного розвитку ІПр, що стосується, першою чергою, генези нормативно-правової бази, експонентного підвищення рівня міжінституційної координації, а також інтегрування інноваційних ІТ.

Також у розділі засвідчено міжнародне співробітництво як наріжний камінь НБ (зокрема, ІБ) України, оскільки такий напрям діяльності української влади продукуватиме: підвищення ефективності управління інформаційними потоками та захист даних; актуалізацію передового досвіду у царині НБ та ІБ, а також регулювання ІПр загалом; стратегічне планування – розробку та реалізацію довгострокових стратегій розвитку ІПр, у яких враховано не лише глобальні тенденції та специфіку розгортання, а й самобутність трансформаційних змін української держави в контексті поточної безпекової ситуації – гібридної й інформаційної російсько-української війни.

Відтак, у розділі підкреслено детермінацію вибору цілей, методів, засобів, механізмів, стратегій та іншого тими чи тим викликами, загрозами, небезпеками тощо як складниками актуалізації стрижневих напрямів ІБП. Це дозволило висвітлити інтегровану, міжвідомчу та ієрархічну природу СПІБ, структура якої корелює з відповідними елементами державного управління з чіткою координацією дій складників останньої. Відповідна ефективність такої системи детермінована оптимальністю, продуманістю, наступністю й ефективністю централізованого управління з низкою локалізованих відомчо-розпорядницьких функцій. Останні дозволяють здійснювати моніторинг та контроль над усіма вищезазначеними складниками національного ІПр. Натомість стрижневою особливістю СПІБ є її гомеостаз, що полягає у здатності до збереження питомих параметрів функціоування останньої за будь-яких ситуацій онтологічної реальності.

Вищезазначене стало підґрунтям для розуміння ІБП як дотичної до окремих аспектів організаційної культури та поведінки, у які входить робота з кадрами (навчання, підвищення кваліфікації, перепідготовка) та розробка етичних норм (стандартів, принципів та іншого) управління інформацією. При

цьому її основною метою є не лише технічних захист даних, а й продукування стійкості та відповідального ставлення до ІР серед громадян та державних службовців. Підкреслено адаптивність ІБП – властивість, що полягає у інтенсифікації видозмін диджиталізаційного складника розвитку НБ (зокрема, ІБ).

Це, природно, вимагає самобутнього підходу, базованого на протидії інформаційним загрозам агресивної політики російської федерації. У межах останньої ворогом актуалізовано комплекс заходів, механізмів, стратегій, кампаній тощо, які мають за мету занапастити ІПр України кібератаками, мізінформацією, дезінформацією та пропагандою, що актуалізують російські наративи. Значущим у цьому контексті вважаємо осягнення глибини, складності, структури й динаміки функціонування вищезазначених викликів, загроз, небезпек. Останні інтенсифікують українські стратегії, механізми тощо продукування НБ (зокрема, ІБ), актуалізуючи потребу у їх регулярній оцінці та вдосконаленні заходів, форм, методів та тому подібного ІБП задля підтримання стабільності, належного функціонування держави в інформаційному середовищі.

РОЗДІЛ 3. ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДНИК ПОЛІТИКИ ДЕРЖАВИ В УМОВАХ ВОЄННОГО СТАНУ

3.1. Диференціація загроз інформаційній безпеці як елемент сучасних політичних стратегій

Вищезазначено (див. 1.3) види ІЗ та їх дискурсивну природу, тому ми зосередимося на стрижневому понятті НБ – інформаційному суспільстві. Останнє задеклароване в розділі 13 Програми інтеграції України [250] у ЄС. У межах цього документа розвиток ІПр безпосередньо визначають *станом ІТ* (програмно-технічних засобів доступу до тих чи тих даних, телекомунікаційним складником тощо), а також кількісним і якісним складом актуальних (доступних, пропонованих, наявних тощо) продуктів. Показово, що 1998 р. ВРУ було розроблено, легітимізовано «Національну програму інформатизації України» [206]. Натомість 1993 рік позначений ухваленням «Комплексної програми створення єдиної національної системи зв'язку» [146], а 2022 рік – Закону України «Про Національну систему конфіденційного зв'язку України» [99] тощо.

Згадаємо також про роль міжнародних відносин у продукуванні НБ: наша країна є членом низки міжнародних організацій зв'язку, диджиталізаційних ініціатив та іншого: Universal Postal Union (далі – UPU), International Telecommunication Union (далі – ITU), European Telecommunications Standards Institute (далі – ETSI) [297]. Окреслене співробітництво є логічним і продуктивним, оскільки цивілізаційний вибір України продукує потребу в актуалізації найкращих взірців та стратегій розвитку країн-членів ЄС. Останній репрезентативний щодо генези всіх форм побутування суспільства (зокрема, у диджиталізаційному вимірі). Відтак актуалізація стратегії становлення інформаційного суспільства ЄС висвітлена в низці відповідних міжнародних нормативно-правових документах між ЄС і Україною.

Релевантним у контексті окресленого є підписаний 1994 р. Протокол про наміри [251] між Державним комітетом зв'язку та інформатизації України (далі – ДКЗІУ) і Генеральним Директоратом XIII (у подальшому – Генеральний Директорат ЄС з проблем інформаційного суспільства (далі – ГДЄСПІС). Цей документ виокремив стрижневі підвалини для продукування спільних дій в інформаційній царині. Трансформаційні зміни Протоколу репрезентовані в Меморандумі про взаєморозуміння між ГДЄСПІС Європейської Комісії і ДКЗІУ щодо розвитку інформаційного суспільства, який підписаний 14 вересня 2000 року [200].

У межах Меморандуму ЄС та наша країна інтенсифікують співпрацю щодо розвитку інформаційного суспільства, визнаючи його невід'ємним складником ефективної ринкової економіки, а також економіки знань [200; 203]. Українська сторона, своєю чергою, задекларувала намір динамічного розвитку програми «eUkraine» [252], що структурно і візійно відповідає потребам українського соціуму, стаючи каталізатором розвитку послуг інформаційного суспільства на нашому підґрунті. Натомість ГДЄСПІС зобов'язався надавати поради, базовані на багаторічному й багатоманітному досвіді, набутому протягом функціонування програми «eEurope» [253]. Окрім того, корисними для нашої країни були поради щодо стратегій ІС, розроблена в України, а також експертна, технічна та інша допомога в межах наявних нормативно-правових документів.

Показовими в контексті досліджуваної теми вважаємо Парламентські слухання з питань розвитку інформаційного суспільства в Україні, які відбувалися 21 вересня 2005 року. У цьому заході взяла участь велика кількість представників: народні депутати України, фахівці державних інституцій (органів державної влади), провідні дослідники та ін. Метою слухань стало продукування пропозицій, рекомендацій, випрацювання стратегій, концепцій, які потенційно мали стати планом дій у випадку ухвалення довгострокової програми розвитку інформаційного суспільства, що мала діяти безвідносно до урядових змін. При цьому головну увагу

зосереджено на відсутності послідовної державної політики в Україні, спрямованої на побудову інформаційного суспільства. Це, своєю чергою, спродукувало відставання України від інших країн, а також диференціацію сучасного інформаційного суспільства в Україні, що набуло багато вимірів: гуманітарного, масмедійного, культурологічного, освітньо-наукового та інших [178, с. 139–140].

У межах розбудови інформаційного суспільства в Україні доцільно говорити про інтенсифікацію використання інформаційних та телекомунікаційних технологій (далі – ІТТ), яка структурно може бути поділена на дві фази. У межах *першої* прискорюється побудова інформаційної та телекомунікаційної інфраструктури шляхом актуалізації зовнішніх і внутрішніх інвестицій. Окрім того, відбувається розширення конкурентного середовища з-поміж інтернет-провайдерів і постачальників мобільного зв'язку й експонентне охоплення державних інституцій та ін. Під час *другої* фази відбувається мобілізація наукових, освітніх, промислових, гуманітарних, масмедійних та інших ресурсів, а також бізнесу на стрижневих напрямах розвитку інформаційного суспільства, базованого на економіці знань [50].

Окреслена стратегія є продуктивною для нашої країни, оскільки уможливить вибудувати розвинений ІПр, конкурентоспроможний сектор інтелектуальних інформаційних технологій (далі – ІІТ) та власну, питому економіку знань. Це призведе до набуття Україною повноправного членства в полісистемі міжнародного співробітництва задля створення глобального інформаційного суспільства. Зокрема, І. Арістова [2] виокремлює такі питомі властивості розвитку інформаційного суспільства в Україні (див. таб. 3.1).

Отже, проведений аналіз історіографії та джерел (здебільшого, нормативно-правових) засвідчує пріоритетність ІБП України у створенні інформаційного суспільства, яке виступає складником генези соціально-культурного життя населення та елементом розв'язання низки глобальних соціополітичних проблем. Природно, що всі країни не можуть продукувати однаковий розвиток своїх суспільств, а відтак і набуття тим чи тим етносом

статусу інформаційного є диференційованим. Це зумовлено обсяговістю розриву між рівнями диджиталізаційних трансформацій найрозвинутіших країн та тих, що мають перехідну економіку.

Таблиця 4

Характеристики розвитку інформаційного суспільства в Україні

№	Характеристика
1.	Утворення в 90-ті рр. комерційного інформаційного сектора економіки: специфіка функціонування (структура, динаміка, зайнятість та інше) не набули достатнього розвитку у історіографії.
№	**Характеристика**
2.	Інтенсифікаці диджиталізаційних змін комерційного сектора економіки (відбувалася за модернізаційною схемою).
3.	Наявність у нашій державі стрижневих сил розвитку інформаційного суспільства: а) *пропаганда привабливого та сучасного способу життя*, позначеного інтенсивними диджиталізаційними трансформаціями (ділове спілкування, банківські операції тощо); б) *актуалізація ролі персонального комп'ютера* (далі – ПК) як необхідного засобу отримання послуг та іншого; в) *кореляція популярності ІТТ з ігровими* (малими користувачами комп'ютерних ігор, які використовуватимуть диджиталізаційний потенціал інформаційних і телекомунікаційних систем у побуті, роботі та тому подібному); г) *комп'ютеризація освіти*, яка продукує сучасність, затребуваність тощо не лише форм подання того чи того навчального матеріалу, а також його змістових особливостей, що детерміновані особливою роллю даних у інформаційному суспільстві; ґ) *здешевлення різноманітних компонентів ІТТ*, що стало рушійною силою розвитку інформаційного суспільства; д) *поширення диджиталізаційних змін*: популяризація електронних пристроїв серед населення та бізнесу в контексті ІБ; ж) *участь сільського населення в економічному, соціальному, культурному і таке інше житті* за допомогою ІТТ, що стимулює розвиток вищезазначеного суспільства.
4.	Початок «домашньої комп'ютерної революції», тобто активне впровадження ІТ у побут наших співгромадян [185; 196; 189].

Водночас процеси інформатизації є каталізаторами розвитку інших сфер суспільного життя (політичного, економічного, культурного та інших його

вимірів), окреслений розрив може лише зростати із часом. Специфічним розв'язанням цієї проблеми є інформаційне суспільство як самобутній інструмент глобалізаційної онтології: воно є певною асоціацією країн, які досягли рівня d окреслених вимірах. Одним з основних показників такого зростання є диджиталізаційний рівень тієї чи тієї країни, який, своєю чергою, корелює з розвитком науки, освіти, культури, соціальної царини та інших сфер, інтегрованих у світову економіку [36, с. 26–27].

Зокрема, стрижневими параметризаційними особливостями такого суспільства є: а) наявність ІКТ та технологій зв'язку; б) актуалізація інноваційного потенціалу науки; в) набуття фізичними та юридичними особами даних і розбудова ефективної інфраструктури їх надання; г) високий ступінь інформаційно-правової культури всіх суб'єктів інформаційних відносин; ґ) матеріально-технічне забезпечення адміністративних та інших послуг, детермінованих обміном даних [67, с. 161–162]. Природно, що процес становлення інформаційного суспільства в нашій країні має свою тривалість, етапність, складнощі та інше, проте його розгортання, інтенсифікація детерміновані світовими тенденціями й обраною зовнішньополітичною стратегією.

Доцільно в цьому контексті згадати про ІБ як складник та середовище для генези інформаційного суспільства: остання, безумовно, є елементом загальної безпекової стратегії, політики, а тому стрімко розвивається у всьому світі й Україні. Передовсім виявом такої безпеки є диджиталізаційні трансформації, які охоплюють усі державні сфери (економічну, воєнну, політичну, промислову, культурну та інші). ІБ в такому розумінні має свою самобутню параметризацію, структуру тощо, а відтак – і загрози, які можуть порушити фізичну (апаратну) та змішану (програмну) природу останньої.

Така пильна увага до ІБ, її значущість засвідчена вже згадкою про неї в Конституції України [150], у тексті якої це поняття актуалізоване поряд зі суверенітетом, територіальною цілісністю, економічною безпекою тощо. Згідно з документом, ІБ належить до питомого функціоналу держави і

досягається шляхом актуалізації сучасних ІТ, розбудовою параметризаційно повної національної інфраструктури й генезою інформаційних відносин [150].

Так, Закон України «Про основи національної безпеки України» [239] декларує спроби маніпулювання громадською думкою як одні зі стрижневих загроз НІ та НБ. Мовиться про актуалізовані рф мізінформацію, дезінформацію та пропаганду: поширення недостовірних, неповних, заангажованих та інших даних. Водночас ст. 3 Закону України «Про інформацію» [95] і Закон України «Про концепцію національної програми інформатизації» [236] висвітлює основні напрями державної інформаційної політики, які детерміновані: а) доступом кожного громадянина до інформації; б) спектром рівних можливостей щодо роботи з даними (збиранням, продукуванням, поширенням, охороною, захистом та ін.); в) формуванням умов для розвитку інформаційного суспільства; г) забезпеченням прозорості діяльності державних інституцій та суб'єктів владних повноважень; ґ) створенням ІКТ і мереж інформації, диджиталізацією тощо та д) розбудовою, оновленням, розвитком, зберіганням національних ІР; е) продукуванням ІБ України й є) інтенсифікацією міжнародних відносин в інформаційній царині з подальшим її входженням до світового ІПр.

Продукування нормативно-правових документів – не єдиний напрям ІБП: окреслений вектор розвитку реалізовано шляхом діяльності державних інституцій, а також інститутами громадянського суспільства. До компетенції останніх входить низка питань щодо створення безпечних умов побутування, розвитку та диджиталізації інформаційної царини. Безпосередньо склад механізму ІБ визначений нормами ст. 4 Закону України «Про основи національної безпеки України» [239] та Закону України «Про основні засади забезпечення кібербезпеки України» [240]: Президент України, ВРУ, Кабінет Міністрів України (далі – КМУ), РНБО України, міністерства та інші ЦОВВ, Національний банк України (далі – НБУ), суди загальної юрисдикції, прокуратура України, місцеві державні адміністрації (далі – МДА) та органи місцевого самоврядування (далі – ОМС), ЗСУ, СБУ, Державна прикордонна

служба (далі – ДПС) України й інші військові формування, утворені відповідно до законів нашої країни.

Функційна самобутність державних інституцій корелює з проблематикою ІБ, яка позначена зміною в повноваженнях і статусі РНБО України. Так, згідно ст. 107 Конституції України, він є координаційним органом з питань НБ і оборони при Президентові України [235]. Значущість параметризаційної специфіки діяльності СБУ ми згадували в попередньому розділі (див. 2.1): ця установа є державним правоохоронним органом спеціального призначення, безпосередньо відповідальним за безпеку нашої країни [276]. Вагомою в цьому контексті вважаємо діяльність Міністерства інформаційної політики (далі – МІП) України [97], покликане захищати ІПр від мізінформації, дезінформації та пропаганди, а також координувати діяльність приватних медіа щодо надання даних громадян на окупованих територіях.

Наявний механізм ІБП, природно, не є досконалим, що, наприклад, засвідчує факт захоплення ІПр Криму, Сходу та Півдня України. Це стало підґрунтям російської окупації Автономної Республіки Крим (далі – АРК) та подальшого розвитку «спеціальної воєнної операції» (термін російської влади; далі – СВО) у Донецькій та Луганській областях, що спричинило повномасштабну російсько-українську війну.

Прикметно, що виявом російської експансії стала й інформаційна (заміна постачальника мобільного та іншого зв’язку російськими), адміністративна (заміна паспортів українських громадян російськими), культурна (стрімка розбудова розважальної інфраструктури, що мала підґрунтям усе російське: твори, авторів та інше) тощо. На сьогодні цілеспрямована й фундаментальна діяльність рф зумовлює соціальну напруженість і подекуди ідеологічне протистояння: формування антиукраїнських настроїв з-поміж нашого населення, меншовартість і дискредитацію всього українського [217, с. 319].

Дослідник О. Шаповалов [304] вважає, що складником реагування на цю проблему є розбудова загальнодержавної системи інформаційної (зокрема, кібернетичної) безпеки України, структурна самобутність якої має полягати в інтегруванні питань захисту суверенітету та просування українських НІ. Функціонування цієї системи продукує: а) *трансформаційні зміни нормативно-правової бази*: її розвиток, суголосно диджиталізаційним трансформаціям і категорійної генези ІБ; б) *виформування (визначення, локалізація) її стрижневого органу в структурі державних інституцій*, який би координував та інтегрував їх діяльність у царині ІБ; в) *виокремлення низки суб'єктів (державних інституцій, інституційних чинників)*, у повноваження яких входить відстеження поточного стану, динаміки, прогнозування ІБ; г) *інтенсифікація наукових досліджень* задля визначення ресурсних лакун у забезпеченні окресленої системи: кадрових, фінансових та ін.; ґ) актуалізація заходів у Міноборони України, Генеральному штабі ЗСУ зі створення полісистеми ІБ як складника національної системи ІБ [304, с. 189].

Таким чином, захист НІ України передбачає моніторинг стану безпекових систем (зокрема, ІБ), які є базою зміцнення державності. Так, збалансована ІБП України є складником соціоекономічної політики, у межах якої актуалізована пріоритетність НІ та загроз НБ країни. Природно, що підґрунтям такої системи є засади правової демократичної держави, які інтегруються шляхом розробки й реалізації відповідних національних доктрин, концепцій, стратегій, скриптів та програм згідно із чинним законодавством.

У розділі 1 наукової роботи ми згадували низку нормативно-правових документів (Закони України: «Про Державну службу спеціального зв'язку та захисту інформації України» [90], «Про державну таємницю» [92], «Про захист інформації в інформаційно-телекомунікаційних системах» [97], «Про інформацію» [95], «Про основи національної безпеки України» [100] та «Про національну безпеку України» [98] тощо), які охоплюють весь спектр проблем продукування ІБ держави. Виокремлюємо такі два ключові документи, як

«Стратегію національної безпеки України» [244] та «Доктрину інформаційної безпеки України» [243], а також Конвенцію про кіберзлочинність [148], ратифікованою ВРУ.

Водночас система нормативно-правових документів, релевантних щодо регулювання відносин в інформаційній царині, переважно обмежена винятково декларативними нормами, що зумовлює потребу в її трансформаційних змінах, які уможливлюють адаптувати таку систему в диджиталізаційному вимірі. Зокрема, мовиться про концептуальну перебудову системи державного управління та інформаційної полісистеми, що в такому контексті є її складником [123, с. 124]. Отже, удосконалення нормативно-правового супроводу СПІБ за умов гібридної та інформаційної російсько-української війни доцільно розглядати стрижневим напрямом, спрямованим на захист інтересів громадян України, суспільства та держави.

Історіографію інформаційної царини докладно висвітлено в розділі 1, тому акцентуємо лише на значущих для нашого дослідження публікаціях, у яких представлено динаміку ІПр України. До таких відносимо працю Д. Зубкова, де проведено аналіз соціальних мереж та їх ролі в поширенні даних (зокрема, неправдивих) під час російської агресії [120]. У праці М. Золотової вивчено самобутність інформаційної російсько-української війни та її кореляція щодо побутування українського суспільства [119]. З-поміж зарубіжних дослідників назвемо науковий здобуток Т. Снайдера [383], де вивчено історію та сучасні події в Східній Європі з екстраполяцією на російську агресію та інформаційну війну в Україні, А. Еплбаум [317], у якому схарактеризовано історіогенез та актуальні події в нашій країні: зокрема, гібридну та інформаційну війну і пропаганду [119; 378; 383].

Трансформаційні зміни ІПр України є репрезентативними і вимірюваними в низці фундаментальних, ґрунтовних досліджень, активних обговорень та ін. Так, від початку 2014 року – першого російського вторгнення на територію України – ІПр нашої країни зазнав низки трансформаційних змін, спродукованих відчутними впливами. У цьому контексті дедалі більшої

значущості набуває проблема кореляції впливу гібридної та інформаційної російсько-української війни на суспільство нашої держави, а також країни-агресора.

Уже перед початком російської агресії цей простір перебував у стані змін та напруження, яке було локалізоване ще 2013 року (під час укладення Україною Угоди про асоціацію з ЄС [250]). Саме це рішення стало наріжним каменем, що зумовило протести на Майдані Незалежності в Києві, спричинивши падіння режиму В. Януковича. Ця подія стала символом боротьби за демократію та незалежність, що особливо показово в контексті аналізу складної ситуації в Україні щодо ефективного реагування на виклики, пов'язані з російсько-українською війною. Прикметним явищем стала тривала й самобутня історична динаміка трансформаційних змін ІПр України, що увиразнює його глибокий контекст і значущість дослідження [78, с. 96].

Ідеться насамперед про активне інтегрування України у глобальну інформаційну інфраструктуру (далі – ГІІ), репрезентативне щодо її відкритості в царині ІТ. Водночас актуалізація ІКТ, які не завжди відповідають високим стандартам, продукує наявність низки труднощів, спричинених невідповідністю витраченого фінансування вихідного продукту, що має вразливість до ІЗ, до того ж ІВ здебільшого розгортається між різними суб'єктами (або системами таких суб'єктів, актуалізованими в різних верствах/ спільнотах), включаючи країни, міжнародні та транснаціональні корпорації, фінансові групи, терористичні й кримінальні організації. Такі взаємодії виформовують складну природу ІПр, у межах якого Україна змушена виявляти гнучківсть, адаптуватися, захищаючи власні НІ та продукуючи свою ІБ. Природно, що ІПр репрезентативний щодо трансформаційних змін та їх спектра, а також диференціації його впливу на різні шари українського суспільства.

Наша країна перебуває під впливом низки міжнародних акторів, одним з найрелевантніших з яких, закономірно, є російсько-українська війна. Показовою в цьому контексті є роль рф, яка декларує свою правонаступницьку

роль щодо СРСР. Дійсно, ця країна отримала певний спадок СРСР, проте, не маючи достатньо ресурсів, на відміну від нього, набула низки обмежень свого впливу в тих чи тих регіонах світу. Характерно, що вищезазначене є елементом дискурсу, який витлумачує російсько-українське протистояння в новому світлі, у межах якого інформаційні стратегії та тактики актуалізовані для впливу на громадську думку й політичні процеси [28, с. 81–84].

У табл. 3.2 репрезентовано стрижневі аспекти та сторони російсько-української війни на базі SWOT-аналізу, що спрощує комплексне оцінювання ІБ України: виокремлення сильних та слабких сторін держави у ІПр:

Таблиця 5

SWOT-аналіз інституційних чинників інформаційної війни рф проти України

S (сильні сторони)	W (слабкі сторони)
1. Об'єднання країн у військово-стратегічному плані. 2. Реформування органів державної влади, створення концепції розвитку сектора безпеки і оборони України. 3. Активізація в Україні національної системи кібербезпеки та нормативно-законодавчої бази для її продукування. 4. Вияв загальнонаціональної свідомості та самоідентифікації як етносу. 5. Зміна психологічного настрою українців щодо інформаційного впливу. 6. Доступ до європейських країн. 7. Створення МІП як головного органу контрпропаганди. 8. Експорт (транзит) газу через територію України, спільність кордону.	1. Контроль рф над всім Чорноморським регіоном, а також Кримським шельфом і відмінною туристичною зоною. 2. Науковий потенціал рф у диджиталізаційному та зв'язковому вимірі: інформаційно-телекомунікаційні компанії, провайдери зв'язку, чат-боти, бот-ферми, спільноти, штат співробітників та інше. 3. Низька конкурентоспроможність України та її інформаційної продукції на світовому ринку. 4. Державний борг України за газ перед рф. 5. Брак спеціалістів інформаційної інфраструктури, телекомунікаційних засобів і технологій в Україні. 6. Зрадництво, колаборанство серед частини населення нашої країни. 7. Конфліктогенна зона на території України (ДНР, ЛНР, АРК). 8. Слабка комунікація між державними інституціями та громадянським (інформаційним) суспільством, низький

Продовження таблиці 5

	рівень захисту від несанкціонованого доступу до даних (з використанням іноземних ІТ).
О (можливості)	**Т (загрози)**
1. Стимулювання в Україні впровадження новітніх ІТ для підвищення її конкурентоспроможності. 2. Зменшення контенту російських медіа у ІПр України. 3. Створення національних стандартів, технічних регламентів застосування ІКТ за міжнародними стандартами. 4. Забезпечення технологічної конкурентоспроможності України у сфері інформатизації та зв'язку. 5. Зворотний ефект ІВ щодо того, що український уряд використовує громадян «у сліпу». Суть останнього у тому, що через вкид такої кількості негативної інформації вона трансформується у свою протилежність, викликаючи замість засудження підтримку. 6. Потенційний вступ України в Євразійський економічний союз та повноправне членство у НАТО. 7. Створення системи швидкого реагування на інформаційні атаки, спеціальних підрозділів сектора безпеки.	1. Загальна інфляція. 2. Спроба нав'язування правового нігілізму свідомості українського населення. 3. Придушення волі українців, знищення віри у перемогу, поширення паніки та іншого. 4. Соціально-економічна криза продукує нестабільність біля кордонів рф. 5. Зменшення території України, втрата людських, земельних, водних ресурсів, а також низка економічних втрат та тому подібне. 6. Поширення у зарубіжному ІПр російської мізінформації, дезінформації та пропаганди, які несуть шкоду НІ України. 7. Незахищеність великої кількості баз даних, зокрема – персональних даних громадян. 8. Негативні впливи, спрямовані на підрив конституційного ладу, територіальної цілісності та недоторканності кордонів нашої країни. 9. Загроза України втрати суверенітету.

Відтак, гібридна та інформаційна російська-українська війна стала одним з найсерйозніших викликів у історії нашої країни. Першою чергою, мовиться про систематичні порушення рф принципів міжнародного права: актуалізацію інформаційно-психологічного впливу (мізінформації, дезінформації та пропаганди). Останній покликаний консолідувати

деструктивні тенденції в українському соціуму, а також виправдати агресивні дії ворога на міжнародній арені. Україна, своєю чергою, відшукує шляхи ефективної протидії вищезазначеному впливу, намагаючись ефективно використати наявну ситуацію й мінімізувати її негативні наслідки: економічну скруту, соціально-психологічні збитки, втрату територій та інше.

Природно, що вищезазначені складники є безпосередніми загрозами НБ України, оскільки вони занапащають її конституційний лад, суверенітет, територіальну цілісність, недоторканість кордонів та інше. Разом з тим, поточна ситуація (інформаційна та гібридна російсько-українська війна) продукує появу низки нових можливостей для нашої країни. Так, ми говоримо про: а) інтенсифікацію диджиталізаційних змін; б) появу систем валідації, фільтрації та іншого даних; в) виформування національних стандартів актуалізації ІКТ згідно міжнародних норм [68] тощо.

Йдеться про те, що активно використання рф низки медіа-ресурсів й актуалізація нею численних інформаційних кампаній та іншого, натомість спричиняє інтенсифікацію СПІБ (зокрема, у окресленій частині роботи з даними). Характерно, що такий активний вплив російських кампаній природно познавчився на роботі українських медіа: частина з них не витримала такого тиску, інша – змінила редакційну політику, чинячи супротив [307, с. 182]. Так, стрижнева параметризаційна властивість будь-якого ІПр, – формування громадської думки, – динамічно використовувана російським урядом задля реалізації низки завдань (див. рис. 7):

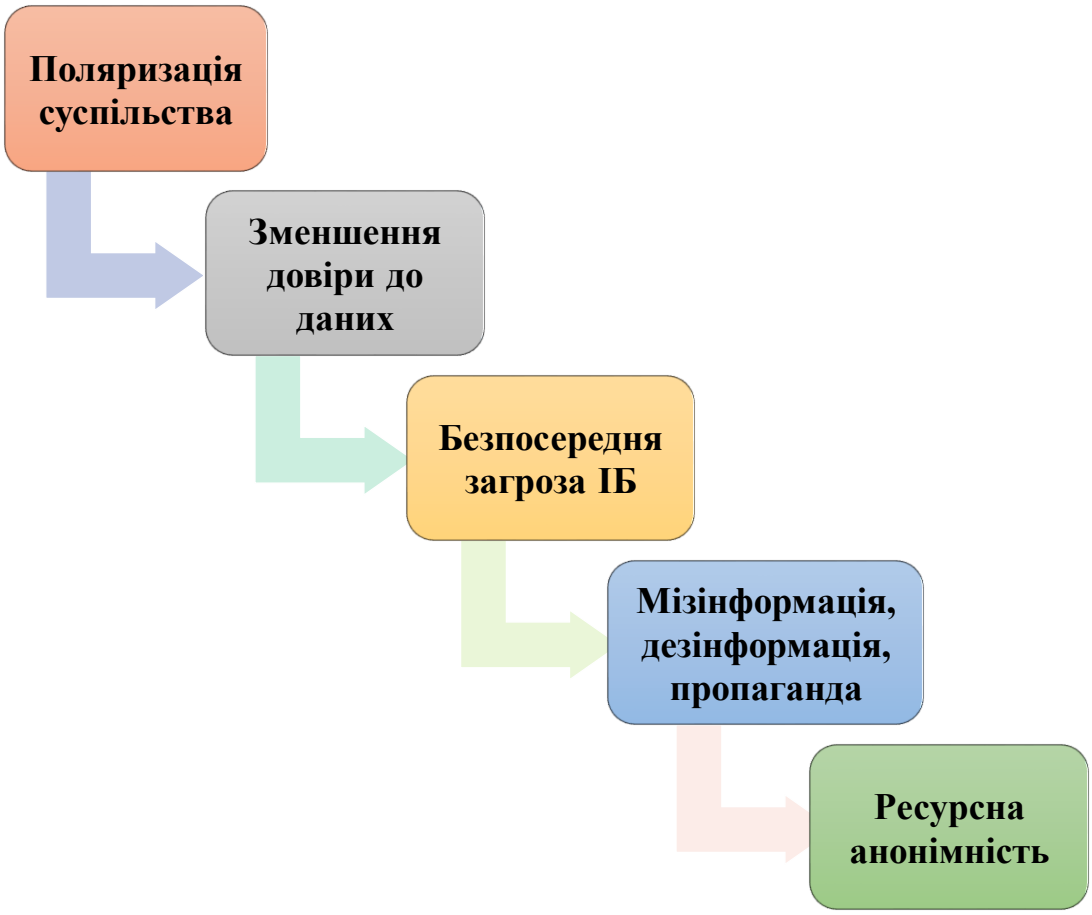


Рис. 7 Параметризація російського впливу на ІБ України (2010–2024 роки).

Отже, як видно з рис. 7, параметризація російського впливу на ІБ України (2010–2024 роки) мала такі складники: а) *поляризація суспільства*: продукування конфліктогенного середовища в українському суспільстві (зростання конфліктних розривів між громадянами, угрупуваннями, партіями тощо); б) *зменшення довіри до даних*: спричинене наявністю взаємовиключної інформації, наслідком чого стає зменшення загальної довіри до неї; в) *безпосередня загроза ІБ*: позначена глобальним дестабілізаційним впливом на ІПр, що детермінує всі напрями побутування українського соціуму (економічний, культурний, освітній та ін.); г) *мізінформація, дезінформація, пропаганда*: актуалізовані шляхом використання низки алгоритмів оперування даними для підвищення поширення антиукраїнських наративів та ін.; г) *ресурсна анонімність*: використання невідомих або прихованих джерел поширюваних даних («надійні джерела» тощо) для інтенсифікації

деструктивного впливу на населення через виформування теорії змови українського уряду, прихованості наданих даних, актуалізації «утаємничування» у ті чи ті неправдиві дані.

Зазначимо, що під час дослідження цієї проблематики було взято до уваги самобутність ІВ рф проти України в період з 2014 року і до сьогодні. Це дало змогу систематизувати й виокремити наймасованіші ІА країни-агресора [193, с. 252, 256]. ІА рф актуалізують широкий спектр дій (кібератаки, психологічне насилля, втручання в соціум та ін.). Головною властивістю ІА є їхня природа щодо ІБ, якій вони становлять особливу загрозу: так, кібератаки можуть порушувати функціонування критичних мереж тощо.

Для якнайкращого розуміння параметризації (динаміки, етапності, структури та іншого) ІА проаналізуємо їх приклади в медіа. Так, рф використовує інформаційні стратегії для створення образу своєї важливості на міжнародній арені та просування іміджу свого президента як символу «останньої істини». Також простежуємо спроби переконати населення в тому, що без участі рф жодна сфера діяльності не може бути успішною чи приносити позитивні результати [267; 272]. Натомість трансформаційні зміни ІПр, викликані ІА, репрезентативні щодо потреби в постійному вдосконаленні системи ІБ та підвищенні медіаграмотності громадян. Відтак аналіз методології ІВ є релевантним у контексті осмислення сучасного конфлікту в Україні та розробки низки стратегій ефективного продукування ІБ.

Зокрема, показовою є чутливість українського інтернет-дискурсу (політичного інтернет-дискурсу) до ІА, що спричинена низкою детермінант його побутування. Стрижневою проблемою тут є відсутність ефективних моніторингових, фактчекінгових та інших систем не лише за створенням і функціонуванням тих чи тих медіа [161; 234], а й за продукованими ними наративами. Окрім того, згадаємо проблему вільного доступу до супутникового мовлення, що функційно може бути використана для поширення інформаційного впливу. Також вагому роль відіграє ефективність боротьби з кіберзагрозами (вірусами, троянами та ін.) і рівень підготовки

медіаспеціалістів щодо ефективної протидії ІА. Релевантною є і відсутність належної інформаційної бази стратегічних і тактичних знань щодо перебігу ІВ, що також підвищує вразливість нашої країни [285].

Саме тому особливу увагу нашому уряду доцільно зосередити на розробці низки ефективних засобів для протидії російській інформаційній агресії та підвищення рівня медіаграмотності населення України. Частково останнє десятиліття підтвердило вищезазначений курс українських посадовців, які виформовують достойну відповідь на виклики гібридної та інформаційної російсько-української війни. Здебільшого це відбувалося шляхом якісного підвищення рівня ІБ: зокрема, такі заходи включали акцентування уваги громадян на вагомих віхах (див. рис. 8):

Рис. 8 Віхи ІБ в Україні [163; 305, с. 15–27;].

Так, реакція української влади на вищезазначені виклики засвідчує релевантність окресленого питання в полісистемі НБ: зокрема, захисту ІПр країни та інформаційного суверенітету [289]. Натомість трансформаційні зміни ІПр під час воєнного стану є динамічним, диференційованим процесом, у якому криється низка викликів, загроз і небезпек, із якими український громадянин стикається щодня, а тому повинен вміти з ними правильно

взаємодіяти, оскільки не лише фізичні загрози є вагомими під час війни. Водночас не тільки локальний (рівень громадянина), а й державний (національний рівень) вагомий у СПІБ, позаяк саме в його межах детермінований ІПр під впливом російської агресії.

Природно, що вагомими викликами, загрозами та небезпеками залишається ІА (мізінформація, дезінформація, пропаганда) та кіберзагрози. Відзначимо в цьому контексті експонентне адаптування українського суспільства до таких загроз у проміжку 2022–2024 років. Так, після початку повномасштабного російського вторгнення відбулося радикальне зменшення споживання контенту ворога, тенденція до переходу на українську мову частини російськомовних громадян та інші віхи ІПр України.

Генеза ІПр нашої країни під час гібридної та інформаційної російсько-української війни засвідчила продуктивність актуалізації обраної урядом стратегії. Низка запроваджених заходів, відповідей та іншого (до прикладу, диджиталізаційний вектор розвитку, який дав змогу зберегти бази даних тощо) передбачала зміцнення ІБ: кіберзахисту, розвитку медіаграмотності, міжнародного співробітництва тощо. Окрім того, Україна активно розробляє стратегії протидії інформаційним кампаніям ворога, покликані зберегти її інформаційну незалежність. Загальний вектор нашої країни засвідчує інтегрованість і спрямованість розвитку СПІБ, що, своєю чергою, є підґрунтям стійкості й протидії впливу російсько-української війни.

3.2. Інформаційна війна як складник гібридної війни в умовах російської агресії в Україні

2014 року Україна зазнала воєнної агресії з боку рф, у межах якої відбулося анексування АРК, а згодом – продукована загроза втрати Донецької та Луганської областей. Проте ще задовго до безпосереднього збройного конфлікту проти нашої країни було розпочато ІВ [4]. У цьому контексті слушною є думка М. Маклюєна [51]про те, що економічні зв’язки, відносини

зазнають низки трансформаційних змін, перетворюючись на обмін знаннями, а не товарами. Своєю чергою, видозмінюється уявлення про медіа, які постають «природними ресурсами», що примножують потенційні можливості, вагу та інше того чи того суспільства [51]. Показовою нам видається концепція біосфери В. Вернадського [140], що декларує значущість тих чи тих досліджень, а також матеріалізації їх результатів у вигляді певних смислових еманацій.

Сказане прикметне щодо ІВ як феномена, досліджуваного М. Лібікі [169], який зазначав, що її завданням є знищення соціуму ворога. Натомість Г. Почепцов [228] підкреслював самобутність інформаційного суспільства, яку він вбачав в актуалізації останнім не дій в онтологічній реальності, а в інтернет-дискурсі. Наголосимо на доволі великому корпусі праць, присвячених темі ІБ, що пояснюється тим, що інформаційні кампанії рф увиразнили лакунізованість українського ІПр і стали предметом багатьох досліджень. Водночас окреслені кампанії локалізували недостатній ступінь сформованості науково-методологічної категоризації, алгоритмів дій та іншого, а також засвідчили потребу в координації діяльності державних інституцій.

Саме тому важливим, на нашу думку, є розуміння питомої дефініції «інформаційна війна», яка була вперше згадана 1985 року в Китаї. Підґрунтям цього поняття китайські дослідники поклали погляди давнього полководця Сунь-Цзи, який першим зауважив дієвість інформаційного впливу на супротивника. У своєму творі «Мистецтво війни» він писав про те, що здобуття перемог у боях – не вершина воєнного мистецтва, а ось підкорення супротивника без них є довершеною досконалістю [39, с. 155]. Натомість Д. Прокоф'єв визначає аналізоване поняття як спрямовані на досягнення певної інформаційної переваги дії, реалізовані шляхом завдання шкоди тим чи тим даним, аналітичним процесам супротивника. Це відбувається паралелізовано, на думку дослідника, із захистом власних даних та процесів, детермінованих їх функціонуванням. При цьому основними методами ІВ є

блокування, спотворення та перекручення наявних даних задля перешкоджання ухваленню тих чи тих рішень супротивника [190].

Прикметно, що перебіг стратегічних ІВ вирізняється самобутністю використовуваних засобів (тут – зброї): вона не завдає фізичної шкоди, проте спричиняє вагомі наслідки. Так, за визначенням В. Маркоменка [194], ІВ характеризує комплексність вжитих заходів. Мовиться про особливу методологію, застосовану для різних операцій (заходів), актуалізованих у певних ситуаціях (здебільшого – конфліктних), де дані набувають статусу зброї, ресурсу і мети. При цьому активно терміном ІВ почали послуговуватися з 1976 р.: деякі джерела називають Т. Рона [341, с. 180], який у звіті для компанії «Боїнг» акцентував увагу на тому, що інформаційна інфраструктура стає стрижневим економічним елементом. Така інтегрованість, на думку дослідника, робить її потенційною мішенню для різного роду атак. Метою ІВ є послабленням моральних і матеріальних активів ворога / конкурента з паралельним зміцненням цих позицій у себе. Питомою ознакою ІВ у такому розумінні стає пропагандистський вплив на свідомість людини в ідеологічній та емоційній сферах.

Отже, ІВ є, по суті, складником ідеологічної боротьби, у межах якої неминучими побіжними наслідками стає фізичне винищення: руйнування об’єктів воєнної та цивільної природи, смерті тощо. Доволі важким є питання наслідків ІВ для психіки людей, спільнот і суспільства загалом: це пов’язано з тим, що масштаби і значення останніх співвимірні з обсягом шкоди класичних воєн, а інколи й перевищують їх. Ще в біблійній легенді актуалізований такий воєнний прийом: так, Гедеон часто вдавався до залякування ворогів та одного разу зумів це зробити настільки майстерно, що супротивник вдарив по своїх військах [177].

Зокрема, інформаційний вплив на стан супротивника (моральний, емоційний та ін.) знаходимо і в Давньому Римі, і в період феодалізму та пізніший час [128, с. 20–22]. Показовими в контексті нашої наукової роботи є 20-ті рр. ХХ ст., коли ІВ набувають самостійного розвитку, відокремлюючись

від класичних. До прикладу, німецько-австрійська радіовійна 1933–1934 рр. з приводу приєднання Австрії до Третього рейху (саме в той час виформувалось поняття «інформаційний агресор») [281]. Інтенсивного розвитку набула ІВ під час Першої та Другої світових воєн. Під час Першої світової війни питома роль друкованих медіа та жорстка цензура мали значний вплив на громадську думку, витворюючи дезінформаційне середовище. Під час Другої – ІВ набула загрозливіших масштабів: згадаємо методи пропаганди Третього Рейху та радянських спецслужб. Відзначимо експонентно щораз більшу роль ІКТ у перебігу війни: у Японії з'явився культ «камікадзе» (божественного вітру), покликаний здійснювати психологічний тиск на ворога. Окрім того, притаманною тому періоду була профілізація: зокрема, Великобританія (1941 р.) заснувала відповідний підрозділ, США (1942 р.) сформували відділ військової інформації тощо.

На увагу заслуговує побутування Організації українських націоналістів (далі – ОУН) та Української повстанської армії (далі – УПА), що актуалізували пропагандистські технології в процесі своєї роботи з імперським пануванням [143, с. 82]. На думку М. Нагірняка [157], весь період визвольної боротьби відзначався динамічним протистоянням з тоталітарним режимом, важливим складником якого була ідеологічна кампанія, що можна позиціонувати елементами психологічної війни. Використання методів впливу ОУН та УПА мало широкий спектр: від тривалих політичних кампаній до одноразових політичних акцій (зокрема, бойкоти виборів, зрив мобілізаційних заходів та ін.).

Вищезазначене закономірно інтенсифікувало генезу ефективного інструментарію для проведення ІВ, випробуваного рф у збройних конфліктах у Чечні, Грузії та згодом в Україні. Цей період позначений появою нової методології ІВ (мовиться про вдосконалення пропаганди, психологічних операцій та інших тактик). Натомість XXI століття видозмінило параметризацію ІВ і самобутність її впливу на історіогенез, що засвідчене популяризацією відповідних наукових досліджень інформаційної

царини [179, с. 315]. Останнє виявилося в популяризації терміна ІВ, що набув широкого поширення після славнозвісної операції «Буря в пустелі» (1991 р.) у Іраку, у межах якої ІТ уперше актуалізовані у воєнних цілях. 1992 року категорійно-понятійний стан терміна був остаточно вирішений: директива міністра оборони США DODD 3600 остаточно виформувала його, декларувавши його корелятивність з радіоелектронною боротьбою [176].

М. Лібікі [169] із цього приводу наголошує на складності повного усвідомлення концепції ІВ: дослідник вказує на категорійне утруднення й онтологічну невизначеність його природи, натомість виокремлює сім основних і двадцять доповнювальних форм ІВ, підкреслюючи недостатню дослідженість цього феномена. Цікавою є думка В. Ліпкан [171], який позиціонує ІВ вищим рівнем онтологічного (що набуло інформаційних обрисів) протистояння. Його використовують для розв'язання конфліктів різного спектра: від соціально-політичних до національно-культурних, а також територіальних. Такому розв'язанню конфліктів властива диференційованість використовуваних методів інформаційного впливу.

Науковці А. Шумка та П. Черник [277] розглядають ІВ як комплекс заходів для здобуття певної низки переваг відповідної природи. Характерно, що вони спрямовані на підтримку національної воєнної стратегії разом з трансформаціями даних та їх систем супротивника. Дослідниця О. Куцька [179] категоризує окреслений феномен комплексною дією на систему державного та воєнного управління супротивника, метою якої є ухвалення певних сприятливих для держави рішень, а також збереження, розвиток та інше власної інформаційної інфраструктури [179]. Цікавою видається позиція О. Копана та В. Мельника [180, с. 5], які локалізують ІВ у контексті актуалізації пропаганди проти супротивника, яка спрямована на дискредитацію державних інституцій та уряду загалом, спонукаючи суспільство до протестів [199]. Прикметними вважаємо також погляди П. Шпиги й Р. Рудника [117, с. 20] (див. рис. 9) та Є. Магди, який звертає увагу

на важливості ІВ у сучасному світі, акцентуючи на неподільності ІВ від воєнних операцій [180, с. 5].

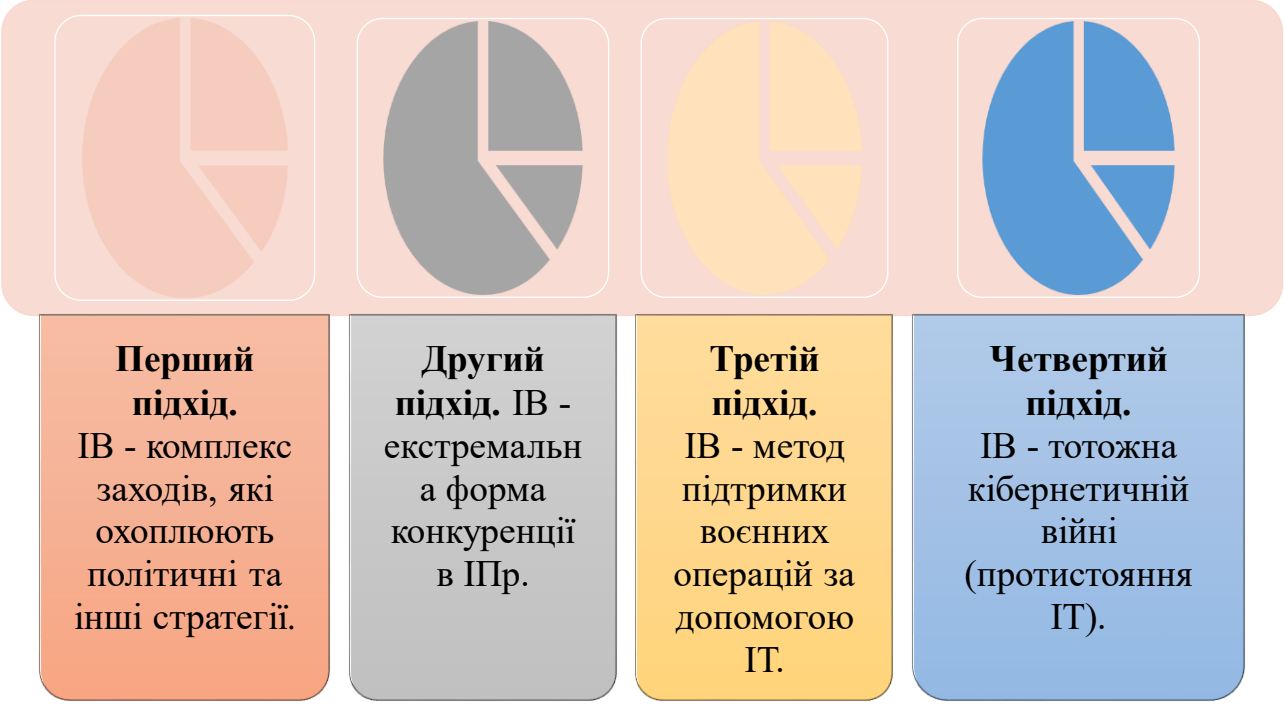


Рис. 9 Концепції ІВ (за П. Шпигою та Р. Рудник) [117, с. 20].

Таким чином, вищезазначені підходи репрезентативні щодо спектра актуалізованих у сучасних ІВ аспектів, стратегій, концепцій та іншого, що увиразнює інтегровану природу, складність тощо останніх. Під час аналізу специфіки категорійно-понятійної генези ІВ ми дійшли висновку про глибину, яка сягає періоду до появи інформаційного суспільства. Останнє засвідчене вищезазначеними прикладами біблійного, римського та інших історичних періодів. Так, інформаційний вплив існував ще з давніх часів, виформовуючи погляди, думки, настрої того чи того суспільства, визначаючи вектор його розвитку або занепаду.

Своєю чергою, це увиразнює диференційованість, дифузність та інше пошуку й виокремлення тієї чи тієї інтенції в умовах флуктуацій смислу. Останнє дало підстави Інституту національно-стратегічних досліджень США та низці західних експертів (Лібікі М., Тоффлер Е., Кіссінджер Г. та ін.)

вичленувати складники ІВ, які релевантні в плані функціонування низки методик, тактик та іншого, що можуть бути досліджені (див. Таблиця 6):

Таблиця 6

Тактики та методики ІВ [203].

№	Назва	Характеристика
1.	*Командно-управлінська тактика*	знищення, перешкоджання роботи комунікаційних систем задля порушення командного ланцюга
2.	*Розвідувальна форма*	пошук, збирання та інше конфіденційних даних та забезпечення захисту власної інформації
3.	*Психологічна війна*	мізінформація, дезінформація, пропаганда, які впливають на громадську думку та деморалізують населення
4.	*Хакерські атаки*	використання вірусів, троянів та іншого шкідливого програмного забезпечення для диверсійних дій проти ІТТ ворога
5.	*Економічна війна*	здебільшого включає інформаційну блокаду, імперіалізм та інше, які мають за мету вплинути на економічну стабільність ворога
6.	*Електронна війна*	спрямована, першою чергою, на апаратні засоби (засоби електронного зв'язку): радіозв'язок, радарні системи та комп'ютерні мережі
7.	*Кібервійна*	актуалізація диджиталізаційних засобів, використовуваних для ведення бойових дій та впливу на інтернет-дискурс (кіберінфраструктуру) ворога

Як бачимо, стрижневим є, власне, онтологія психологічної війни, тобто самобутність її ведення, що підводить нас до думки про корелятивну природу масових маніпуляцій, метою яких є: а) *інтегрування шкідливих (ворожих) наративів у суспільну та індивідуальну свідомість* (до прикладу, приреченості на поразку та іншого); б) *продукування шляхом дезорієнтації та мізінформації, дезінформації, пропаганди дифузності онтології народу супротивника* (до прикладу, «братскій народ», «братья-славяне» та под.) [188]; в) *категорійне розмивання стрижневих підвалин вищезазначеної онтології, метою яких є втрата етнічної специфіки громадян* (до прикладу,

«ми – русскіє», «адін народ» тощо); г) *залякування власного народу образом супротивника* (до прикладу, «бандерівцями»); ґ) *залякування супротивника власною могутністю або можливим використанням наявних ресурсів* (до прикладу, використанням атомної зброї).

Доволі репрезентативним щодо перебігу пропагандистських кампаній є діяльність ідеолога фашизму Й. Геббельса, що окреслено в статтях і промовах на основі його праці «Залізне серце» [354]. Він виокремлював такі принципи пропаганди: 1. *Єдине джерело пропаганди*, яке сплановано, послідовно здійснює вплив. 2. *Авторитетність визначення її цілей*, корелює з суб'єктивною площиною побутування. 3. *Видова, типологічна та інші диференціації*: так, актуалізація «чорної» пропаганди відбувається тоді, коли залучення «білої» не доцільне або не має належного ефекту. 4. *Маркованість репрезентації в призмі пропаганди*, позначена охарактеризуванням подій, людей та іншого прикметними фразами, гаслами тощо. 5. *Актуалізованість пропагандистських даних*, детермінована інтересом, суголосністю дискурсу й використанням привабливого ІПр [303, с.202].

Сила пропаганди Й. Геббельса спродукувала прихід до влади Німеччини фашистів і початок Другої світової війни. На жаль, незважаючи на позірне відсторонення російської влади від фашистської ідеології, на сьогодні ця країна має з нею дуже багато спільного. Так, рф наслідує, повторює, актуалізує й розвиває прийоми фашистської пропагандистської машини: зокрема, анексію АРК в їх столиці пояснили «відновленням історичної справедливості» та «захистом російськомовних громадян». Прикметно, що останні при цьому були атомізовані від питомих меж власної приналежності й актуалізовані в контексті «руського міра», представників якого треба відстоювати в усьому світі. Приблизно ті самі ідеологеми були озвучені фашистською Німеччиною для пояснення виокремлення від Чехії Судетської області (1939 р.).

Репрезентативними вважаємо цитати сучасних політиків та представників влади рф, у яких останні намагають аргументувати військове втручання в сусідню країну. Зокрема: «У нас ще є можливість посилити війну

в Україні. Через півроку такої можливості вже не буде. Подивіться на динаміку: якщо в грудні 2013 р. нацистів було 2 тис. в Києві, то в лютому – вже 20 тис. В травні їх уже 50 тис. разом з військовими, в середині літа їх буде 100 тис., а у вересні їх буде200 тис. до кінця року вони мобілізують 500 тис. осіб. Ми отримаємо потужну військову машину, орієнтовану проти нас, нашпиговану нацистами, ідеологічно заряджену проти Росії. Кінцевою метою всіх цих дій є війна з Росією» [298]. Показовою в цьому плані є класифікація форм дезінформації та маніпулювання В. Петрика [221; 222] (див. табл. 7).

Таблиця 7

Форми мізінформації, дезінформації, пропаганди та маніпулювання даними [221;222].

Формальне представлення				
тенденційний виклад фактів	*«зворотне» дезінформування*	*категорійне «мінування»*	*дезінформування*	
			«сіре»	*«чорне»*
репрезентація фактів за допомогою спеціально підібраних правдивих даних, які вибудовані дозовано й дискредитативно щодо певної мети	надання правдивих фактів, проте у перекрученому вигляді з порушенням причиново-наслідкового зв'язку, що продукує їх викривлену інтерпретацію	викривлення питомих значень релевантних термінів і витлумачень загально-світоглядної й оперативно-прикладної природи	актуалізація самобутнього поєднання правдивих даних з неправдивими	використання здебільшого неправдивих даних

Взірцевим прикладом дезінформування є трансляція від 12 липня 2014 року на Першому російському телеканалі сюжету про нібито розіп'ятого українськими силовиками хлопчика [222]. Природно, що поширення цієї брехні російськими медіа мало експонентну природу: таким чином, російські громадяни отримали ще одну цеглину в ідеологічне підґрунтя для ненависті до українців, нагнітання страху. Так, у праці Дж. Догерті [68] досліджено

динаміку актуалізованих у російських медіа за останніх років процесів: зокрема, авторка досліджує генезу пропаганди в них, зазначає, що російська пропаганда має дуальну природу: використовує класичні методи (мізінформацію, дезінформацію, пропаганду), поєднуючи їх з корпусом сучасної інформаційної зброї (у широкому спектрі: від електронних медіа, цифрових комунікацій до блогів і соціальних мереж).

Натомість М. Гессен [267, с. 268] висловлює тезу про те, що рф позиціонує себе лідером антизахідного світу, а в. путіна – месією, головним поборником «содомії», «толерастії» та іншого, осередком «традиційних» цінностей. Так, метою методу диверсифікації громадської думки є розпорошення уваги населення на низку штучно витворених проблем з акцентуванням на важливості їх розв'язання. Таким чином, відбувається відволікання уваги від поточних першочергових завдань суспільно-політичного, культурного, економічного та інших розвитку. Стрижневими формами функціонування цього методу є: а) актуалізація інформаційної кампанії, спрямованої проти політичного курсу наявного уряду та окремих її лідерів різними міжнародними організаціями; б) ініціювання антидемпінгових кампаній і розгляду інших скандальних судових справ, використання міжнародних санкцій з тих чи тих причин [27].

Слушною тут є думка В. Гусарова [56], який стверджує, що рф розпочала нову ІА для підтримки нового витка експансії: продукування тиску на уряд України задля актуалізації ним бажаного сценарію врегулювання конфлікту. Експерт виокремлює такі напрями ІА: 1. Продукування думки про неспроможність українського керівництва до ухвалення логічних, обдуманих і корисних для країни рішень. 2. Виформування ідеї про відстороненість українських посадовців від поточних проблем на Сході Україні на тлі нескінченних суперечок щодо виборів до парламенту. 3. Продукування негативних суджень про український уряд щодо невдалих воєнних стратегій, відсутності перемовин з рф тощо, наслідком чого є невиправдані жертви серед цивільного населення й військовослужбовців. 4. Поширення даних щодо

деморалізованості й неспроможності ЗСУ вести бойові дії тощо. 5. Виформовування думки про те, що Україна не зможе пережити зиму без російського газу, наслідком чого є потреба в перегляді газових домовленості та інше.

В. Гусаров також зазначає, що цільовою аудиторією (далі – ЦА) рф є передовсім її населення, а також російськомовні громадяни інших країн (діаспора, населення України та інші групи, які можуть потенційно поділяти проросійські погляди). Експерт підкреслює, що на сьогодні левову частку СПІБ має перебрати на себе українська влада та дипломатичний корпус з підтримкою вітчизняних медіа [56].

Згадаємо також про психологічний і психотропний тиск як складник ІВ, суть якого у впливі на психіку людини шляхом погроз (залякування) та іншого, з метою продукування в неї потрібної поведінкової моделі. Формами такого впливу є: а) виформовування перед його об'єктом широкого спектра минулих, реальних і потенційних загроз онтологічній тяглості; б) продукування наративів про потенційні деструктивні дії з таким об'єктом, його рідними й близькими людьми: репресій, переслідувань, катувань, убивств тощо; в) спричинення масових жертв шляхом вибухів, підпалів, отруєнь та іншого задля посилення соціального, психологічного напруження в об'єктів впливу: громадян, суспільства та ін.

Прикметно, що базовим інструментарієм продукування психологічного тиску є «телефонний тероризм», який полягає в інформуванні щодо мінувань місць масового скупчення людей (закладів загальної середньої освіти (далі – ЗЗСО), ЗВО, театрів, кінотеатрів тощо), інфраструктурних об'єктів (вокзалів, аеропортів тощо). Також згадаємо актуалізацію ворогом низки заборонених методів – методів психотропної дії (зокрема, технології двадцять п'ятого кадру). Так, СБУ засвідчило використання цієї технології російськими телеканалами: зокрема, мовиться про випуск новин телеканалу «Росія-24», у якому її актуалізовано. Протягом усього випуску новин про події в нашій країні в куті екрана з'являються малопомітні написи («підпал», «Правий

сектор», «людей убивають бандерівці», «Нацгвардія – вбивці» та інші). Окрім того, російські медіа активно послуговуються іншими методами впливу на свою аудиторію: використовують напівправдиві дані, деталізовано висвітлюють сцени вбивств і насильства, вчиняють емоційний тиск тощо [265].

Отже, у ІВ проти нашої держави рф активно послуговується широким спектром засобів впливу на свідомість населення, не гребуючи використанням заборонених технологій. Наслідком цього стало перетворення українців, які були актуалізовані в контексті наративу про меншовартісний («малороси», «хохли» та інші), проте «братній народ» у часи СРСР, до кровожерливих міфічних «бандерівців», «американських маріонеток» і безпосередньо ворогів. Природно, що цей процес мав і зворотний зв'язок, трансформуючи ставлення українців до колишніх союзників, які колись гарантували цілісність і неподільність території їх держави.

Нині практично не можна знайти українця, байдужого до лихоліття, спричиненого йому, його сім'ї, близьким, друзям, колегам та іншим співгромадянам. Це засвідчують результати опитування, проведеного російською соціологічною організацією «Левада – Центр» та Київським міжнародним інститутом соціології (далі – КМІС). Так, за три місяці 2014 року (з лютого по травень – до початку військових дій на Сході України) чисельність толерантних до рф громадян України стрімко скоротилася: з 78% (у лютому) до 52% (у травні). Закономірно, що у рф ставлення до українців також змінилося: позитивне сприйняття скоротилося, якщо порівнювати з лютим, з 66% до 35%, а вороже ставлення експонентно зросло: з 26% до 49% [80, с. 277].

Звернемо увагу також на організаційні відмінності гібридної та ІВ, яка вирізняється тим, що практично весь ІПр країни-агресора зосереджено в одному центрі ухвалення рішень. Також відзначимо підготовленість ворога до ІВ за рахунок актуалізації в цьому процесі організаційних, лобістських, фінансових та інших ресурсів. Із цього приводу влучною вважаємо думку

П. Шевчука [305], який підкреслює наявність цілого спектра актуалізованих тактик щодо України. Зокрема, автор виокремлює такі: а) стабільне зниження міжнародного іміджу нашої країни з метою зменшення її значущості на геополітичній арені; б) видозміна даних (мізінформація, дезінформація, пропаганда), покликана дестабілізувати внутрішню ситуацію та спричинити ефект «керованого хаосу»; в) виформовування меншовартісного образу українців як недонації, що має підірвати почуття національної ідентичності; г) продукування концепції «руського міра», у межах якого просувають російську мову, культуру, традиції та інше як питомі, одночасно зменшуючи роль української мови, культури, традицій тощо. Вищезазначені тактики спрямовані на зміцнення впливу рф та послаблення позицій України на міжнародній арені з поступовою експонентною девальвацією її мови, культури, традицій та ідентичності [305; 307].

Показовою в цьому плані є діяльність низки інформаційних агентств, які підтримують рф у гібридній та ІВ, стратегія яких здебільшого базована на актуалізації неправдивих, перекручених тощо даних. Зокрема, агентства використовують неправдиві новини для введення в оману своєї аудиторії: безвідносно – української чи російської. З-поміж таких медіа: інформаційне агентство «Новороссия», видання «Молот правды», «Новости ДНР», «Комсомольская правда», «V-news» та інші, які упереджено, перекручено, тригерно й тенденційно висвітлюють ті чи ті події, описуючи вигаданий світ з «укрнаціоналістами», «націоналістичними батальйонами» та подібними примарними утвореннями [307]. Прикметною також є акумулювання ІР рф, яке засвідчує їх кореляцію на державному та федеральному рівнях: мовиться про базованість на імпліцитних директивах вищих органів влади країни-окупанта. Таким чином, інформаційні агентства здебільшого актуалізують масове поширення неправдивих даних задля маніпуляцій, пропаганди та ін.

При цьому, на жаль, наша країна, система її державних інституцій, суспільство та інше не були готові до такого фундаментального підходу ворога до інформаційної й військової агресії, який дістав назву «гібридна війна».

Вищезазначене закономірно продукує виокремлення як першочергового завдання розробки нагальних ефективних заходів щодо нейтралізації такої диверсійної діяльності рф проти України й протидію її подальшій генезі. Це можливе лише за умови залучення громадських, державних, експертних, наукових та інших інституцій, організацій, установ і негайної розробки згаданої нами в попередніх розділах наукової роботи Доктрини національної безпеки України. Вона, своєю чергою, продукуватиме інтенсифікацію модернізаційних процесів всієї системи ІБ нашої держави [6].

Особливої значущості набувають науково-практичні дослідження щодо розробки нових тактик, стратегій, доктрин державного управління в царині захисту ІПр України. Так, рф, розпочавши з анексії АРК, зрештою перейшла до відкритого протистояння 24 лютого 2022 року, що, характерно, на звавши його СВО. Насправді цей своєрідний coming out ворога є показовим у контексті ІВ, що фактично почалася від проголошення незалежності України й інтенсифікувалася після факту анексії АРК. Головними засобами такої війни узвичаєно стали медіа, через які супротивник поширює неправдиві та інші дані [89, с. 42].

Ю. Озюменко [213, с. 123–130] проаналізував російські медіа, що дало науковцеві підстави стверджувати про диференційованість актуалізованих у них методів ІВ. За словами автора, там побутують такі методи: а) дозованість репрезентованих фактів та їх перекручення з метою відповідності певному бажаному наративу; б) суб’єктивність, а не об’єктивність витлумачення представленої інформації та специфіка актуалізованого матеріалу; в) використання техніки «25-го кадру», яка є забороненою міжнародним законодавством, тощо. Природно, що перераховані дослідником методи, використані в російських медіа, спрямовані на продукування сприятливого ІПр шляхом контролю над сприйняттям подій серед свого населення.

За даними пошукової системи Google, словосполучення «ІВ» продукує віднаходження понад 8 мільйонів покликань, половина з яких стосується безпекової ситуації в нашій країні. Останнє засвідчує актуальність,

злободенність і затребуваність аналізованої проблематики: в інтернет-дискурсі постійно публікують новини про події в Україні, матеріали яких часто мають спотворену, негативну та інші конотації. Зокрема, аналіз заголовків на сайтах «правда.ру» [229], «московський комсомолець» [204] з новинами виявив, що здебільшого в них актуалізована емоційно-забарвлена лексика щодо України, її уряду та громадян. Дані досліджень на таких «вагомих» ресурсах, як «правда.ру» та «московський комсомолець» [204; 229], здебільшого містять широкий спектр пропагандистських методів: продукування ярликів (використання зневажливих термінів на адресу українських лідерів або громадян), апелювання до «авторитетів» (посилання на думки проросійських експертів для підтвердження власних тез), демонізацію опонентів (зображення української сторони як агресора або джерела проблем), спрощення зображуваних подій і виформовування емоційного резонансу (подання складних ситуацій у чорно-білому світлі, без урахування нюансів) [122; 311].

Усе це покликане формувати в аудиторії почуття приналежності до «великої» російської культури, пропагуючи її глибину, фундаменталізм та значущість.

Така методологія актуалізована в новій формі війни – ІВ, яку не можна декларувати класичною воєнною операцією. Згадаємо експонентну природу дій рф: так, перед військовою окупацією території нашої держави було проведено низку «навчань» біля кордонів України. Окрім того, такі «навчання» провели і в Калінінграді, провокуючи зростання небезпеки балтійських країн та Польщі. Показовим також вважаємо недоступність українських медіа в окупованих територіях, що відрізало їх від усієї країни з одночасною інтенсифікацією кремлівської пропаганди, що витворювала паралельну реальність. Головними засобами такого впливу стали: а) медіа, б) сили інформаційних операцій, в) боти, г) представники культури. Натомість така методологія включає: руйнування механізму самоідентифікації; актуалізацію штампів і кліше; мізінформацію, дезінформацію та пропаганду;

блокування українських медіа; дискредитацію критичного мислення [53, с. 17, 23].

Початок російсько-української війни виявив прагнення рф щодо контролю нашої країни, що рухалася своїм цивілізаційним вибором. До того ж вплив ворога узвичаєно став продукуватися за рахунок гібридної (фактично неоголошеної) війни, яка мала низку спільних рис з терористичною діяльністю [154]. Так, розпочата супротивником ІВ була спрямована на підтримку сепаратистського руху в Україні, ослаблення контролю влади та виформовування низки проблем безпекової й економічної природи. Під час здійснюваних рф дій (анексії АРК, окупації територій на Сході нашої країни) її інформаційна політика зазнала трансформаційних змін, у межах яких відбулося перетворення такої політики на воєнну дезінформаційну агресію, що мала на меті дискредитувати керівництво України та ЗСУ.

Прикметною при цьому є стрижнева роль ІВ у подібних гібридних конфліктах, яка полягає в тому, що продуковані дії створюють несталий ІПр, підриваючи довіру в суспільстві тощо. Наслідком цього є глибокий слід, який лишається після її актуалізації в постраждалих від неї країнах (зокрема, у нашій країні, яка зазнала тривалої дії ІВ). Природно, що вищезазначений вплив можна розглядати в різних контекстах (див. рис. 10):

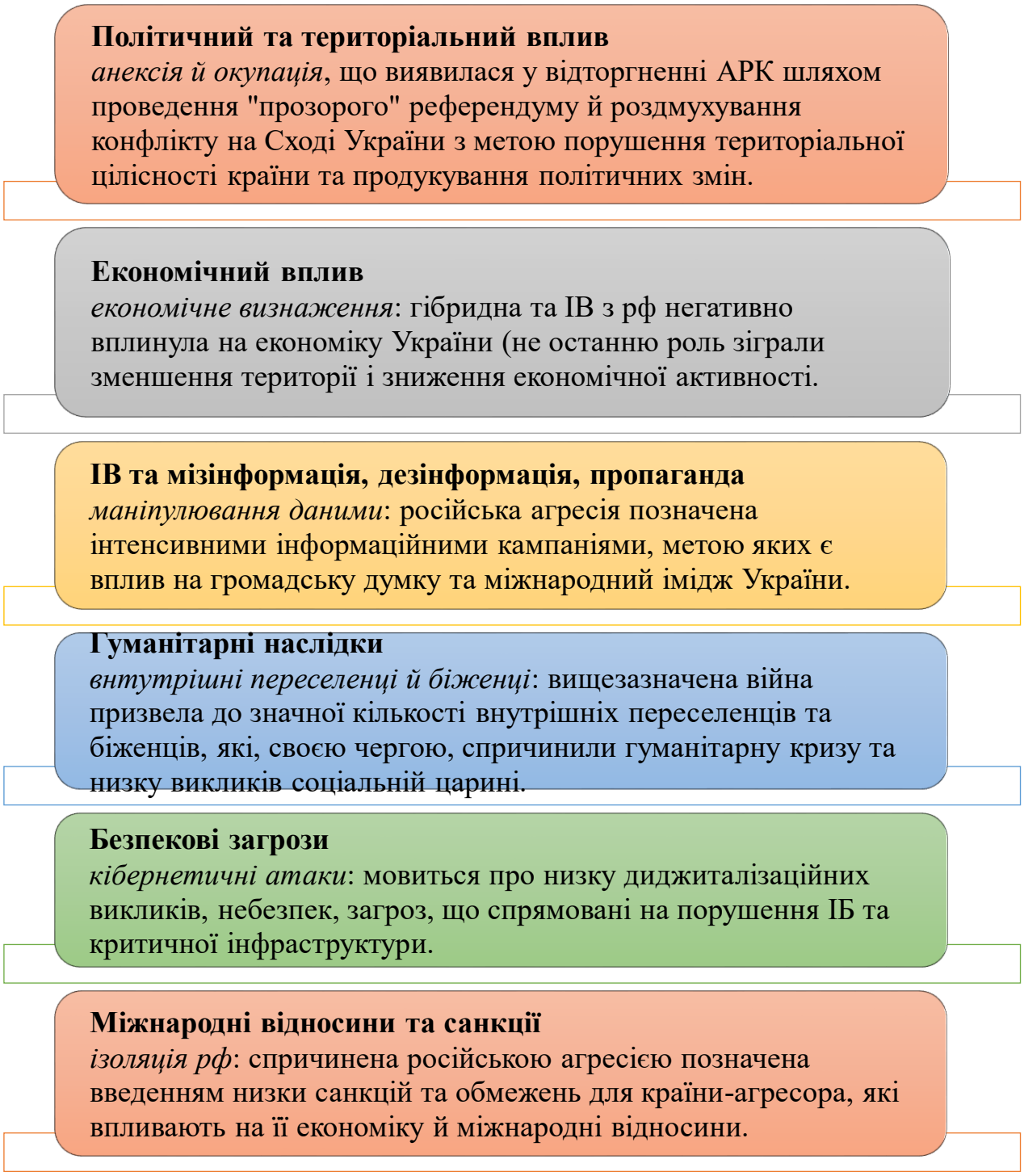


Рис. 10 Впливи російської агресії [301].

Ця параметризація (рис. 10) засвідчує широту спектра впливів російської агресії на українську державу: зокрема політичні, економічні, культурні, соціальні, управлінські й інші, що зумовлює потребу в дослідженні побутування цього феномена в окреслених вимірах, уможливлюючи всебічно, ґрунтовно й комплексно його вивчити. Натомість останнє є першим етапом

випрацювання, формування ефективних стратегій протидії такому впливу й відновлення належного функціонування країни. Доцільно розглянути роль інформаційних операцій докладніше в контексті ІВ як стрижневого інструмента в протистояння агресії рф. Так, стрижневими завданнями, релевантними для побутування ІВ, є:

1. *Маніпулювання громадською думкою*, що є стратегічною метою ІВ: зміна світоглядних орієнтирів, моральних детермінант та іншого, що корелюють з поведінкою громадян.

2. *Хаотизація, дезорієнтація населення*, яка має на меті порушення належного функціонування державних інституцій, умов соціального контракту та іншого.

3. *Занепад морально-психологічного стану громадян*, реалізований через психологічний тиск, який впливає на ухвалення рішень, продукування суджень та іншого.

4. *Вплив на поточну політичну ситуацію* шляхом спотворення даних про події, що відбулися, або наративне витлумачення останніх з метою дискредитації уряду або політичних акторів.

5. *Кібербезпекові загрози*, які корелюють з низкою кібератак задля порушення роботи ІТТ, видобуття конфіденційних даних та ін. [198, с. 99–105].

Відтак ІВ – невід'ємна частина стратегій агресорів, оскільки її методологія є не лише ефективною, а й доволі важко локалізованою, що, своєю чергою, зумовлює складність протидії їй. Параметризаційна природа цього інструментарію в тому, що він впливає не лише на суспільство загалом, а й на державні інституції, продукуючи зупинку, ускладнення та інше їх діяльності та, зрештою, посилення напруги в суспільстві через це. Так, динаміка ІВ в нашій країні є самобутньою, оскільки рф демонструє вагомий деструктивний потенціал, що актуалізує проблему медіаграмотності українського населення. Остання детермінована здатністю українців до критичної оцінки, аналізу та осягнення даних, які вони споживають. Базовими критеріями такого процесу

є критичне мислення – здатність до аналізу, обробки та репрезентації тих чи тих даних. Окрім того, ідеться про локалізацію того чи того джерела та ступеня його потенційної достовірності чи брехливості, тобто фактчекінгові вміння.

Ця здатність позначена перевіркою фактів перед її репрезентацією та поширенням, а також мінімізацією взаємодії з неправдивими даними. До прикладу, у випадку ідентифікації в певному дописі в соціальних мережах як брехливого абощо не доцільно коментувати його або поширювати, нехай і позначаючи зміст останнього. Це пов'язано з алгоритмами роботи соціальних мереж, які такі дії позиціонують у контексті його популярності й покажуть ще більшій кількості користувачів. Якщо ж у цьому є сенс, то варто зв'язати з його автором, аргументувавши неспроможність або нікчемність наведених фактів щодо онтологічної дійсності, і попросити прибрати допис.

Також доцільно згадати про необхідність актуалізації різних джерел, що дасть змогу валідувати факти, репрезентовані в одному, порівнявши з низкою їх інтерпретацій у інших. Зокрема, доцільною є актуалізація таких критеріїв оцінки даних: а) *джерело* (варто уникати «ру» в адресі того чи того сайту); б) *авторитетність* (мовиться про рівень викладу даних і його співвимірність: так, манікюрниця не може бути експертом з економічних питань абощо); в) *доказова база* (навіть найскладніша проблема може бути донесена таким чином, аби нефахівцям була зрозуміла її суть); г) *об'єктивність* (ідеться про врахування низки попередніх і потенційних подій безвідносно до статі, професії та іншого мовця: так, розлучена жінка може робити матеріал про весілля за умови безвідносної щодо свого минулого його репрезентації); г) *контекст* (одна і та ж подія може бути інтерпретована діаметрально протилежно на різному тлі: у мирний час та воєнний тощо) [219, с. 162].

Характерною є актуалізація ІВ рф, яка використовує її як засіб досягнення своїх геополітичних цілей, серед жертв яких назвемо такі країни (див. табл. 3.5), що засвідчує диференційованість, ефективність актуалізованих рф методів в ІВ:

Таблиця 8

Жертви геополітичних цілей рф [129].

№	Назва	Характеристика
1.	Грузія	актуалізована для легітимізації військової інтервенції та впливу на громадську думку
2.	Молдова	маніпулювання громадською думкою та створення незгоди серед населення у межах придністровського конфлікту
3.	Литва, Латвія, Естонія	низка інформаційних провокацяй, які продукують появу й посилення соціального напруження
4.	Сирія	задіяння мізінформації, дезінформації та пропаганди щодо діяльності рф та впливу на громадську думку
5.	США	втручання у вибори засвідчує кореляцію інструментарію ІВ рф з інтенсивністю впливу на політичні процеси

Релевантною в цьому контексті є думка М. Максимовича [38, с. 22–24], який підкреслює ключову природу спотворення даних, їх наративного витлумачення й пропаганди, активно використовувані російськими медіа у формуванні поняття «рашизм». Вищезазначену дефініцію здебільшого використовують для позначення низки подібних рис у використовуваних росіянами методів до тих, якими свого часу послуговувалися нацисти. Так, Г. Сасин [47, с. 136, 140], звертає увагу на спільні риси інформаційної війни, яку веде рф, з методами пропаганди, що застосовувалися нацистським режимом. Він також зазначає, що, хоча Україна зазнає значних втрат у сфері інформаційного протистояння, це не варто трактувати як поразку, оскільки країна не є носієм нацистської ідеології чи практик.

Медіа в диджиталізованому світі є джерелом даних, а відтак з його допомогою можна маніпулювати ними різними способами. Ідеться про спотворення, однобічний підхід до репрезентованої проблеми, редагування з додаванням нових відтінків значень, коментування та інше, що продукує появу «інформаційного шуму». Ці методи актуалізовані в контексті виформування сприятливого ІПр та впливу на громадську думку й засвідчують широту використовуваного рф у ІВ з Україною спектра.

Закономірно, що існують методи протидії цим впливам (на особистому та державному рівнях), проте, на думку В. Христенка [299], у межах гібридної та ІВ, обсяг корпусів текстів експонентно зростає, набуваючи нечуваної насиченості, що робить таке завдання дедалі складнішим. Однак доцільно дотримуватися низки правил, серед яких: а) ознайомлення з повним текстом новини, а не лише з його заголовком; б) ретельний фактчекінг наданих даних за кількома джерелами, а бажано за офіційними каналами комунікації державних інституцій; в) актуалізація хронологічних меж тієї чи тієї інформації, оскільки інформація може бути застарілою або публікуватися повторно для привернення уваги; г) використання згаданих у тексті джерел, ознайомлення з їх змістом та на його підставі формування думки про текст, у якому вони згадуються; ґ) перевірка мультимедійних елементів, актуалізованих у «тілі» тексту: достовірність та ін.

Щодо інституційного і, зокрема, адміністративного рівня у вищезазначених процесах, то ефективним є формування власних каналів комунікації з метою надання достовірних даних міжнародній спільноті. Так, показовим є англійськомовний телеканал «Ukraine Today» від «1+1 медіа» та анонсований 2015 р., проте, на жаль, так і не створений телеканал іноземного мовлення «Ukraine Tomorrow». Окрім того, згадаємо Проєкт Ради Європи «Зміцнення свободи медіа та створення системи Суспільного мовлення в Україні» [254], метою якого є зміцнення ролі медіа та суспільного мовлення як інструментарію для досягнення злагоди в українському суспільстві. Останній був актуалізований у межах Плану дій Ради Європи для нашої країни в період 2015–2017 рр. [224].

Сказане засвідчує ефективність протидії ІА рф на державному рівні шляхом видозміни (передовсім захисту ІПр України) та продукування НБ нашої країни. Релевантними для актуалізації окресленого є такі стратегії:

1. Розробка, актуалізація та розвиток комплексної полісистеми ІБП.

2. Продукування, удосконалення й структурування систем захисту ІПр від зовнішніх впливів.

3. Підхід до всього українського з брендових позицій, а відтак його поширення й популяризація.

4. Аудит наявних медіа та приведення їх до сучасних вимог задля забезпечення продукування ними якісного контенту з особливою увагою на ті, які працюють на міжнародну аудиторію.

5. Атомізація олігархічних структур і вищезазначених медіа з метою уникнення впливу на них і продукування упереджених даних останніми.

6. Популяризація ідеї неподільності за одночасної різноманітності українського народу та поваги й рівних умов до всіх його представників, безвідносно приналежності до національних, сексуальних або інших меншин, людей з особливими потребами тощо.

7. Аналіз частки впливу іноземних медіа (зокрема, російських) на український ІПр та їх контроль (обмеження, дозування, заборона).

8. Інтенсифікація просування НІ шляхом використання розвідувальної діяльності, міжнародної співпраці та підвищення професійної підготовки фахівців у царині ІБ [130; 131; 220].

Отже, вивчення ІВ, продукованою рф проти України, репрезентативне щодо ролі медіа як потужного інструментарію динамізації політичних стратегій, механізмів і політично- комунікаційних особливостей влади (зокрема, державних інституцій та громадськості). Стрижневою особливістю актуалізованих ворогом інформаційних кампаній є динамічне використання медіа як засобу конструювання онтологічної реальності: політичних реалій і безпосередньо недоліків реалізації тих чи тих ініціатив «на місцях». За наявних умов для України врахування вищезазначеного ми вважаємо стратегічною детермінантою майбутньої перемоги. Так, зменшення рівня мізінформації, дезінформації, пропаганди та іншого супротивника разом з інтенсифікацією комунікації з громадськістю й активним використанням зворотного зв’язку з нею є ключовим для об’єктивної репрезентації нашої держави у світі.

Останнє, закономірно, доцільно вибудувати шляхом: а) *посилення медійної присутності* (контроль над репрезентованими даними, що продукує підтримку міжнародного співтовариства); б) *активного використання соціальних мереж* (надання доступної інформації широкій аудиторії та можливість висвітлення власної позиції та її донесення населенню); в) *належно вибудованої комунікації з міжнародною спільнотою* (утворення коаліцій, набуття партнерської підтримки та обопільна протидія інформаційним кампаніям рф).

На сьогодні наша держава перебуває на шляху диджиталізаційної генези, що, з одного боку, створює широкий спектр можливостей для її розвитку, з іншого – зумовлює лакунізованість її НБ (зокрема, ІБ). Україна опановує інформаційний інструментарій, підтримуючи свої стратегічні цілі, виокремлюючи інноваційні методи взаємодії з громадськістю та міжнародним товариством. Водночас це продукує наявність низки викликів / небезпек / загроз, рішуче, планомірно працюючи над їх розв'язанням, український уряд репрезентує розуміння значущості і ваги «інформаційного фронту». Водночас це зумовлює використання ним практично всіх доступних ІР задля збереження суверенітету, контролю інтегрованих у наш ІПр російських наративів та їх впливу, а також актуалізацію ШІ в належному адмініструванні.

Відтак низка стратегій, концепцій та ініціатив тощо засвідчує готовність України до розвитку в обраному цивілізаційному векторі, що підтверджує те, що країна не лише протистоїть російським інформаційним кампаніям (зокрема, інтегрованим ними наративам), а й виформовує власний. Такий український наратив має на меті підтримку внутрішнього гомеостазу й інтенсифікацію міжнародних відносин з набуттям всіх параметризаційних властивостей сучасної демократичної держави. Так, попри обмеженість наявних ІР, низку проблем економічного, соціокультурного та іншого планів, що пов'язані з війною, Україна виявляє рішучість, незламність і цілеспрямованість своєї європейської самоідентифікації.

3.3. Інформаційна політика України в контексті євроінтеграї та безпеки інформаційного суспільства

Цивілізаційний вектор розвитку нашої держави корелює з динамікою євроінтеграційного процесу, який є стрижневим стабілізуючим чинником формування її позитивного іміджу. Окрім того, у певному розумінні, він є також і складником СПІБ, регулюючи базові аспекти функціонування ІПр України [88, с. 203]. Закономірно, що ІБ є невід'ємним складником євроінтеграції й продукує належну діяльність державних інституцій й дієве інтегрування досвіду ЄС на українське підґрунтя. Так, релевантним є не лише прагнення нашої країни до збереження власної ідентичності, самобутності та іншого, а й репрезентаційна функція останніх, реалізована через диджиталізаційний інструментарій [33, с. 97–99].

У контексті наукової роботи показовою є специфіка побутування державних інституцій (інституційних чинників), релевантних щодо перебігу, динаміки, трансформаційних змін ІБП у вимірі інтеграційних процесів. Варто також підкреслити роль політичної участі громадян як чинника демократизації євроінтеграційних процесів та суспільної підтримки інформаційно-безпекової політики. Зазначимо, що ІП та євроінтеграція мають широкий спектр актуалізацій, зумовлюючи інтерес дослідників до цієї тематики. Профільними дослідженнями в цій галузі варто згадати монографію В. Марчука «Ukraine's European Integration in the Political Dimension of Central and Eastern Europe» [365], у якій автор характеризує процес європейської інтеграції України в контексті політичних реалій Центральної та Східної Європи, розглядаючи виклики та перспективи для національної безпеки; в іншій праці В. Марчука, В. Дудкевича, В. Мельничука «European Integration of Ukraine: Political and Security Practices» [366] співавтори досліджують політичні та безпекові аспекти європейської інтеграції України, акцентуючи увагу на практичних кроках і стратегіях гарантування національної безпеки в цьому процесі; питання національної безпеки України у площині європейської інтеграції з

акцентом на політико-правові аспекти цього процесу проаналізовано в праці дослідниці Ю. Кобець «Національна безпека України в контексті інтеграції до Європейського Союзу: політико-правовий аспект» [144].

В умовах трансформаційних процесів, пов'язаних з євроінтеграцією, особливу увагу заслуговує цифрова форма політичної участі, яка виступає одним з важливих інструментів подолання кризи представницької демократії. Як зазначає Н. Ротар, цифровізація створює нові умови для залучення громадян до політичного процесу, сприяючи посиленню політичної суб'єктності та формуванню інформаційної культури в суспільстві [266, с.163–165]. Дослідження Н. Ротар також акцентує на тому, що цифрова комунікація виступає не лише як технологічне нововведення, а як інструмент демократичного контролю, який в умовах війни та гібридних загроз набуває особливого значення з точки зору мобілізації суспільства та зміцнення національної безпеки [266].

Прикметним, на нашу думку, є наявний діалектичний взаємозв'язок європейської та глобальної стратегій становлення інформаційного суспільства. Останній висвітлено в стрижневій доповіді Європейської Комісії з проблем інформаційного суспільства «Європа і глобальне інформаційне суспільство: рекомендації для Європейської Ради ЄС» (1994 р.) [81]. У ній задекларовано кореляцію глобальних інформаційних процесів зі становленням нової ієрархії держав, яка: а) продукує низку нових можливостей промислового, культурного та інших розвитку; б) зумовлює виформування відповідної нормативно-правової бази; в) підвищує рівень культурогенезу шляхом інтенсифікування міжнародних відносин.

Так, ЄС усвідомлює значущість глобалізаційних процесів, а також переваги спільного продукування певних напрямів діяльності: зокрема, інтелектуального виробництва, недоторканності приватного життя та іншого. Така прогресивність європейських урядовців корелює з необхідністю адаптації до нових умов і у випадку зриву вищезазначеного можливої втрати конкурентоспроможності на світовому й регіональному ринках з низкою

соціальних наслідків [58]. Виокремимо стрижневі європейські інтереси у інформаційній царині (див. рис. 11).

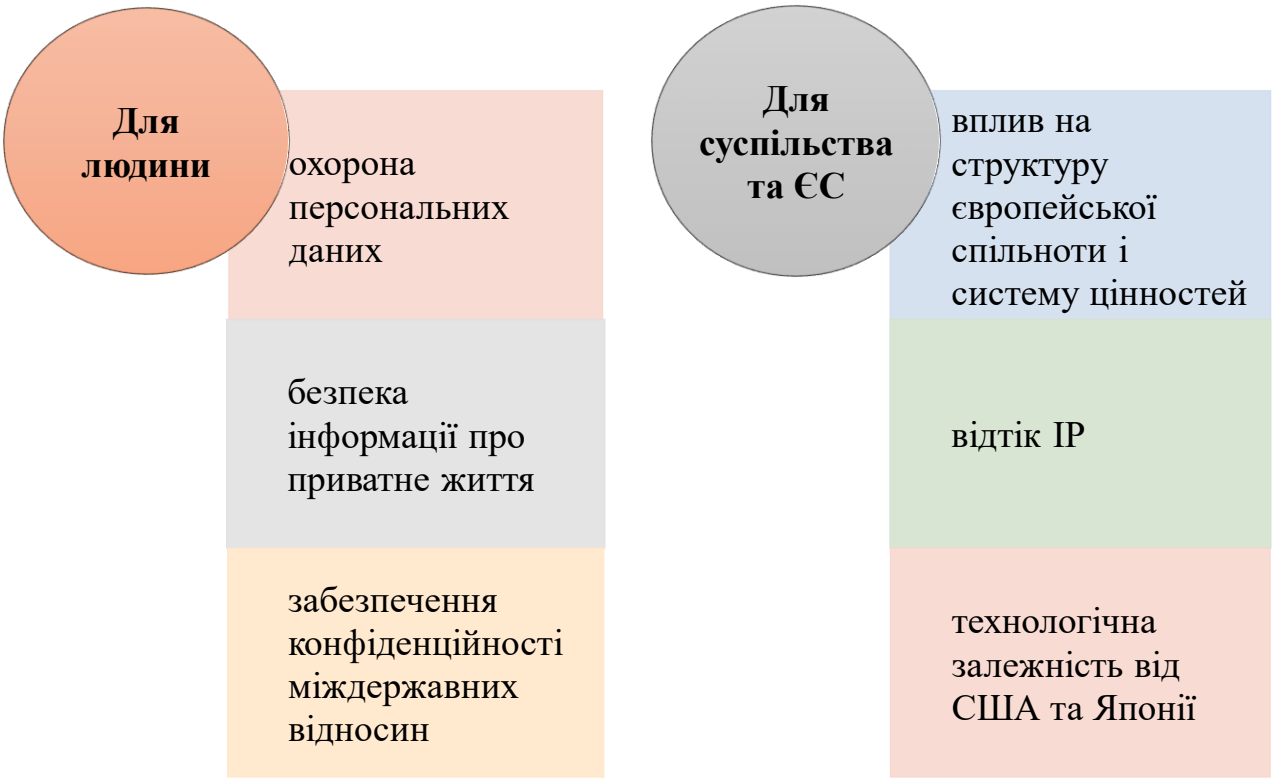


Рис. 11 Європейські інтереси у інформаційній царині.

Натомість серед стрижневих напрямів ІБП ЄС назвемо: а) інтенсифікування генези нового ІПр; б) розвиток міждержавної взаємодії на тлі актуалізації інформаційного суспільства; в) продукування вільного побутування даних у суспільстві як детермінанти демократичного ранжування політичних процесів і забезпечення вільного доступу до ІР (зокрема, інтернету) та захист інтелектуальної / інформаційної власності, розширення інформаційної інфраструктури (до прикладу, «EuroNet»); г) розбудови вищезазначеної в попередніх розділах цієї наукової роботи економіки знань (інформаційної економіки); ґ) виформування та актуалізація сучасних, конкурентоспроможних тощо ІР та задіяння потенціалу Європи в міжнародному економічному середовищі; д) попередження розвитку кіберзлочинності; е) розв'язання низки соціальних проблем європейського населення: зокрема, працевлаштування за умов інформаційного суспільства;

є) недопущення всіх форм дискримінації: за статтю, за вірою, за сексуальними уподобаннями, за рівнем медіаграмотності тощо та поширення ідей, знань, інформації та іншого на рівних підставах [136, с. 15–17].

Характерними є також права громадян країн-членів ЄС, які мають доволі широкий спектр: від вищезазначених прав на дані відкритої природи (нормативно-правові та ін.) до культурних надбань (художніх творів, наукових досліджень, необмежених авторськими правами, тощо) і програмного забезпечення та непатентованих стандартів [181, с. 81–87]. При цьому реалізація стратегічної мети ЄС в інформаційній царині (інформаційного суспільства) реалізована за допомогою низки інституцій (інституційних чинників): Європейської Ради (далі – ЄР), Європейської Комісії (далі – ЄК), Генеральних Директоратів за різними напрямами та ін.

Окрім того, згадаємо спеціально створені інституційні механізми – Генеральний Директорат з інформаційного суспільства, Форум інформаційного суспільства ЄС [200]. Показовою є структурна й цільова самобутність ЄС, яка, за ст. 3 «Договору про Європейський Союз» [183], є єдиною інституцією, що координує, продукує й забезпечує неперервність діяльності в межах локалізованих завдань. Серед них – логічність, наступність і послідовність зовнішньополітичної діяльності в таких аспектах, як: міжнародні відносини, безпекові, економічні, політичні та інші питання.

Вагому роль у розв’язанні цих питань відіграє ЄК, у повноваження якої входить розробка політичних стратегій, кампаній та іншого у відповідних напрямах побутування європейського суспільства. Установа також контролює виконання тих чи тих зобов’язань країн-учасниць, які підпорядковані реалізації спільної стратегії ЄС. ЄК також було підготовлено низку релевантних для інформаційного суспільства документів [320; 337], проте особливо важливим ми вважаємо розроблений нею «Шлях Європи до інформаційного суспільства» (1994 р.) [109, с. 96]. Цей документ декларує формування європейської інформаційної політики шляхом збереження

самобутності кожної нації, її лакун та ідентичності спільноти через вільний доступ до інформаційних послуг.

Водночас глобалізаційні, диджиталізаційні та інші процеси, а також їх роль у становленні європейського інформаційного суспільства закономірно продукують актуальність безпекової проблематики, щодо якої показовою є роль ЄК, яка ухвалила «Резолюцію про запобігання поширенню в Інтернеті інформації незаконного змісту, шкідливої для морального здоров'я суспільства» (1996 р.) [259]. Цікавою є потенційна відкритість поняття «шкідливий зміст», яке корелює в документі з культурними, релігійними та іншими традиціями, особливостями й реаліями, та поняття «незаконний зміст», детерміноване чинним законодавством.

У контексті безпеки даних у мережі Європейський Союз нещодавно ухвалив кілька ключових документів, які визначають сучасні підходи до захисту інформації та кібербезпеки: Директива (ЄС) 2022/2555 від 14 грудня 2022 року про заходи для високого загального рівня кібербезпеки [82], Акт про цифрові послуги [83], Регламент ЄС 2023/2854 про гармонізовані правила щодо справедливого доступу до даних та їх використання [260]. При цьому стрижневими заходами продукування безпеки даних у мережі в контексті досвіду ЄС є: а) забезпечення свободи комунікації й захисту персональних даних у інтернет-дискурсі; б) локалізація обов'язків сторін (зокрема, постачальників послуг) і правового статусу доменів; в) упровадження систем захисту інтелектуальної власності в онлайновому режимі; г) регулювання змісту даних, актуалізованих у інтернет-дискурсі (зокрема, політичному інтернет-дискурсі) [265].

Реорганізація ЄК 1996 р. призвела до створення Генерального директорату ЄС з інформаційного суспільства, який функційно став правонаступником цієї установи. Чільне місце в діяльності цієї інституції посіла проблема продукування безпеки інформаційного суспільства Європи. Так, Є. Макаренко [181-182] акцентує увагу на працях ЄС, де підкреслено продуктивність, релевантність і актуальність виформовування загальної

структури цифрового підпису та кодування задля збільшення рівня убезпечення електронної торгівлі. Окрім того, Директоратом було ініційовано розробку й підготовку низки документів щодо побутування ІТТ, супутникового зв'язку, розвитку індустрії медіа й пов'язаної з нею медійної (мовиться про контент) політики, функціонування інформаційної діяльності та ін. [181, с. 84].

Іншою інституцією, діяльність якої ми вважаємо релевантною в контексті цього дисертаційного дослідження, є Форум інформаційного суспільства (далі – ФІС), до повноважень якого входить адміністрування низки економічних, соціальних, управлінських, науково-освітніх та інших проблем щодо розвитку інформаційного суспільства. За своєю природою ця інституція є консультативним органом, діяльність якого не обмежена аналітикою поточної ситуації (функціонування, проблем та іншого) щодо інформаційного суспільства Європи, а й спрямована на продукування низки практичних результатів, серед яких – виформовування пропозицій, концепцій, стратегій, рекомендацій тощо задля поліпшення вищезазначеної ситуації, виправлення вектора розвитку.

Показово, що учасниками ФІС можуть бути представники національних / державних інститутів / організацій та низки соціальних, фінансових тощо груп: зокрема, розробники програмного забезпечення, виробники ІТ та інші фахівці не лише ЄС, а й інших країн. Рішення ФІС оформлюють у вигляді декларацій, директив та тому подібного, а їх виконання є обов'язковим для урядів країн-членів ЄС, натомість має рекомендаційну природу – для всіх інших [320, с. 109].

У межах діяльності ФІС актуалізовано низку обговорень, дискусій, присвячених таким напрямам: а) інформаційному суспільству в контексті підтримки національних ініціатив країн-членів; б) ранжуванню аксіосфери: генезі соціальних, культурних, економічних та інших цінностей і специфіці диджиталізаційних трансформацій послуг медіа; в) соціальному захисту населення в умовах самобутності сучасної комунікації; г) правовим аспектам

побутування даних у сучасному світі: рівності доступу до інформаційних надбань; г) самобутності кореляцій управлінської та громадської взаємодії, особливостям зворотного зв'язку в роботі державних інституцій; д) медіаграмотності європейського населення та шляхам, формам, способам її розвитку в контексті сучасних безпекових викликів / загроз / небезпек [320].

Прикметним є бачення інституції щодо розв'язання безпекового циклу проблем для продукування належного функціонування європейського ІПр, яке полягає в: 1. Інтенсифікації інвестиційних процесів, що зумовлені лібералізацією функціонування ІТТ. 2. Розвитку електронної торгівлі й виформуванню належних безпекових заходів задля захисту таких економічних операцій. 3. Генезі нормативно-правової бази: передовсім у царині електронної комерції, ШІ, інтелектуальної та інформаційної власності тощо. 4. Перегляді, розвитку та осмисленні крізь призму диджиталізаційних змін діяльності медіа в демократичному суспільстві, виформуванню нових журналістських стандартів. 5. Створенні національних консультативних органів (комітетів), які мають за мету динамізувати процес інтегрування концепції інформаційного суспільства в побут держав-учасниць. 6. Запровадженні державної інституції для координування виконання національної програми інформаційного суспільства і поширення інформації про стрижневі віхи її генези. Зокрема, у повноваження Генерального Директорату ЄС із освіти та культури входить, окрім іншого, проблематика інтелектуальної власності: візуальне та аудіовізуальне піратство, медіаграмотність, дистанційна освіта та освіта протягом життя (як її називають в Україні, – освіта дорослих) тощо [200].

Глобалізація та низка інформаційних процесів лімітують процес становлення нової ієрархії держави, відкриваючи можливості промислового розвитку, які, своєю чергою, потребують оновлення й диджиталізації нормативно-правової бази, інтенсифікують культурогенез та інше [18, с. 199]. Глобальні процеси також виформовують новий тип національних, регіональних та інших відносин, інтегруючи можливі наслідки генези

інформаційного суспільства, охорони прав і свобод громадян за нових умов та ін. [265]. Саме тому ми стверджуємо, що ЄС має фундаментальне підґрунтя становлення та розвитку такого суспільства, яке виявляється насамперед у багатому досвіді, що уможливлює моделювати розвиток цього процесу, ураховуючи позитивні та негативні наслідки задля успішного інтегрування в Україні.

Водночас безпекові питання питомо є стрижневими в цьому процесі, оскільки без їх продукування неможлива подальша розбудова всіх інших його компонентів (зокрема, «eUkraine») [242]. Так, першочерговим тут, на нашу думку, є розв'язання комплексу організаційно-правових проблем, чільне місце в яких посідає виформовування Концепції державної інформаційної політики України в контексті її інтеграції у ЄС. Окрім того, виокремимо: а) адаптивні зміни української нормативно-правової бази в інформаційній царині до світових (зокрема, європейських) стандартів; б) актуалізацію диджиталізаційного виміру урядування, репрезентовану запровадженням ІТТ у діяльність державних інституцій (зокрема, електронного урядування); в) динамічного, ефективного та іншого інтегрування Національної програми інформатизації, яка забезпечить належний, наступний рівень диджиталізаційних змін. Це становить фундаментальне підґрунтя процесу гармонізації нормативно-правової бази України з європейським відповідником [42].

Зазначена ідея покликана актуалізувати питомі принципи ІП ЄС у внутрішньодержавній площині України. У цій площині показовими є два нормативно-правових документи, які розроблені у Європі і які уможливлюють інтегруватися Україні в електронний монопростір ЄС: закони «Про електронну комерцію» [94] та «Про електронний цифровий підпис» [93]. Останній, до речі, доволі успішно показав себе в практиці урядування України: на сьогодні існує онлайнове і офлайнове подання пакетів документів з відповідним завіренням останнього узвичаєним чи електронним підписом (до прикладу, від «ПриватБанк»). Ці ключові закони деякі країни імплементують

у свій правовий дискурс без змін, інші – з ними, адаптуючи їх до національних, культурних та інших особливостей свого регіону [47, с. 128–132].

Показовою в цьому плані є самобутність України, яка має всю низку відповідних нормативно-правових документів, що дає підстави говорити про сформованість українського законодавства. Водночас відзначмо певну атомізацію одних документів від інших: з одного боку, вони різноманітні, однак взаємопов'язані, з іншого – існує низка суперечностей, які потребують коригування й уточнення, передовсім в інституційному плані й щодо практичних механізмах утілення. Окрім того, тут є низка вагомих проблем, детермінованих потребами в безпосередній імплементації, адаптації використовуваних систем електронного урядування, інформаційно-правових норм з європейськими тощо [135, с. 18–21].

З огляду на це особливої значущості для нашої країни набуває виформовування належного, захищеного ІПр, яке є стрижневою віхою електронного уряду, що є новою парадигмою державного управління, продуктивною щодо переосмислення, формального представлення тощо стосовно взаємодії з громадянами. Актуалізація цієї системи на українському підґрунті дає змогу інтенсифікувати низку напрямів роботи уряду (антикорупційний, інвестиційний та ін.). Зокрема, самобутність процесу переходу України до інформаційного суспільства в контексті державної програми «eUkraine» досліджено в праці Н. Дніпренко [72], у якій акцентовано на низці наявних чинників соціоекономічного, науково-технічного, культурного розвитку, які вона декларує передумовами переходу до інформаційного суспільства [72].

Окреслені дослідницею диджиталізаційні зміни стали надійним підґрунтям для виформовування низки серйозних передумов (у подальшому – умов) розвитку інформаційного суспільства. Наслідком цього стала динамізація інтеграції України у світове інформаційне товариство, що базувалася на зростанні релевантності даних як ресурсу політичного, економічного та інших аспектів розвитку й відповідного її використання.

Окрім того, важливу роль відіграє експонентно зростаюча кількість сайтів в інтернеті з паралельною генезою ІТТ. Ідеться насамперед про: а) збільшення кількості корпоративних інформаційних мереж і числа абонентів світових відкритих джерел; б) розвиток, розширення й оновлення національної мережі зв'язку: зокрема, зростання ринку засобів мобільного зв'язку, інтеграцію мобільних операторів за умов воєнного стану тощо; в) диджиталізацію економічної сфери (до прикладу, поява Monobank з принципово відмінним підходом до надання банківських послуг з активним використанням ІТ) та ін.

Питомою і незмінною детермінантою диджиталізаційних змін та елементом розвитку інформаційного суспільства в Україні (з 2008 р. і до сьогодні) лишається фінансово-економічна криза [46; 145, с. 41]. Оскільки така зчепленість є доволі поширеною, то прикметним є виголошений ЄС у межах Сьомої рамкової програми вектор розвитку інформаційного суспільства як засіб виходу з неї. Зокрема, саме тому до Програми діяльності КМУ «Подолання впливу фінансово-економічної кризи та поступальний розвиток» [248] уперше було включено окремим підрозділом «Розбудова інформаційного суспільства». У ньому окреслено пріоритетні напрями розбудови такого суспільства, подібні до зазначених напрямів ЄС, проте адаптовані для українського підґрунтя. Серед яких: а) інтенсифікація електронного документообігу, цифрового підпису та інших диджиталізаційних елементів; б) відкритість, прозорість і доступність даних для громадян; в) розвиток ІТТ суголосно продукуванню основних положень Національної програми інформатизації [132]; г) розробка національної цільової програми інтегрування в державних інституціях програмного забезпечення із закритим кодом: оскільки використання відкритого коду спродукує збільшення ймовірності зламу таких інформаційних систем; г) динамізація змін нормативно-правової бази з метою її актуалізації щодо наявної диджиталізаційної бази; д) належне стандартування, що має на меті гармонізацію українських стандартів до їх відповідників у ЄС.

Відзначимо самобутність побутування знань у царині ІБ (зокрема, у політичному вимірі останньої), досліджувану такими вченими, як В. Гайдук [26], О. Гарань [37], І. Бекешкіна [10] та ін. Науковці аналізують специфіку: а) параметризації інституційних реформ; б) інтегрування ІТ; в) захисту даних; г) боротьби з мізінформацією, дезінформацією, пропагандою; ґ) виформовування прозорого ІПр у контексті євроінтеграційних процесів [264]. Результати низки досліджень узвичаєно локалізують потребу вдосконалення української нормативно-правової бази й генезу ролі державних інституцій в ІБП, розвитку цифрової інфраструктури та кібербезпеки щодо євроінтеграційних процесів.

Особливості поточної безпекової ситуації в Україні спричинені характером російської агресії, у якій чільне місце посідають численні інформаційні кампанії та інше як інструменти воєнної стратегії. Метою цих дій є підрив авторитету, довіри та іншого щодо діяльності українського уряду, що, своєю чергою, має спричинити дестабілізацію з подальшим розгортанням громадянської війни тощо. Спектр використовуваних у цьому процесі методів доволі широкий: від фізичних та кібератак на інфраструктуру (енергетичну, інформаційну та ін.) до поширення неправдивих даних і маніпулювання громадською думкою за допомогою медіа.

Прикметним щодо вищезазначеного є трансформаційні зміни використовуваної рф методології: ідеться про розрахованість, точність та поліаспектність останніх. Так, якщо на початку ми простежуємо безпосередні атаки конкретних цілей, то на сьогодні локалізуємо актуалізацію методів соціальної інженерії. Згадаємо передовсім фішинг або обманювання громадян задля доступу до їх даних: до прикладу, славнозвісна спроба російського уряду їх викрадення. Це відбулося шляхом підробки застосунку «Резерв+» від Міноборони України, за допомогою якого військовозобов’язані могли оновити свої дані. Так, переломним стала зміна фокусу російських атак з продукування звичайних перебоїв до системи витоку чутливих даних, які можуть використовуватися для політичного, воєнного, економічного та інших

видів пресингу. Окрім того, значущими для російської агресії стають тактики, у межах яких актуалізовано довготривалі кампанії, що дестабілізують, руйнують, переривають роботу інформаційних і телекомунікаційних урядових систем тощо [9, с. 7–12].

Відзначимо позитивні зміни щодо боротьби з мізінформацією, дезінформацією та пропагандою у ЄС: помітне експонентне зростання протидії функціонуванню таких даних порівняно з 2014 р. Здебільшого це також пов'язано з відкритістю окресленої діяльності рф і прозорим демонструванням країною-агресором шляхів, методів і специфіки такої роботи. Щодо інституційної репрезентації протидії цій діяльності рф, то тут назвемо розроблені ЄС «Спільні принципи протидії гібридним загрозам» (2016 р.) [84], куди входить: а) захист критичної інфраструктури задля забезпечення цілеспрямованої комунікації й подолання інформаційних кампаній та інших гібридних загроз; б) розвиток комунікаційних систем і протидії функціонуванню неправдивих даних у ІПр, а також актуалізація медіа в стратегічних та; в) здійснення систематичної аналітики даних, що надходять не з ЄС та відслідковування трансформаційних змін смислів у них.

2016 р. ЄС ухвалив Резолюцію «Стратегічні комунікації Європейського Союзу» [258], зміст якої полягає у висвітленні механізмів, стратегій та іншого задля подолання мізінформації, дезінформації, пропаганди. Логічним продовження цього вектора дій ЄС став ухвалений «План дій проти дезінформації» (2018 р.) [225], який безпосередньо зосереджений на методах боротьби з вищезазначеною діяльністю рф (зокрема, щодо пандемії COVID-19). У документі акцентовано на потребі міжнародної співпраці в межах Великої Сімки (Групи Семи; далі – G7) та НАТО задля випрацювання ефективних методів, механізмів протидії поширенню неправдивих даних з маніпулятивною метою [257].

Загалом відзначимо позитивну динаміку в цьому напрямі ЄС: так, активно проходить розробка комплексної програми стратегії протидії мізінформації, дезінформації та пропаганди, продукованих рф. Цікаво, що така

діяльність на сьогодні розглядається в нерозривному зв'язку із зовнішньою політикою держави-агресора. Ця стратегія передбачає низку обмежень діяльності російських медіа, що використовують неправдиву інформацію для маніпулювання громадською думкою, а також актуалізацію зворотного зв'язку з громадськістю, співробітництво з освітніми, науковими та іншими установами. Окрім того, відбувається інтенсивне спростування панівних російських наративів, представлених фейковими, викривленими та іншими даними, які побутують у ІПр.

Водночас політиці ЄС у відносинах з рф притаманна непослідовність, нелогічність і неоднозначність політичних кроків [44, с. 20–23]. Ідеться передовсім про дуальність природи актуалізації рф у таких відносинах: незважаючи на питоме порушення міжнародного права, яке відбулося під час окупації АРК, ця країна є важливим складником і фігурантом низки безпекових, економічних та інших угод. Відтак рф, окрім своєї окупантської природи, має значення важливого економічного партнера, розрив відносин з яким буде мати фінансові наслідки (до прикладу, в енергетичному секторі, регіональній політиці).

Відповідно дуальність природи рф у відносинах з ЄС безпосередньо корелює з ефективністю наданої ЄС допомоги Україні й інтенсивністю інформаційної протидії такому «партнеру». До всього, це також актуалізує проблематику продуктивності євроінтеграційного процесу за таких умов. Оскільки рф так і лишиться важливим фігурантом полісистеми ЄС, а це означатиме необхідність різного роду взаємодії (політичної, економічної, культурної та інших) з нею на геополітичному рівні України, що, на нашу думку, є вкрай небажаним. Так, ми не можемо прийти в гості до знайомої родини, відвідавши при цьому одного її члена й паралельної ігноруючи інших, і, навпаки, не можна ігнорувати когось одного, взаємодіючи з іншими у «гостях».

Окреслене дає підстави висновувати потребу розробки власної ефективної стратегії протидії мізінформації, дезінформації, пропаганді, яка

має формуватися безвідносно членства у ЄС (хоча це не заважає актуалізувати його досвід). Підтвердження потреби адаптування такого досвіду є низка складностей, які спіткали Україну в процесі безпосередньої імплементації європейських практик.

Зокрема, воєнний стан та низка особливостей роботи медіа спродукували потребу виформовування самобутнього шляху протидії, що здебільшого полягає в блокуванні осередків таких даних, відслідковуванні каналів і перешкоджанні їх поширення тощо. Відзначимо також продуктивність синхронізації української ІП із санкціями проти російських медіа: зокрема, формування і першої, і других за єдиними принципами, що значно нівелювало деструктивний вплив [191].

На нашу думку, репрентативним у контексті сказаного є продукування єдиної, інтегрованої, сучасної моделі такої протидії, у межах функціонування якої має відбуватися триангулювання слідів країни-агресора за тим же принципом, за якою низка мобільних застосунків визначають «російський слід» тієї чи тієї компанії за штрих-кодом товару. Це, своєю чергою, створить низку труднощів, унеможливлюючи рф продукувати ІП, базовану на мізінформації, дезінформації та пропаганді. Значущість протидії такій політичній стратегії передовсім зумовлена підривом основ міжнародного права та порушенням полісистеми міжнаціональних відносин. Так, факт анексії АРК та окупації частини визнаних попередньо територій іншої держави рф підриває, так би мовити, практично таке право, натомість така ІП остаточно знищує його навіть на концептуальному рівні.

Виходом із такої ситуації є інвестиції в інновації та технології й продукування диджиталізації всіх сфер життя тієї чи тієї держави (зокрема, електронного врядування та ін.). Цей підхід створить сучасну, адаптивну інформаційну полісистему такої держави, водночас продукуючи появу ефективного належного інструментарію для ІБП загалом та, зокрема, боротьби ІА «на місцях»: під час роботи державних інституцій. У контексті України такий підхід, на нашу думку, є оптимальним, оскільки інноватівний вектор

розвитку сприятиме зміцненню кібербезпечного підґрунтя та його стійкості до низки викликів / небезпек / загроз.

Відтак наріжним каменем інформаційної генези української держави є адаптивність продукованих урядом стратегій до сучасних умов: зокрема, російська-українська війна є вагомою змінною такого процесу. Так, мовиться про регулярне оновлення, перегляд, удосконалення тощо підходів до СПІБ у призмі диджиталізаційних трансформацій, підвищення кваліфікації державних службовців і громадян (насамперед ідеться про медіаграмотність). Окреслене засвідчує низку кореляцій між ІП та євроінтеграцією, унаочнюючи взаємозалежну та взаємопродукувальну природу цих процесів.

Так, ІП покликана підтримати європейську аксіосферу (ціннісну парадигму), сприяючи культурогенезу й інтенсифікуючи інтегрування української самості у європейський поліконтекст. Натомість це виформовує параметризаційну специфіку ІПр України на шляху її (специфіки) євроінтеграційних трансформацій. Так, незважаючи на гібридну та інформаційну російсько-українську війну, що триває багато років (зокрема, її інтенсифікацію, що розпочалася у лютому 2022 р.), наша країна перебуває в неперервному розвиткові своїх інституційно-громадських вимірів, співпрацюючи із західними та європейськими союзниками на інформаційному фронті та інтегруючи диджиталізаційні зміни в сервісні й побутові сфери.

У контексті євроінтеграційних процесів ІП набуває особливої значущості, репрезентуючись системою стратегічних дій, метою яких є виформування інтегрованої, ефективної та сучасної комунікаційної й інформаційної інфраструктури. Окрім того, мовиться про продукування образу України як передовсім демократичного, європейського й сучасного осередку знань (даних) з потенцією до неперервного розвитку своїх інституційних та інших полісистем. У такому розумінні ІП декларована як діяльність, що має на меті підтримання зовнішньої / внутрішньої (тобто горизонтальної / вертикальної) інтеграції, обміну знаннями та досвідом задля інтенсифікації участі своїх громадян у євроінтеграційних

процесах [33, с. 102]. Продуктивним, на нашу думку, є представлення питомої природи зв'язку між ІП та євроінтеграцією (див. рис. 12):

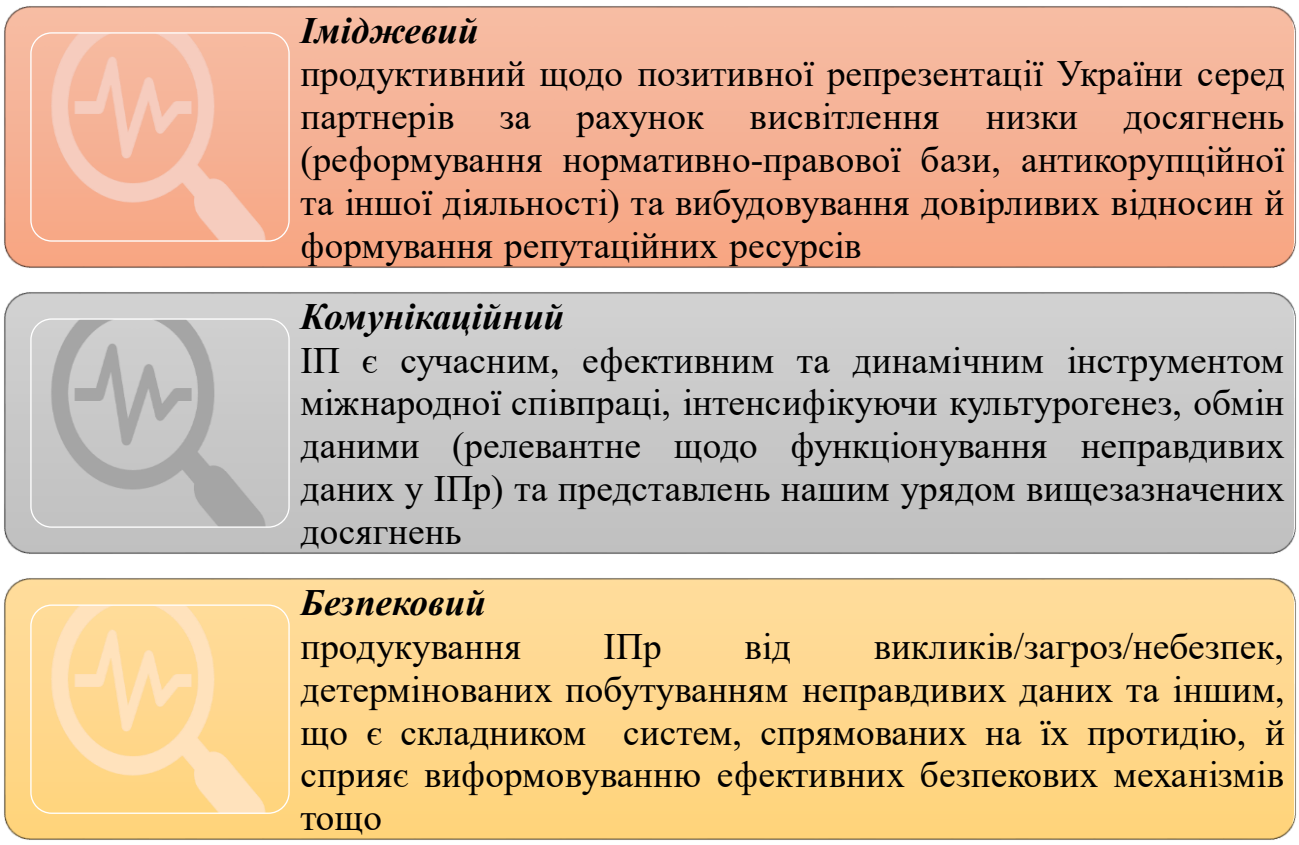


Рис. 12 Зв'язок між ІП та євроінтеграцією [191].

Природно, що стрижневою детермінантою ефективної протидії інформаційним кампаніям рф під час гібридної та ІВ стало розуміння питомої ролі державних інституцій, які мобільно, оперативно й сучасно організували відсіч нападникам шляхом ухвалення низки доцільних політичних рішень, продукуючи перелом ситуації на полі бою й ІПр. Так, вагому роль також відіграла система міжнародних відносин України, медіаграмотність її урядовців (зокрема, Мінцифри України й М. Федорова), яка інтенсифікувала інтеграцію останньої у ЄС. Саме тому ІБП України спрямована на продукування захисту, стійкості та безпеки ІПр країни, а також підвищення усвідомленості, відповідальності та націєтворчий потенціал українського єднання навколо майбутньої перемоги.

Натомість важливим складником є досвід ЄС у царині розвитку ІП як інструмента протидії російській інтервенції не лише територіального, а й ІПр нашої країни. Саме тому продукована нашим урядом інформаційна стратегія має наріжне значення для успішного інтегрування України у ЄС та гарантування стабільності її ІПр. Мовиться про ефективну взаємодію, об'єднання навколо спільної мети низки різноманітних інституційних суб'єктів (насамперед державних), які мають виформувати динамічний, актуальний та сучасний зворотний зв'язок, вплинувши на формування та актуалізацію Стратегії ІП, у межах якої доцільно актуалізувати кібербезпекові, антидезінформаційні та інші заходи, а також інтенсифікувати міжнародні відносини як джерело досвіду й натхнення для інтегрування безпекових заходів і полісистем [33; 34].

Вищезазначене суголосне тій стрижневій ролі інформації (даних) та потреби в її обробці, актуальній у межах соціального контракту сучасного інформаційного українського суспільства. Зокрема, мовиться про превалювання ресурсного підходу до даних з активним впровадженням диджиталізаційних змін.

Отже, у цьому розділі наукової роботи висвітлено диференціацію загроз ІБ як складник сучасних політичних стратегій, виокремлено роль ІВ у контексті гібридної війни на тлі російської агресії в Україні, а також відстежено самобутність здійснення ІП євроінтеграції щодо безпекового виміру інформаційного суспільства України. Зокрема, увиразнено актуальність низки питань у полісистемі НБ: захисту ІПр України та її інформаційного суверенітету як динамічного, диференційованого тощо процесу, а також специфіку диференціації ІПр у широкому спектрі викликів / загроз / небезпек.

Постульовано, що ці детермінанти, на жаль, є узвичаєними для побуту українських громадян, що дало змогу акцентувати на значущості не лише локального (цього рівня – рівня громадянина), а й державного (національного рівня) у СПІБ. Акцентовано на тому, що функціонування СПІБ зумовлене

вагомістю інформаційної агресії рф: мізінформації, дезінформації, пропаганди й кіберзагроз. Це дало змогу передовсім простежити експонентне адаптування українського суспільства до вищезазначених загроз у проміжку 2022–2024 рр. Мовиться про низку стратегій, механізмів та іншого на державному рівні та радикальне зменшення споживання контенту ворога, тенденція до переходу на українську мову частини російськомовних громадян, інші віхи генези ІПр України.

Цей процес засвідчив продуктивність актуалізації обраної урядом стратегії: низка актуалізованих ним заходів, відповідей та іншого (до прикладу, диджиталізаційний вектор розвитку, який уможливив зберегти бази даних тощо) передбачала зміцнення ІБ: кіберзахисту, розвитку медіаграмотності, міжнародного співробітництва та ін. Також заслуговує на увагу активна розробка Україною стратегій протидії інформаційним кампаніям ворога, покликаним зберегти її інформаційну атомізацію й незалежність. Ідеться, наприклад, про загальний вектор нашої країни, якому властиві інтегрованість і спрямований розвиток СПІБ, що стає базою для виформування стійкості й протидії впливу російсько-української війни.

Підкреслено, що аналіз ІВ, продукованої рф проти України, репрезентативний щодо потужної інноваційної ролі медіа як інструментарію інтенсифікації політичного дискурсу (тут – стратегій, механізмів, комунікаційної специфіки тощо) влади (зокрема, державних інституцій). Звернено увагу на стрижневу особливість використання такого засобу (медіа) ворогом, яка полягає в національній і мовній картинах світу, засобу конструювання онтологічної реальності (тут – низки політичних лакун, реалій та іншого).

Зокрема, зменшення рівня впливу мізінформації, дезінформації та пропаганди рф продуковане інтенсифікацією комунікації з громадськістю (громадянами на території України та поза її межами) й актуалізацією зворотного зв’язку, що є питомим для об’єктивної репрезентації нашої держави у світі. Своєю чергою, цей процес доцільно вибудувати шляхом:

а) *посилення медійної присутності* (контроль над репрезентованими даними, що продукує підтримку міжнародного співтовариства); б) *активне використання соціальних мереж* (надання доступної інформації широкій аудиторії й можливість висвітлення власної позиції та її донесення населенню); в) *належно вибудована комунікація з міжнародною спільнотою* (утворення коаліцій, набуття партнерської підтримки та обопільна протидія інформаційним кампаніям рф) тощо.

Природно, що стрижневою детермінантою ефективної протидії інформаційним кампаніям рф під час гібридної та ІВ стало розуміння питомої ролі державних інституцій, які мобільно, оперативно й сучасно організували відсіч нападникам шляхом ухвалення низки доцільних політичних рішень, продукуючи перелом ситуації на полі бою та ІПр. Вагому роль також відіграла система міжнародних відносин України, сучасність і медіаграмотність її урядовців (зокрема, Мінцифри України й М. Федорова), яка інтенсифікувала інтеграцію останньої у ЄС. Саме тому ІБП України спрямована на продукування захисту, стійкості та безпеки ІПр країни, а також підвищення усвідомленості, відповідальності та націєтворчий потенціал українського єднання навколо майбутньої перемоги.

Натомість важливим складником є досвід ЄС у царині розвитку ІП як інструмента протидії російській інтервенції не лише територіального, а й ІПр нашої країни. Саме тому продукована нашим урядом інформаційна стратегія має наріжне значення для успішного інтегрування України у ЄС та гарантування стабільності її ІПр. Мовиться про продуктивну взаємодію, об’єднання навколо спільної мети тощо низки різноманітних інституційних суб’єктів (насамперед державних), які мають виформувати динамічний, актуальний та сучасний зворотний зв’язок, вплинувши на формування та актуалізацію Стратегії ІП.

У межах останньої доцільно актуалізувати кібербезпекові, антидезінформаційні та інші заходи, а також інтенсифікувати міжнародні відносини як джерело досвіду й натхнення для інтегрування безпекових

заходів і полісистем. Своєю чергою, вищезазначене суголосне тій стрижневій ролі інформації (даних) та потреби у її обробці, актуальній в межах соціального контракту сучасного інформаційного українського суспільства. Характерно, що має превалювати ресурсний підхід до даних з активним впровадженням диджиталізаційних змін.

Ключовим напрямом формування інформаційної політики в контексті європейської інтеграції є актуалізація політичної участі громадян як чинника забезпечення інформаційної безпеки. Саме включення громадян у процеси ухвалення рішень, реалізація права на доступ до інформації та контроль за владою створюють умови для прозорості, підзвітності та стійкості демократичних інституцій, що, своєю чергою, зменшує ризики маніпуляцій, дезінформації та інформаційних загроз у цифрову епоху.

Відтак низка стратегій, концепцій та ініціатив тощо засвідчує готовність України до розвитку в обраному цивілізаційному векторі: останнє висвітлює те, що Україна не лише протистоїть російським інформаційним кампаніям (зокрема, інтегрованим ними наративам), а й виформовує власний. Такий український наратив має на меті підтримку внутрішнього гомеостазу й інтенсифікацію міжнародних відносин з набуттям всіх параметризаційних властивостей сучасної демократичної держави. Так, попри обмеженість наявних ІР, низку проблем економічного, соціокультурного та іншого планів, що пов’язані з війною, Україна виявляє рішучість, незламність і цілеспрямованість своєї європейської самоідентифікації.

ВИСНОВКИ

У дисертаційній роботі здійснено теоретичне узагальнення та запропоновано розв'язання актуального теоретико-прикладного завдання, що полягає у дослідженні інституційних чинників ІБП в умовах воєнного стану. Зокрема, було розв'язано такі дослідницькі завдання: а) доповнено й систематизовано теоретико-методологічні засади дослідження поняття НБ та її диджиталізаційний вимір у контексті інституційних чинників ІБП; б) висвітлено трансформаційні зміни категорійно-понятійного апарата вищезазначеної політики щодо динаміки, специфіки тощо останнього й виокремлено кореляції між поняттям НБ та ІБ; в) локалізовано самобутню генезу поняття НІ у диджиталізаційному вимірі й категоризовано, структурувано та інше, вибудувано за значущістю щодо зовнішніх/внутрішніх складників; г) відстежено особливості побутування системи ІПр, диференційовано останню щодо функційної параметризації покладених на неї питомих завдань; ґ) досліджено та сформульовано власне визначення поняття ДПМ ІБ шляхом аналізу джерельної (нормативно-правової бази) та оцінки ефективності наявних моделей останнього; д) проаналізовано сучасні виклики безпеці ІПр України в контексті параметризаційних особливостей розгортання гібридної російсько-української війни та інформаційної агресії, яка її супроводжує; е) екстрапольовано міжнародний досвід західних держав-партнерів щодо інформаційного протистояння під час гібридних й ІВ; є) ідентифіковано види наявних та потенційних загроз, продукованих рф для України, задля формування рекомендацій до адаптації й імплементації вищезазначених практик, стратегій тощо.

Проведений аналіз історіографії засвідчив специфіку феномена ІБП та локалізував його співвіднесеність з низкою інституційних чинників в умовах воєнного стану, виявивши лакунізовану природу цієї проблематики. Мовиться про інтегровану, дискурсивну та інші особливості природи останньої, що, закономірно продукує потребу у її фундаментальному аналізі в контексті

сучасних політологічних досліджень. Натомість продукування високорівневої захищеності, питомої для НІ, виформовує належні умови для сталого, динамічного й планомірного розвитку громадянина, суспільства та держави, що є стрижневим завданням ІБП. Прикметно, що головною умовою побутування останньої виступає пріоритет несилових шляхів захисту НІ (цінностей, культурної й історичної пам'яті та інших здобутків), які є її підґрунтям. У такому контексті безпеку доцільно розглядати інтегративним утворенням, концептом, у якому акумульовано всі сфери життєдіяльності суспільства, де стрижневою є інформаційна.

Подана низка визначень та історично-концептуальних підходів до поняття НБ природно спричинила потребу у репрезентації універсалізованої авторської дефініції. У межах останньої НБ позиціонуємо багатошаровим концептом, що охоплює комплекс життєво важливих інтересів громадянина, суспільства та держави від внутрішніх/зовнішніх загроз. При цьому НБ є комплексною полісистемою, функціонування якої вимагає скоординованого підходу у вищезазначених царинах, а також гнучкого, оперативного, динамічного тощо реагування на поточні реалії, виклики та загрози. До цієї полісистеми входить не лише поточне реагування на наявні загрози й виклики, а й стратегічне планування, метою якого є випередження таких проблем й превентивне їх подолання.

Своєю чергою, ІВ є актуальною проблемою сучасного світу, що продукує потребу у низці змін нормативно-правової бази, виконавчих механізмах та іншому. Зокрема, першою чергою, доцільно виструнчити концепцію НБ, доктрину ІБ, а також стратегію інформаційної боротьби. Водночас, Україна інтенсивно розробляє і впроваджує передовий досвід зарубіжних партнерів, продуктивно адаптуючи його (досвід) на своєму підґрунті: розробляючи і впроваджуючи нормативно-правові, соціальні та інші ініціативи, пов'язані з ІБ. Також відзначимо бурхливу міжнародну діяльність українського уряду: укладення низки угод, договорів та іншого, які впливають на ІБ. Вищезазначені документи суголосні диджиталізаційним

трендам, викликам, небезпекам та іншому, які стоять перед сучасною демократичною державою, якою є Україна.

Також заслуговує на увагу бурхливий розвиток ефективних, сучасних та інноваційних механізмів впровадження окреслених ініціатив та контроль їх трансформаційних змін. При цьому важливу роль, природно, відіграють інституційні чинники (державні інституції): СБУ, Міноборони України, МВС та інші, повноваження яких дотичні до питань ІБ. Прикметно, що динамічні зміни у глобальному та регіональному геополітичних дискурсах продукують потребу у постійному перегляді та вдосконаленні української законодавчої та нормативно-правової бази задля ефективного реагування на нові виклики, ІБ глобалізованого світу.

Саме тому актуальним є комплексний, фундаментальний та ґрунтовний підхід й злагоджена, інтенсивна взаємодія діяльності інституційних чинників (державних інституцій). Разом з тим згаданий ІПр позиціоновано нами стрижневим складником НБ (зокрема, розвитку ІБ), що продукує його відкритість як полісистеми, готової до змін (постійної генези, інтенсивної диджиталізації) задля зменшення впливу людського фактора на побутування ІТТ. При цьому підкреслено вагу комплексу безпекових заходів задля планомірного, поступового й логічного розвитку ІПр, що стосується, першою чергою, генези нормативно-правової бази, експонентного підвищення рівня міжінституційної координації, а також інтегрування інноваційних ІТ.

Засвідчено міжнародне співробітництво як наріжний камінь НБ (зокрема, ІБ) України, оскільки такий напрям діяльності української влади продукує: підвищення ефективності управління інформаційними потоками та захист даних; актуалізацію передового досвіду у царині НБ та ІБ, а також регулювання ІПр загалом; стратегічне планування – розробку та реалізацію довгострокових стратегій розвитку ІПр, у яких враховано не лише глобальні тенденції та специфіку розгортання, а й самобутність трансформаційних змін української держави в контексті поточної безпекової ситуації – гібридної й інформаційної російсько-української війни.

Відтак, підкреслено детермінацію вибору цілей, методів, засобів, механізмів, стратегій та іншого тими чи тим викликами, загрозами, небезпеками тощо як складниками актуалізації стрижневих напрямів ІБП. Це дозволило висвітлити інтегровану, міжвідомчу та ієрархічну природу СПІБ, структура якої корелює з відповідними елементами державного управління з чіткою координацією дій складників останньої. Відповідна ефективність такої системи детермінована оптимальністю, продуманістю, наступністю й ефективністю централізованого управління з низкою локалізованих відомчо-розпорядницьких функцій. Останні дозволяють здійснювати моніторинг та контроль над усіма вищезазначеними складниками національного ІПр. Натомість стрижневою особливістю СПІБ є її гомеостаз, що полягає у здатності до збереження питомих параметрів функціонування останньої за будь-яких ситуацій онтологічної реальності.

Вищезазначене стало підґрунтям для розуміння ІБП як дотичної до окремих аспектів організаційної культури та поведінки, у які входить робота з кадрами (навчання, підвищення кваліфікації, перепідготовка) та розробка етичних норм (стандартів, принципів та іншого) управління інформацією. При цьому її основною метою є не лише технічний захист даних, а й продукування стійкості та відповідального ставлення до ІР серед громадян та державних службовців. Підкреслено адаптивність ІБП – властивість, що полягає у інтенсифікації видозмін диджиталізаційного складника розвитку НБ (зокрема, ІБ).

Це, природно, вимагає самобутнього підходу, базованого на протидії інформаційним загрозам агресивної політики рф. У межах останньої ворогом актуалізовано комплекс заходів, механізмів, стратегій, кампаній тощо, які мають за мету занапастити ІПр України кібератаками, мізінформацією, дезінформацією та пропагандою, що актуалізують російські наративи. Значущим у цьому контексті вважаємо осягнення глибини, складності, структури й динаміки функціонування вищезазначених викликів, загроз, небезпек. Останні інтенсифікують українські стратегії, механізми тощо

продукування НБ (зокрема, ІБ), актуалізуючи потребу у їх регулярній оцінці та вдосконаленні заходів, форм, методів та тому подібного ІБП задля підтримання стабільності, належного функціонування держави в ІПр.

Увиразнено актуальність низки вищезазначених питань у полісистемі НБ: захисту ІПр України та її інформаційного суверенітету як динамічного, диференційованого тощо процесу, а також специфіку диференціації останнього в широкому спектрі викликів / загроз / небезпек. Постульовано, що вищезазначені детермінанти, на жаль, є узвичаєними для побуту українських громадян, що дало змогу акцентувати на значущості не лише локального (цього рівня – рівня громадянина), а й державного (національного рівня) у СПІБ. Акцентовано на тому, що функціонування останньої зумовлене вагомістю інформаційної агресії рф: мізінформації, дезінформації, пропаганди й кіберзагроз. Першою чергою, це дозволило спостерегти експонентне адаптування українського суспільства до вищезазначених загроз у проміжку 2022–2024 років. Мовиться про низку стратегій, механізмів та іншого на державному рівні та радикальне зменшення споживання контенту ворога, тенденцію до переходу на українську мову у побуті частини російськомовних громадян та інші віхи генези ІПр України.

Своєю чергою, вищезазначений процес засвідчив продуктивність актуалізації обраної урядом стратегії: низка актуалізованих ним заходів, відповідей та іншого (до прикладу, диджиталізаційний вектор розвитку, який дозволив зберегти бази даних тощо) передбачала зміцнення ІБ: кіберзахисту, розвитку медіаграмотності, міжнародного співробітництва та іншого. Також заслуговує на увагу активна розробка Україною стратегій протидії інформаційним кампаніям ворога, покликаним зберегти її інформаційну атомізацію й незалежність. Зокрема, мовиться про загальний вектор нашої країни, для якого властиві інтегрованість й спрямований розвиток СПІБ, що стає базою для виформування стійкості й протидії впливу російсько-української війни.

Підкреслено, що аналіз ІВ, продукованої рф проти України репрезентативний щодо потужної інноваційної ролі медіа як інструментарію інтенсифікації політичного дискурсу (тут – стратегій, механізмів, комунікаційною специфіки тощо) влади (зокрема, державних інституцій). Також звернено увагу на стрижневу особливість використання такого засобу (медіа) ворогом, яка полягає у національній і мовній картинах світу, засобу конструювання онтологічної реальності (тут – низки політичних лакун, реалій та іншого).

Зокрема, зменшення рівня впливу мізінформації, дезінформації та пропаганди рф продуковане інтенсифікацією комунікації з громадськістю (громадянами на території України та поза її межами) й актуалізацією зворотного зв'язку, що є питомим для об'єктивної репрезентації нашої держави у світі. Своєю чергою, цей процес доцільно вибудувати шляхом: а) *посилення медійної присутності* (контроль над репрезентованими даними, що продукує підтримку міжнародного співтовариства); б) *активного використання соціальних мереж* (надання доступної інформації широкій аудиторії й можливість висвітлення власної позиції та її донесення населенню); в) *належно вибудованої комунікації з міжнародною спільнотою* (утворення коаліцій, набуття партнерської підтримки та обопільна протидія інформаційним кампаніям рф) тощо.

Природно, що стрижневою детермінантою ефективної протидії інформаційним кампаніям рф під час гібридної та ІВ стало розуміння питомої ролі державних інституцій. Останні мобільно, оперативно й сучасно організували відсіч нападникам шляхом прийняття низки доцільних політичних рішень, продукуючи перелом ситуації на полі бої й ІПр. Так, вагому роль також відіграла система міжнародних відносин України, медіаграмотність її урядовців (зокрема, Мінцифри України й М. Федорова), яка інтенсифікувала інтеграцію останньої у ЄС. Саме тому ІБП України спрямована на продукування захисту, стійкості та безпеки ІПр країни, а також

підвищення усвідомленості, відповідальності та націєтворчий потенціал українського єднання навколо майбутньої перемоги.

Натомість важливим складником є досвід ЄС у царині розвитку ІП як інструмента протидії російській інтервенції не лише територіального, а й ІПр нашої країни. Саме тому продукувана нашим урядом інформаційна стратегія має наріжне значення для успішного інтегрування України у ЄС та гарантування стабільності її ІПр. Мовиться про продуктивну взаємодію, об'єднання навколо спільної мети тощо низки різноманітних інституційних суб'єктів (першою чергою, державних), які мають виформувати динамічний, актуальний та сучасний зворотний зв'язок, вплинувши на формування та актуалізацію Стратегії ІП.

У межах останньої доцільно актуалізувати кібербезпекові, антидезінформаційні та інші заходи, а також інтенсифікувати міжнародні відносини як джерело досвіду й натхнення для інтегрування безпекових заходів й полісистем. Своєю чергою, вищезазначене суголосне тій стрижневій ролі інформації (даних) та потреби у її обробці, актуальній в межах соціального контракту сучасного інформаційного українського суспільства. Характерно, що має превалювати ресурсний підхід до даних з активним впровадженням диджиталізаційних змін.

Відтак, низка стратегій, концепцій та ініціатив тощо засвідчує готовність України до розвитку у обраному цивілізаційному векторі: підкреслюючи те, що країна не лише протистоїть російським інформаційним кампаніям (зокрема, інтегрованим ними наративам), а й виформовує власний. Такий український наратив має на меті підтримку внутрішнього гомеостазу й інтенсифікацію міжнародних відносин з набуттям всіх параметризаційних властивостей сучасної демократичної держави. Так, попри обмеженість наявних ІР, низку проблем економічного, соціокультурного та іншого планів, що пов'язані з війною, Україна виявляє рішучість, незламність та цілеспрямованість своєї європейської самоідентифікації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. Алямкін Р. Правове забезпечення національної інформаційної безпеки. *Наукові записки Інституту законодавства Верховної Ради України*. 2013. № 4. С. 91–96.

2. Арістова І.В. Державна інформаційна політика та її реалізація в діяльності ОВС України: організаційно-правові засади. *Дис. д-ра. юрид. наук: 12.00.07. Націон. ін-т внутр. справ*. Харків, 2002. 408 с.

3. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти. *МВС України, Ун-т внут. справ*. Харків, 2000. 366 с.

4. Бабенко Ю. Інформаційна війна – зброя масового знищення. URL: http://www.pravda.com.ua/rus/articles/2006/04/20/4399050/ (дата звернення: 05.12.2023).

5. Баранов А. Інформаційний суверенітет чи інформаційна безпека? *Нац. безпека і оборона*. 2001. № 1(13). С. 70-76.

6. Беззуб І. Нова Воєнна Доктрина: керівництво до дії чи декларація? URL:http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=1459:bezpeka1&catid=8&Itemid=350 (дата звернення: 06.11.2023).

7. Березовська-Чміль О. Інформаційна безпека як складова соціальної стабільності держави. *Соціально-гуманітарний вісник: зб.наук.пр. Вип. 37*. Харків: СГ НТМ «Новий курс», 2021. С. 69-70.

8. Березовська-Чміль О.Б. Національна безпека України в контексті інтеграції до Європейського Союзу: політико-правовий аспект (2014–2019 рр.). *Politicus. Науковий журнал. Спецвипуск*. ВД «Гельветика», 2022. С. 7-14. (у співавт. з Кобець Ю.В., Міщук М.Б.)

9. Березовська-Чміль О.Б. Соціальні аспекти національної безпеки держави. *Прикарпатський вісник НТШ. Думка*. 2019. № 6 (50). С.7-12.

10. Бекешкіна І. Є. Інформаційна безпека України: соціологічний вимір. *Київ: Інститут соціології НАН України,* 2011. с. 240.

11. Біленець Д. А., Веселий В. С., Возняковська К. А., Волощук О. Т., Демчук Т. І., Латковська Т. А., Марчук В. В., Глиняний І. В., Факас І. Б. Національна безпека України в реаліях масштабної військової агресії: колективна монографія; *За заг. ред. К. А. Возняковської.* - *Чернівці,* 2024. С. 380.

12. Біленчук П. Д., Борисова Л. В., Неклонський І. М., Собина В. О. Правові засади інформаційної безпеки України. Харків, 2018. 289 с.

13. Білько С. Інституційне забезпечення інформаційної безпеки України. Економіка і регіон. – 2021. – №3 (82). С. 43–45.

14. Богданович В.Ю. Роль та місце воєнно-політичної моделі держави у розробленні та здійсненні політики забезпечення воєнної безпеки. *Наука і оборона*. 1999. № 1. С. 34-37.

15. Богуш В., Юдін О. Інформаційна безпека держави. *Гол. ред. Ю. О. Шпак. -К.: "МК-Прес"*. Київ. 2005.

16. Боднар І. Р. Інформаційна безпека як основа національної безпеки. *Механізм регулювання економіки*. 2014. № 1. С. 68–75.

17. Боднар І.Р. Державна політика та інформаційна безпека України: післякризові виклики. *Актуальні проблеми післякризового відновлення економіки України: зб. матер. наук.-практ. конф*. Львів, 2013. С. 29-32.

18. Боднарчук О.В. Політичні комунікації в євроінтеграційному курсі України. *Дис. ... канд. наук: 25.00.02. Державний вищий навчальний заклад «Прикарпатський національний університет імені Василя Стефаника*. Івано-Франківськ, 2015. 199 с.

19. Бодрук О. С. Структури воєнної безпеки: національний та міжнародний аспекти. Київ, 2001. 300 с.

20. Бондаренко В. О., Литвиненко О. В. Інформаційна безпека сучасної держави: концептуальні роздуми. URL: http://www.crime-research.iatp.org.ua/library/strateg.html (Дата звернення 28.11.2023).

21. Брижко В. М., Гальченко О. М., Цимбалюк В. С. та ін. Інформаційне суспільство. Дефініції: людина, її права, інформація,

інформатика, інформатизація, телекомунікації, інтелектуальна власність, ліцензування, сертифікація, економіка, ринок, юриспруденція. *Інтеграл*. Київ: 2002.

22. Величко А., Волощук І. Національні інтереси, національні цінності та національні цілі як структуроформуючі чинники політики національної безпеки. *Гілея: науковий вісник*, 2014, Вип. 84 (№5), С. 465–471.

23. Власюк О. С. Національна безпека України: еволюція проблем внутрішньої політики. *НІСД*. Київ: 2016. 528 с.

24. Войтенко О.Г., Рачковська Л.В. Інформаційна війна Російської Федерації проти України: методи, засоби, наслідки. *Державний інститут керівних кадрів*. Київ. 2018. С.16-22.

25. Ворожко Т. Ґрунт готувався століттями: Експерти – про російську пропаганду. URL: https://nv.ua/ukr/opinion/chomu-rosiyani-pidtrimuyut-viynu-putina-proti-ukrajini-propaganda-rosiji-ostanni-novini-50227642.html (дата звернення 23.03.2022).

26. Гайдук В. О. Інформаційна безпека України: проблеми та перспективи розвитку. *Київ: Наукова думка,* 2010. с. 320.

27. Галіпчак В. Сучасні виклики та стратегії забезпечення інформаційної безпеки України в умовах російської агресії: перспективи та завдання. *Науковий журнал «Регіональні студії»*, 2023. №35. С. 65-70.

28. Галіпчак В. Безпека інформаційного простору України в умовах російської агресії на сучасному етапі: основні завдання та виклики. *Науковий журнал «Регіональні студії»*, 2023. №34. С. 81-85.

29. Галіпчак В. Вплив інформаційних технологій на захист національних інтересів в Україні: виклики та можливості. *X Міжнародна науково-практичніа конференція «Пріоритетні шляхи розвитку науки і освіти»* (м. Львів, 29-30 листопада 2023 року). URL: http://www.lviv-forum.inf.ua/save/2023/29-30.11/Збірник.pdf

30. Галіпчак В. Державно правовий механізм забезпечення інформаційної безпеки. *Матеріали III Всеукраїнської науково-практичної*

конференції «Політичні процеси сучасності: глобальний та регіональний вимір» (м.Івано-Франківськ, 27-28 травня 2021р.).

31. Галіпчак В. Державно-правовий механізм здійснення інформаційної безпеки: агенти і методи впливу. *Матеріали Всеукраїнської науково-практичної конференції «Теоретичні та практичні аспекти політичного розвитку в Україні і світі в умовах повномасштабної російсько-української війни (пам'яті Любомири Мандзій)»* (м.Львів, 10 травня 2023р.). URL: https://filos.lnu.edu.ua/wp-content/uploads/2023/05/Conf_Program_May23.pdf

32. Галіпчак В. Державно-правовий механізм інформаційної безпеки України в умовах російської агресії. *Політикус*, 2023. №5. С. 19-24.

33. Галіпчак В. Інституційні чинники інформаційної політики євроінтеграції України: безпековий вимір. *Політикус*, 2023. №3. С. 97-102.

34. Галіпчак В. Основні методологічні засади поняття національної безпеки: інформаційний вимір. *POLITIA. Вісник наукових робіт молодих вчених*. Івано-Франківськ: ЯРИНА, 2023. Вип. 5. С. 192–225. URL: https://kpip.pnu.edu.ua/wp-content/uploads/sites/121/2023/04/politia-5.pdf

35. Галіпчак В. Роль інституційних механізмів у забезпеченні інформаційної безпеки: аспекти управління та взаємодії. *IX Міжнародна науково-практична конференція «Практичні та теоретичні питання розвитку науки та освіти»* (м. Львів, 29-30 жовтня 2023 року). URL: http://www.lviv-forum.inf.ua/save/2023/29-30.10/Збірник.pdf

36. Галіпчак В. Трансформація інформаційного простору України під впливом російської агресії: зміни та виклики. *Політикус*, 2023. №4. С. 26-31.

37. Гарань О. В. Інформаційна політика України: виклики та загрози національній безпеці. *Київ: Фенікс,* 2012. С. 256.

38. Герасимов, І. Інформаційна війна ізоляції: російська агресія проти України в медійному просторі. *Інститут медіафорсайт*. Вінниця, 2018. С. 22-24.

39. Геращенко А.М., Поліщук І.М. Інформаційна війна: сучасні виклики та загрози національній безпеці. *Кондор*. Київ, 2016. С. 155.

40. Гіда О. Ф. Інформаційно-психологічні атаки як одна з форм реалізації технологій деструктивного впливу на суспільство. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2015. № 1. С. 153-158.

41. Глобенко С. Інформаційний простір держави та проблеми забезпечення його захисту в Україні. *Науковий вісник: Державне управління*. 2023. № 1. С. 195–210. https://doi.org/10.33269/2618-0065-2023-1(13)-195-210 *Науковий вісник: Державне управління* : вебсайт. URL: https://goo.su/tNDyJ (дата звернення: 17.08.24).

42. Гнатовський М.М. Становлення та тенденції розвитку європейського правового простору. *Київський національний університет імені Тараса Шевченка*. Київ, 2002. 193 с.

43. Головне управління розвідки Міністерства оборони України. *Головне управління розвідки Міністерства оборони України*: вебсайт. URL: https://goo.su/1c9AjyE (дата звернення: 17.08.24).

44. Голуб'як Н., Кобець Ю. Оборонна та безпекова політика Європейського Союзу: суперечності трансформації. *Науково-теоретичний альманах Грані*. 2023. Вип. 5. С. 19-25.

45. Гонцяж Я., Гнидюк Н. Свобода інформації та виконавча гілка влади: Правові норми. Інституції. Процедури. *Міленіум*. Київ, 2002. 240 с.

46. Гончаренко О.М., Лисицин Є.М. Методологічні засади розробки нової редакції концепції національної безпеки України. *Національний інститут стратегічних досліджень. Серія «Національна безпека»*. Випуск 4, 2001.

47. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення. *Вісник Національної академії державного управління при Президентові України*. 2015. № 1. С. 136-141.

48. Горбулін В. П. Національна безпека України та міжнародна безпека. *Політична думка*. 1997. № 1. С. 76-89.

49. Горбулін В. Тези до другої річниці російської агресії проти України. URL: http://uacrisis.org/ua/40347-gorbulin-tezy (Дата звернення: 28.11.2023).

50. Горленко В. В. Формування сучасного громадянського суспільства в Україні: особливості впливу держави. *Вчені записки Таврійського національного університету імені В. І. Вернадського*. 2019. № 4. С. 221–226.

51. Гриценко В. Гібридна війна Росії проти України: інформаційні аспекти. *Інформаційна безпека України: виклики та загрози*. Київ, 2017. 220 с.

52. Гурковський В. І. Інформаційна безпека в Україні як складова національної безпеки. *Наукові праці Української академії державного управління*. 2002. № 2. С. 9-18.

53. Гурковський В. Механізми використання інформації в умовах Російської гібридної агресії. *Освіта регіону*. 2016. № 4. С. 16-23.

54. Гурковський В.І. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки. Київ, 2004. 225 с.

55. Гурковський В.І. Розбудова інформаційного суспільства в Україні в умовах сьогодення: практичні аспекти. URL: http://www.dy.nayka.com.ua/?op=1&z=228 (Дата звернення: 16.11.2023).

56. Гусаров В. Кремль розпочав нову інформаційну операцію проти України. URL: http://osvita.mediasapiens.ua/material/34281 (Дата звернення: 14.11.2023).

57. Даниленко С., Пацьора Ж. Комунікаційні стратегії НАТО в контексті російсько-української війни. *Актуальні проблеми міжнародних відносин.* 2024. Том 1 № 158, с.36-42.

58. Декларація принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті». *Верховна Рада України.* Офіційний

вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/995_c57?find=1&text=%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81#w1_2 (дата звернення 06.12.2023).

59. Дерев’янко С. Гібридна війна: інформаційний вимір. *Національна і регіональна безпека в умовах інформаційної війни*. Матеріали Міжрегіон. наук.-практ. конф. Івано-Франківськ, 30.11.2018. Івано-Франківськ, 2018. С. 62–67.

60. Дерев’янко С.М. Безпековий вимір народовладдя в умовах гібридної війни. *Держава і право: зб. наук. пр. Серія. Політичні науки*. Вип. 87. Ін-т держави і права ім. В. М. Корецького НАН України. Київ, "Юридична думка", 2020. С. 308–318.

61. Дерев'янко С. М. Гібридна війна: інформаційно-безпековий вимір. *Вісник Прикарпатського університету. Серія: Політологія,* 2024, Вип. 18, с. 11–18.

62. Державна служба спеціального зв’язку та захисту інформації України. *Вебсайт. URL:* https://goo.su/txUNZZd (дата звернення: 17.08.24).

63. Державна служба спеціального зв’язку та захисту інформації України. Річний звіт про кіберінциденти та заходи кібербезпеки (2022–2023). *Вебсайт – URL*: https://cip.gov.ua (дата звернення: 07.12.24).

64. Державне бюро розслідувань. Державне бюро розслідувань: вебсайт. URL: https://goo.su/eqMrKZ (дата звернення: 17.08.24).

65. Державний комітет телебачення і радіомовлення України. Державний комітет телебачення і радіомовлення України: вебсайт. URL: https://goo.su/Znbi5 (дата звернення: 17.08.24).

66. Дерев’янко С. Народовладдя у безпековому вимірі. *Актуальні проблеми політики, інформації та безпеки: монографія*. Прикарпат. нац. ун-т ім. В. Стефаника. Івано-Франківськ, "Ярина", 2022. С.4–29.

67. Дерев’янко С., Марчук В. Рецензія на монографію Матвієнків С.М. «Регіональні ЗМІ: функціональні особливості та вплив на інформаційний

простір держави (досвід Івано-Франківщини)». *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2022. № 1 (12). С. 161–164. DOI: https://doi.org/10.29038/2524-2679-2022-01-161-164.

68. Джил Догерті (Jill Dougherty). Усі брешуть, або як трансформувалися російські ЗМІ. URL: http://osvita.mediasapiens.ua/material/33880 (Дата звернення: 11.11.2019).

69. Дзьобань О. П. Інформаційна безпека: нові виміри загроз, пов'язаних із інформаційно-комунікаційною діяльністю. 2015.

70. Дзьобань О.П. Формування інформаційної картини світу як результат відображення генезису базових форм буття. *Матеріали "круглого столу" Проблема інформаційного суспільства: соціально-правовий аналіз*. Полтава, ТОВ "Фірма "Техсервіс", 28 лют. 2013. С. 26-36.

71. Дзюбань О. П. Національна безпека в умовах соціальних трансформацій (Методологія дослідження та забезпечення). *Константа*. Харків, 2006. 324 с.

72. Дніпренко Н. К. Зміна парадигми в державному управлінні інформаційною сферою: *Теорія та історія державного управління*. 2005. С.20

73. Добровольська А. Інформаційний простір: проблеми становлення нової якості національного росту. *Наука України у світовому інформаційному просторі*. Вип. 3, 2010. С. 61–70.

74. Довгань О.Д., Ткачук Т.Ю. Система інформаційної безпеки України: онтологічні виміри. *Інформація і право*. № 1(24)/2018. С.89-103.

75. Долженко К. І. Нормативно-правове регулювання інформаційної безпеки регіону. *Право і Безпека*. 2014. № 3. С.43-48.

76. Доповідь про стан та розвиток інформатизації в Україні за 2009 рік. Офіційний вебпортал. URL: http://zakon.nau.ua/ doc/?uid=1064.1305.0 (дата звернення 16.11.2019).

77. Дослідження Інституту масової інформації про пропагандистські наративи у медіа-просторі України (2021–2023). Вебсайт –URL: https://imi.org.ua (дата звернення 28.10.2024).

78. Дубас О. П. Інформаційний розвиток сучасної України у світовому контексті. *Генеза*. Київ. 2004. С. 96.

79. Дубняк К. А. Інформаційний простір: структура функціональні параметри. *Держава та регіони. Серія: Соціальні комунікації.* 2015. № 4(24). С. 21–25.

80. Дуцик Д. Українська інформаційна політика в умовах війни: критичні зауваження. *Протидія російській інформаційній агресії: спільні зусилля задля захисту демократії. Аналітичний звіт. Телектирика.* Київ. 2015. С. 77.

81. Європейська Рада ЄС. Європа і глобальне інформаційне суспільство: рекомендації для Європейської Ради ЄС. *Брюссель: Європейська Рада,* 1994, с. 45. Вебсайт - URL: https://ec.europa.eu/digital-strategy/communication_en (дата звернення 28.10.2024).

82. Європейський Парламент та Рада Європейського Союзу. Директива (ЄС) 2022/2555 від 14 грудня 2022 року про заходи для високого загального рівня кібербезпеки в Союзі (NIS 2). *Офіційний вісник Європейського Союзу, L 333,* 27 грудня 2022, с. 80–119.

83. Європейська Комісія. Акт про цифрові послуги (Digital Services Act) – Регламент (ЄС) 2022/2065 від 19 жовтня 2022 року про єдиний ринок цифрових послуг. *Офіційний вісник Європейського Союзу, L 277*, 27 жовтня 2022, с. 1–102. Вебсайт –URL: https://eur-lex.europa.eu/legal-content/UK/TXT/?uri=CELEX%3A32022R2065 (дата звернення 28.10.2024).

84. Європейська Комісія. Спільні принципи протидії гібридним загрозам (2016 р.). *Брюссель: Європейська Комісія, 2016,* с. 35. Вебсайт – URL: https://eur-lex.europa.eu/legal content/UK/TXT/?uri=CELEX%3A52016DC0415 (дата звернення 28.10.2024).

85. Єрмак О.М., Шевченко С.М. Інформаційна війна в контексті гібридної війни Росії проти України. *Інститут національної безпеки*. Київ. 2017. С. 12-21.

86. ЄС розпочинає найбільший проєкт підтримки цифрової трансформації України із загальним бюджетом 17,4 млн євро. *Представництво Європейського Союзу в Україні*: вебсайт. URL: https://goo.su/UrlnxbM (дата звернення: 17.08.24).

87. Єсімов С. Шляхи удосконалення нормативно-правового регулювання в сфері інформаційної безпеки. URL: http://webcache.googleusercontent.com/search?q=cache:IEH_xfZJ2cQJ:irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe%3FC21 COM%3D2%26 I21DBN%3DUJRN%26P21DBN%3DUJRN%26IMAGE_FILE_DOWNLOAD% 3D1%26Image_file_name%3DPDF/Nzlubp_2013_11_21.pdf (Дата звернення: 05.12.2023).

88. Єфімова В. В. Державна інформаційна політика України в контексті інтеграції в Європейський Союз. *Вісник Національної академії оборони України*. 2009. № 3 (11). С. 203.

89. Загирняк, М. Інформаційна війна Росії проти України: особливості, методи та наслідки. *"Гібридна війна": виклики та загрози національній безпеці України.* Київ. 2015. С. 42.

90. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» від 12.07.2001 №2759. *Офіційний вебпортал: Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/1644-15 (дата звернення 28.10.2024).

91. Закон України "Про доступ до публічної інформації" від 13 січня 2011 року № 2939-VI. *Офіційний вебпортал: Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/2939-17 (дата звернення 28.10.2024).

92. Закон України «Про державну таємницю» від 21.01.1994 №3855. *Офіційний вебпортал: Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/3855-12 (дата звернення 28.10.2024).

93. Закон України «Про електронний цифровий підпис» від 22.05.2003 № 852. *Офіційний вебпортал: Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/852-15#Text (дата звернення 07.12.2023).

94. Закон України «Про електронну комерцію» від 3 вересня 2015 року № 675-VIII. *Офіційний вебпортал: Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/675-19 (дата звернення 07.12.2023).

95. Закон України про інформацію від 02.10.1992 №2657. *Офіційний вебпортал: Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення 07.12.2023).

96. Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 № 851-IV. *Офіційний вебпортал: Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення 07.12.2023).

97. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 1994 року. *Київ: Верховна Рада України,* 1994. Вебсайт: URL: https://ips.ligazakon.net/document/Z008000 (дата звернення 28.10.2024).

98. Закон України «Про національну безпеку України» від 2018 р. №31. *Офіційний вебпортал: Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення 07.12.2023).

99. Закон України «Про Національну систему конфіденційного зв'язку України» від 2022р. №45. *Офіційний вебпортал: Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/1706-20 (дата звернення 28.10.2024).

100. Закон України «Про основи національної безпеки України» від від 19.06.2003 № 964-IV. *Офіційний вебпортал: Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/964-15#Text (дата звернення 07.12.2023).

101. Закон України «Про основні засади забезпечення кібербезпеки України» від 2017 р. *Офіційний вебпортал: Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 07.12.2023).

102. Залєвська І.І., Удренас Г.І. Інформаційна безпека України в умовах російської військової агресії. *Південноукраїнський правничий часопис*. 2022. № 1-2. С. 20-26.

103. Захаренко К. Відкритість інформаційного простору та контроль за доступністю інформації. 2020. Вип. 14. С. 46–55.

104. Захаренко К. Глобальна природа інформаційної безпеки. *Політологічний вісник*. 2015. Вип. 79. С. 181–189.

105. Захаренко К. Держава як суб'єкт інформаційної безпеки суспільства. *Політологічний вісник*. 2015. Вип. 78. С. 86–96.

106. Захаренко К. Диверсифікація джерел інформації в контексті інформаційної безпеки. *Политикус*. 2019. № 1. С. 5–9.

107. Захаренко К. До питання про розвиток національної системи інформаційної безпеки: досвід сусідів. *Вісник Харківського національного педагогічного університету імені Г. С. Сковороди*. *Філософія.* 2018. Вип. 50. С. 176–189.

108. Захаренко К. Інформаційна безпека суспільства як предмет правового регулювання. *Гілея: науковий вісник*. 2019. Вип. 148. С. 26–31.

109. Захаренко К. Міжнародний досвід інформаційної безпеки. *Сучасне суспільство: політичні науки, соціологічні, культурологічні науки*. 2019. Вип. 1 (17). С. 95–109.

110. Захаренко К. Політичні інститути інформаційної безпеки України: трансформація, модернізація, розвиток. *Вид-во НПУ імені М.П. Драгоманова*. Київ. 2017. С. 389.

111. Захаренко К. Стратегія формування ефективної системи державної інформаційної безпеки. *Гілея: науковий вісник*. 2018. Вип. 131. С. 268–272.

112. Захаренко К. Чинники здійснення державної інформаційної політики України. *Регіональні студії*. 2019. № 17. С. 15–19.

113. Захаренко К. В. Інституційний вимір інформаційної безпеки України: трансформаційні виклики, глобальні контексти, стратегічні орієнтири: дис. … 23.00.02 / Львівський національний університет імені Івана Франка. Львів, 2021. 287 с. *Львівський університет*: вебсайт. URL: https://goo.su/hZIbd (дата звернення: 17.08.24).

114. Звіт Державної служби спеціального зв'язку та захисту інформації України про кіберінциденти за 2021–2023 роки. *Вебсайт - URL:* https://cip.gov.ua (дата звернення 07.12.2024).

115. Звіт РНБО України про інформаційні витоки в державному секторі за 2021–2023 роки. *Вебсайт - URL:* https://www.rnbo.gov.ua (дата звернення 07.12.2024).

116. Звіт StopFake.org про російську дезінформацію та її вплив на український інформаційний простір. *330 відтінків російської дезінформації: досліджуємо інформаційний простір Східної Європи. 2022. Вебсайт - URL:* https://www.stopfake.org/uk/330-vidtinkiv-rosijskoyi-dezinformatsiyi-doslidzhuyemo-informatsijnij-prostir-shidnoyi-yevropi/ (дата звернення 07.12.2024).

117. Зіма І.І, Ніколаєв І.М. Інформаційна війна та інформаційна безпека (огляд думок зарубіжних політологів та воєнних спеціалістів). *Наука і оборона*. 1998. С. 56 – 58.

118. Зозуля О. С. Державне управління забезпеченням інформаційної безпеки України в умовах інформаційно-психологічного протиборства; *дис. ... канд. наук з держ. упр.: 25.00.01. НАДУ.* Київ. 2017. С. 251.

119. Золотова М. «Інформаційна війна Росії в Україні та кібербезпека». URL: вебсайт: https://www.radiosvoboda.org/a/28580039.html (дата звернення 28.10.2024).

120. Зубков Д. «Інформаційно-комунікаційна діяльність та аналітика під час російсько-української війни на прикладі соціальних мереж». 2023 р., №23, с.156–163. *URL: вебсайт:* https://www.researchgate.net/publication/373894315 (дата звернення 28.10.2024).

121. Іваненко Д. Кібербезпека в контексті гібридної війни: виклики та стратегії. Київ. 2020. С. 234.

122. Іваницька О. М. «Основні методи пропаганди в російському інтернет ЗМІ «Правда». *Вісник Національного університету „Львівська політехніка“. Серія: Журналістика,* 2019, №3, с. 87–93.

123. Іванов, О. Інформаційна безпека України: сучасний стан та виклики. *Національний інститут стратегічних досліджень*. Київ, 2019 с. 124.

124. Іванова Є. І. Воєнно-інформаційна безпека України за умов ескалації конфлікту на Сході України. 2022. С. 20-26.

125. Іванова, О.М. Дослідження сучасних технічних та стратегічних аспектів кібербезпеки, ідентифікація загроз та рекомендації для їхнього подолання. *Кібербезпека та Сучасні Загрози: Аналіз і Стратегії*. Київ. 2020.

126. Інститут масової інформації. Моніторинг впливу пропаганди та дезінформації у регіональному розрізі (2021–2024). Вебсайт – URL: https://imi.org.ua (дата звернення 07.12.2024).

127. Інститут масової інформації. Моніторинг дезінформації та інформаційних загроз в Україні (2021–2024). Вебсайт – URL: https://imi.org.ua (дата звернення 07.12.2024).

128. Інформаційна війна Росії: особливості та методи впливу на Україну. *Збірник наукових праць Інституту військових стратегічних досліджень.* Київ, 16-22 с.

129. Інформаційна складова війни. *Сайт:Радіо Свобода.* URL: https://www.radiosvoboda.org/a/informatsiyna-viyna-rosiyskyy vplyv/31811302.html (дата звернення 08.12.2023).

130. Інформаційне повідомлення. Негативне ставлення українців і росіян одне до одного виросло врази. *Сайт: Українська правда.* URL: http://www.pravda.com.ua/news/2014/06/17/7029323/ (дата звернення 14.11.2023).

131. Інформаційне повідомлення. Радник Путіна запропонував вдарити по українській армії, поки вона не зміцніла. *Сайт: Уніан.* URL: http://www.unian.net/politics/926969 - sovetnik-putina-predlojil-udarit-po-ukrainskoy-armiichtobyi-ne-dat-ey-okrepnut.html (дата звернення 08.11.2023).

132. Кабінет Міністрів України. Основні положення Національної програми інформатизації. *Київ: Кабінет Міністрів України,* 1998, с.56.

Вебсайт – URL: https://www.kmu.gov.ua/document/67890 (дата звернення 28.10.2024).

133. Кавун С.В., Носов В.В., Манжай О.В. Інформаційна безпека. *Вид. ХНЕУ*. Харків, 2018. Ч. 2. С. 196.

134. Калюжний Р. А., Шамрай В. О., Павловський В. Д. та ін.; за ред. Р. А. Калюжного та В. О. Шамрая. Інформаційне забезпечення управлінської діяльності в умовах інформатизації: організаційно-правові питання теорії і практики. *АДПС України*. Київ, 2002. С. 296.

135. Калюжний Р. А., Новицька Н. Б. Становлення інформаційного суспільства. *Правова інформатика*. 2006. №3 (11), С. 17-22.

136. Катренко А. Особливості інформаційної безпеки за міжнародними стандартами. *Альманах економічної безпеки*. 1999. № 2, С. 15-17.

137. Качинський А. Б. Стратегічне планування: вирішення проблем національної безпеки. *Київ: НІСД,* 2010. с.166.

138. Кирильчук Є. Проблеми національної інформаційної безпеки України в контексті сучасних національних державотворчих процесів та світової інтеграції. *Наукові праці МАУП*. 2013. Вип. 1 (36), С. 60–63.

139. Кісілевич-Чорнойван О. Інформаційна безпека та міжнародна інформаційна безпека: проблема визначення понять. *Юриспруденція: теорія і практика*. 2009. № 8, С. 11–18.

140. Климовський С. Гібридна війна в Україні, як пролог глобальної війни. *Сайт: Вартайм.* URL: http://wartime.org.ua/18985-gbridna-vyna-v-ukrayin-yak-prolog-globalnoyi-vyni.html (Дата звернення: 06.07.2023).

141. Кобець Ю. В., Кобець Т. А. Теоретико – методологічні підходи до дослідження політичної безпеки. *Політичні процеси сучасності: глобальний та регіональні виміри*. *Матеріали IV Всеукраїнської науково-практичної конференції.* Івано-Франківськ, 27-28 жовтня 2022. С. 45-51.

142. Кобець Ю., Міщук М. Особливості інтеграції ЄС і України в умовах “гібридної війни”: безпековий вимір. *Соціально-гуманітарний вісник*. Вип. 32-33. Харків: "Новий курс", 2020. С.190-192.

143. Кобець Ю.В. «Гібридна війна» як загроза національній безпеці: основні підходи та тлумачення. *Національна і регіональна безпека в умовах інформаційної війни*. *Матеріали Міжрегіональної науково-практичної конференції.* Івано-Франківськ, 2019. С. 82-86.

144. Кобець Ю. В. Національна безпека України в контексті інтеграції до Європейського Союзу: політико-правовий аспект. *Івано-Франківськ: Плай, 2020.* Вип.14. С. 97-102.

145. Козьміних А. В. Інформаційні механізми євроінтеграційної політики України. *Актуальні проблеми політики*. Вип. 65. Одеса: "Гельветика", 2020. С. 41-48.

146. Комплексна програма створення єдиної національної системи зв'язку 1993 року. *Київ: Кабінет Міністрів України,* 1993. URL: https://www.kmu.gov.ua/ua/docs/1993-programa-evropeyzacziya (Дата звернення: 28.10.24).

147. Конах В. Забезпечення інформаційної безпеки держави як складової системи національної безпеки (приклад США). *Автореф. дис. канд. політ. н. (спеціальність: 21.01.01 – основи національної безпеки держави).* Київ, 2005. 20 с.

148. Конвенція про кіберзлочинність (Будапештська конвенція). *Страсбург: Рада Європи,* 2001, с.35. Вебсайт: URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention (дата звернення 28.10.2024).

149. Кондратьєв Я. Ю., Ліпкан В. А. Концепція національної безпеки України: теоретико правові аспекти зарубіжного досвіду. *Національна академія внутрішніх справ України*. Київ, 2003. 20 с.

150. Конституція України від 28.06.1996 ст.30. Офіційний вебпортал: Президент України. URL: https://www.president.gov.ua/documents/constitution (дата звернення 08.12.2023).

151. Копійка М. Інституціональний концепт інформаційної безпеки України. *Деокупація і реінтеграція інформаційного простору Криму:*

міжнародно-правові та медіакомунікаційні інструменти: матеріали міжнародної науково-практичної конференції. Київ, 18 квітня 2019 року. Київ, 2019. С. 17–22.

152. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України. *Монографія*. Одеса: Юридична література, 2003. С. 472.

153. Кормич БА. Інформаційна безпека України: організаційно-правові основи. *Навчальний посібник*. Київ: Кондор, 2004. 384 с.

154. Корнієнко С. Путін веде в Україні гібридну війну – Генерал Каппен. *Сайт: Радіо Савобода.* URL: http://www.radiosvoboda.org/content/article/25363591.html(дата звернення 05.12.2023).

155. Корольов М. Проблематика дослідження питань інформаційної безпеки у державному управлінні. *Вісник Східноукраїнського національного університету ім. В. Даля*. 2013. № 15(1). С. 88–92.

156. Косогов О.М. Пріоритетні напрямки державної політики щодо забезпечення безпеки національного кіберпростору. *Збірник наукових праць Харківського університету Повітряних Сил*. Харків: ХУПС, 2014. Вип. 3 (40). С. 127-129.

157. Косогоров О., Сірик А. Основні проблемні питання та напрями підвищення ефективності державної інформаційної політики України в умовах гібридної війни. *Інформаційний вимір гібридної війни: досвід України: матеріали міжнародної науково-практичної конференції*. Київ: НУОУ, 2017. С. 44–46. URL: https://nuou.org.ua/assets/documents/zbirn-gibr-mizhn-konf.pdf

158. Кочубей Л.О. Інформаційна безпека держави: інструменти захисту українського інформаційного поля (на прикладі особливостей інформаційно комунікаційних технологій у сучасному Донбасі. *Наукові записки Інституту політичних і етнонаціональних досліджень імені І. Ф. Кураса*. 2015. Вип. 3. С. 220-237.

159. Кравець Є. Інформаційна безпека держави. *Юридична енциклопедія: У 6 т. Ред. кол.: Ю. Шемшученко (голова редкол.) та ін.* Київ: Укр. Енцикл., 1998–1999. Т. 2. С. 714–715.

160. Кравець Є. Національна безпека України: до концепції законодавства. *Вісник АН України*. 1994, № 1, С. 83-90.

161. Кравченко Ю. Кібербезпека в Україні: проблеми та перспективи. Київ, 2022. С. 198

162. Крилова Н. Підходи до визначення і розуміння поняття «інформаційна безпека» в рамках національного безпекознавства. *Гілея: науковий вісник: зб. наук. пр.* 2010. Вип. 36. С. 423−428.

163. Кузьмінська Р.В. Забезпечення інформаційної безпеки України в умовах російсько-української війни. Київ, 2023. С. 38-42.

164. Левицька М.Б. Теоретико-правові аспекти забезпечення національної безпеки України органами внутрішніх справ України. *Дис...канд..юрид. наук / 12.00.01*. Київ, 2002. С. 206.

165. Левченко О. В. Нормативно-правове регулювання інформаційної безпеки України: стан та шляхи вирішення проблем. *Збірник наукових праць Харківського університету Повітряних сил*. 2014. Випуск 3 (40). С.130–135.

166. Левченко О. Проблеми і шляхи формування системи інформаційної безпеки держави. *Збірник наукових праць Харківського університету повітряних сил*. 2014. Вип. 2 (39). С.166–168.

167. Литвин М. Кібербезпека та захист інформації в умовах інформаційної війни: український досвід. Київ, 2019. с. 245.

168. Литвиненко О. Інформація і безпека. *Нова політика*. 1998. № 1. С. 47-49.

169. Лібікі М. «Що таке інформаційна війна?» URL: http://viysko.com.ua/texnologiji-voyen/martin-libiki-shho-take-informacijna-vijna/ (дата звернення 07.11.2023).

170. Ліпкан В. А. Теорія національної безпеки. *Підручник*. Київ: КНТ, 2009. 631 с.

171. Ліпкан В. Інформаційна безпека України в умовах євроінтеграції. URL:http://mobile.pidruchniki.com/15800119/politologiya/ponyattya_zmist_zagroz_informatsiyniy_bezpetsi (дата звернення 07.12.2023).

172. Ліпкан В.А. Теоретико-методологічні засади управління у сфері національної безпеки України. *Монографія*. Київ: Текст, 2005. С. 210.

173. Ліпкан В.А., Ліпкан О.С., Яковенко О.О. Національна і міжнародна безпека у визначеннях та поняттях. Київ: Текст, 2006. С.146–147.

174. Ліпкан В.А. Безпекознавство. *Навчальний посібник*. Київ: Вид-во Європ. унту, 2003. С. 35.

175. Ліпкан ВА. Теоретичні основи та елементи національної безпеки України. *Монографія*. Київ: Текст, 2003. С.333–343.

176. Лісовський, О. Кібербезпека та інформаційна війна: виклики та загрози. *Магнолія.* Львів. 2021. С.16-23.

177. Логінов О.В. Сучасні проблеми забезпечення інформаційної безпеки в контексті формування системи державного управління. *Науковий вісник Юридичної академії Міністерства внутрішніх справ: Збірник наукових праць*. 2003. № 3. С.199–204.

178. Логовський І. Проблеми розвитку інформаційного простору України як чинника формування духовно-моральних якостей сучасного студентства. *Духовно-моральні основи та відповідальність особистості у долі людської цивілізації: зб. наук. праць*. Харків: НТУ «ХПІ», 2015. С.139–142.

179. Лях, М. Інформаційна війна як складова гібридної війни: досвід України. *Гібридна війна: сучасні виклики та загрози*. Київ, 2016. 315 с.

180. Магда Є. В. Виклики гібридної війни: інформаційний вимір. *Наукові записки Інституту законодавства Верховної Ради України*. 2014.№5. URL:http://irbisnbuv.gov.ua/cgibin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Nzizvru_2014_5_29.pdf (дата звернення 06.09.2023).

181. Макаренко Є.А. Європейське інформаційне суспільство: виклики XXI століття для країн Центральної та Східної Європи. *Вісник Київського університету. Міжнародні відносини*. 2000. № 16. С. 81-87.

182. Макаренко ЄА. Міжнародна інформаційна політика: структура, тенденції, перспективи. *Дис. д-ра. політич. наук: 23.00.04*. Київ: Національний університет ім. Т. Шевченка, 2003 С. 475.

183. Максименко Ю. Є. Інформаційне суспільство в Україні: стан та перспективи становлення. URL: http://goal-int.org/informacijne-suspilstvo-v-ukraini-stan-ta-perspektivi-stanovlennya/ (дата звернення 24.11.2023).

184. Малик І. Народження «Доктрини інформаційної безпеки України»: від теорії до практики. *Українська національна ідея: реалії та перспективи розвитку: Збірник наукових праць*. Львів: Видавництво Львівської політехніки, 2010. Вип. 22. С. 76-81.

185. Малик Я. Забезпечення інформаційної безпеки України у контексті світового досвіду. *Збірник наукових праць: «Ефективність державного управління»*. Випуск 32. 2012. С.20-27.

186. Марков В. Актуальні проблеми інформаційної безпеки України в системі міжнародної координації. *Право і Безпека: Науковий журнал*. 2013. № 1 (48). С. 78-80.

187. Марутян Р. Інформаційний складник гібридної війни проти України: сучасні виклики та загрози. URL: https://matrix-info.com (дата звернення 06.12.2023).

188. Марчук В.В. До проблеми політичної консолідації і збереження національної ідентичності українського інформаційного простору. *Аксіологічні аспекти трансформації сучасного українського суспільства*. Івано-Франківськ, 2012. С.113-115.

189. Матвієнків С., Головчинський Н. Теоретико-методологічні засади дослідження поняття «війна». *Вісник Прикарпатського університету. Сер. Політологія. Плай. Прикарпатський національний університет імені Василя Стефаника. Івано-Франківськ.* 2020. Вип. 14. С. 103-113.

190. Матвієнків С.М. Державна інформаційна політика в контексті інтеграції України в Європейський Союз. *Вісник Прикарпатського університету. Політологія*. Прикарпатський національний університет імені Василя Стефаника. Івано-Франківськ: ЛІК, Вип.12. 2018. С.227-234.

191. Матвієнків С.М. Інструментарій протидії загрозам в інформаційній сфері. *Держава і право: Збірник наукових праць. Юридичні і політичні науки*. Випуск 41. Київ: Інститут держави і права ім. В.М. Корецького НАН України, 2008. С. 646-653.

192. Матвієнків С.М. Інформаційний простір сучасної України як складова національної безпеки і суверенітету держави. *Політична наука: теорія, методологія, практика: монографія*. [за ред. Климончука В.Й.]; Прикарпатський національний університет імені В. Стефаника; Факультет історії, політології і міжнародних відносин. Івано-Франківськ: Супрун В.П., 2021. С. 207-225.

193. Матвієнків С.М. Інформаційний простір України як чинник інтеграції суспільства. *Українознавчі студії. Науково-теоретичний журнал Інституту українознавства*. Івано-Франківськ: Видавничо-дизайнерський відділ ЦІТ, 2007-2008. № 8 – 9. С. 252 – 258.

194. Матвієнків С.М. Інформаційні війни: їх суть та вплив на політичну сферу суспільства. *Науковий вісник Ужгородського університету. Серія: Політологія. Соціологія. Філософія*. Випуск 10. Ужгород: Вид-во УжНУ „Говерла", 2008. С. 113-119.

195. Матвієнків С.М. Інформаційний простір сучасної України: законодавчий аспект. *Держава і право: Збірник наукових праць. Серія Політичні науки*. Випуск 83. Київ: Вид-во «Юридична думка», 2019. С. 74-84.

196. Матвієнків С. М., Шмаленко Ю. І., Кольцов В. М. Національний інформаційний простір України: проблеми та перспективи розвитку. *Актуальні проблеми філософії та соціології*. Вип. 37. 2022. С. 223–227. *Репозитарій (відкритий електронний архів) Національного університету*

«Одеська юридична академія»: вебсайт. URL: https://goo.su/0hKQe (дата звернення: 17.08.24).

197. Махній М. Мережеве суспільство: кіберпсихологічний путівник. *Academia.edu*. Київ. 2018. С. 176.

198. Мацегора, О. Інформаційна війна в контексті гібридної війни проти України. *Вісник Черкаського державного технологічного університету. Серія: Економічні науки*. 2019. №1(3), С. 99-106.

199. Мельник О. Технологічні виклики сучасності: кіберзахист та інформаційна безпека. Київ. 2016. С. 176.

200. Меморандум про взаєморозуміння між Генеральним Директоратом з питань інформаційного суспільства Європейської Комісії і Державним комітетом зв'язку та інформатизації України щодо розвитку інформаційного суспільства від 14 вересня 2000 року. *Офіційний вебпортал: Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/main/994_447 (дата звернення: 14.10.2023).

201. Міністерство культури та інформаційної політики України. Офіційний звіт про функціонування єдиного інформаційного простору «Єдині новини» (2022–2023). *Вебсайт – URL:* https://mkip.gov.ua (дата звернення: 28.10.2024).

202. Міністерство цифрової трансформації України. *Міністерство цифрової трансформації України* : вебсайт. URL: https://goo.su/Bxb9 (дата звернення: 17.08.24).

203. Мороз О.В. Інформаційна безпека держави в умовах гібридної війни. *Національна академія державного управління при Президентові України*. 2016.

204. Московський комсомолець. URL: https://www.mk.ru/ (дата звернення: 28.10.2024).

205. Національна комісія зі стандартів державної мови. *Національна комісія зі стандартів державної мови*: вебсайт. URL: https://goo.su/zSLcE61 (дата звернення: 17.08.24).

206. Національна програма інформатизації України 1998 року. *Київ: Кабінет Міністрів України:* вебсайт. URL: https://www.kmu.gov.ua/ua/docs/1998-programa (дата звернення: 28.10.24).

207. Національна рада України з питань телебачення і радіомовлення. *Національна рада України з питань телебачення і радіомовлення*: вебсайт. URL: https://goo.su/ThwmM54 (дата звернення: 17.08.24).

208. Національний інститут стратегічних досліджень України. Оцінка рівня довіри до державних ЗМІ: аналітичний звіт за 2021–2024 роки. *Вебсайт – URL:* https://niss.gov.ua (дата звернення: 07.12.24).

209. Недбай В. В. Соціально-політичні особливості інформаційного суспільства. *Автореф. дис. к-та політ. наук.* Одеса, 2004.

210. Несвіт Г.П. Інформаційна політика держави як фактор реформування суспільства. *Одеська національна юридична академія*, *Автореф. дис. канд. політ. наук.* Одеса, 2001.

211. Нижник Н.Р., Ситник Т.П., Білоус В.Т. Національна безпека України (методологічні аспекти, стан і тенденції розвитку). *Навчальний посібник. За заг. ред. П.В. Мельника, Н.Р. Нижника.* Ірпінь, 2000. С. 304.

212. Ніщименко О. А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. *Наше право*. 2016. № 1. С. 17-23.

213. Озюменко Ю. «Сучасна російсько-українська інформаційна війна: завдання, методи та особливості». *Регіональні студії,* 2018, №28, с.123–130.

214. Олійник О. Адміністративно-правові засади інформаційної безпеки. *Європейські перспективи*. 2012. № 4 (1). С. 65–68.

215. Олійник О. Стан забезпечення інформаційної безпеки в Україні. *Юридичний вісник. Повітряне і космічне право*. 2014. № 2. С. 59–65.

216. Осмоловська А. О. Інформаційний простір України: національний та зовнішньополітичний виміри. *Матеріали наукової конференції професорсько-викладацького складу, наукових працівників і здобувачів наукового ступеня за підсумками науково-дослідної роботи за період 2019–2020 рр. (квітень-травень 2021 р.)*, 2021. С. 278–280. *Збірники наукових праць*

професорсько-викладацького складу ДонНУ імені Василя Стуса: вебсайт. URL: https://goo.su/wjUz (дата звернення: 17.08.24).

217. Отрешко В. Інформаційна безпека в контексті мовних пріоритетів українського державотворення. *Гілея: науковий вісник*. 2014. Вип. 89 (10). С. 319−323.

218. Паламарчук Д. Національна безпека : національні цінності, інтереси, цілі, завдання. *Борисфен Інтел : вебсайт. URL: https://goo.su/JfzqT8* (дата звернення: 17.07.24).

219. Панченко, О. Інформаційна безпека України в умовах гібридної війни. *Український інформаційний простір: стан, проблеми та перспективи розвитку*. Київ, 2018. 162 с.

220. Парубій А. Війна Росії проти України і світу. URL: http://ipress.ua/mainmedia/viyna_rosii_proty_ukrainy_i_svitu_78460.html (дата звернення 15.06.2023).

221. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. URL: http://justinian.com.ua/article.php?id=3222 (дата звернення 15.06.2023).

222. Пилипчук В. Г., Дзьобань О. П. Глобальні виклики і загрози національній безпеці України в інформаційній сфері. *Стратегічні пріоритети*. 2014. № 3. С. 127-132.

223. Питання діяльності Міністерства інформаційної політики України: Постанова Кабінету Міністрів України від 14 січня 2015 р. № 2 // Офіційний вебпортал: *Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/2-2015-%D0%BF#Text (дата звернення 06.12.2023).

224. План дій для України на 2015–2017 роки. *Страсбург: Рада Європи,* 2015. Вебсайт – URL: https://rm.coe.int/16802ee5e1 1. (дата звернення 28.10.2024).

225. План дій ЄС проти дезінформації (2018 р.). *Брюссель: Європейська Комісія,* 2018, с. 15. Вебсайт – URL:

https://ec.europa.eu/commission/presscorner/detail/en/IP_18_6637 (дата звернення 28.10.2024).

226. Політична енциклопедія. *редкол.: Ю. Левенець, Ю. Шаповал. К.: Парламентське видавництво.* 2011. С. 808.

227. Постанова Верховної Ради України про Рекомендації слухань з питань інформаційного розвитку суспільства в Україні від 15 квітня 2005 року. Офіційний вебпортал: *Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/main/3175-15 (дата звернення:16.10.2023).

228. Почепцов Г. Росія і Україна у співставленні їх комунікативно-пропагандистських можливостей. URL: http://osvita.mediasapiens.ua/material/33291 (дата звернення: 03.12.2023).

229. Правда. Ру. URL: https://www.pravda.ru/ (дата звернення: 28.10.2024).

230. Присяжнюк М. Інформаційна безпека України в сучасних умовах. *Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки*, 2013. Вип. 30. С. 42−46.

231. Приходько Д. П. Інформаційна війна Росії проти України: поле бою - свідомість людей. URL: http://www.hups.mil.gov.ua/assets/doc/science/stud-conf/informacijna-agresiya-rf-proti-ukraini/22.pdf (дата звернення 14.11.2023).

232. Про забезпечення функціонування української мови як державної ^ Закон України від 25 квітня 2019 року № 2704-VIII. *Верховна Рада України*: вебпортал. URL: https://goo.su/w50cM (дата звернення: 17.08.24).

233. Про засудження комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів в Україні та заборону пропаганди їхньої символіки : Закон України від 9 квітня 2015 року № 317-VIII. *Верховна Рада України*: вебпортал. URL: https://goo.su/1fLcylI (дата звернення: 17.08.24).

234. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України. Рішення РНБО від

28.04.201. Офіційний вебпортал: *Верховна Рада України.* URL: http://zakon2.rada.gov.ua/laws/show/n0004525-14 (дата звернення 21.09.2023).

235. Про інформацію: Закон України від 02.10.1992. Офіційний вебпортал: *Верховна Рада України.* URL: http://zakon3. rada.gov.ua/laws/show/2657-12 (дата звернення 21.10.2023].

236. Про концепцію національної програми інформатизації: Закон України Відомості Верховної Ради України від 1998р., № 27-28. Офіційний вебпортал: *Верховна Рада України. URL:* http://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80.

237. Про Національний координаційний центр кібербезпеки : Закон України від 7 червня 2016 року № 242/2016. *Верховна Рада України*: вебпортал. URL: https://goo.su/7btaE (дата звернення: 17.08.24).

238. Про основи національної безпеки України: Закон України від 2023р. №29. *Офіційний Вісник України.* URL: https://zakon.rada.gov.ua/laws/show/964-15 (дата звернення 02.08.2023).

239. Про основи національної безпеки україни: Закон україни від 19.06.2003 р. No 964-IV. *Офіційний вебпортал: Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/964-15#Text (дата звернення 05.09.2023).

240. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. *Верховна Рада України*: вебпортал. URL: https://goo.su/eIng3 (дата звернення: 17.08.24).

241. Про Програму інтеграції України до Європейського Союзу: Указ Президента України від 14 вересня 2000 року. *Офіційний вебпортал: Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/1072/2000 (дата звернення: 06.10.2023).

242. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану»: Указ Президента України від 19 березня 2022 року №152/2022. *Офіційний вебпортал: Верховна Рада України.* URL: https://zakon.rada.gov.ua/go/152/2022 (дата звернення: 06.10.2023).

243. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». Указ Президента України від 25.02.2017 №47/2017. *Офіційний вебпортал: Верховна Рада України.* URL: http://www.president.gov.ua/documents/472017-21374 (дата звернення: 06.10.2023).

244. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України». Указ Президента України від 26.05.2015 № 287/2015. . *Офіційний вебпортал: Верховна Рада України.* URL: http://zakon3.rada.gov.ua/laws/show/287/2015/paran7#n7 (дата звернення: 06.10.2023).

245. Про рішення Ради національної безпеки і оборони України від 24 лютого 2022 року щодо введення воєнного стану: Указ Президента України від 24.02.2022 №64/2022. *Офіційний вебпортал: Сайт Президента*. URL: https://www.president.gov.ua/documents/642022-41397 (дата звернення 28.10.2024).

246. Про розвідку: Закон України від 17 вересня 2020 року № 912-IX. *Верховна Рада України*: вебпортал. URL: https://goo.su/rNV5z (дата звернення: 17.08.24).

247. Про основні засади забезпечення кібербезпеки: Закон України від 25.03.1992. *Офіційний вебпортал: Верховна Рада України.* URL: http://zakon4.rada.gov.ua/laws/show/2229-12 (дата звернення: 16.10.2023).

248. Програма діяльності «Подолання впливу фінансово-економічної кризи та поступальний розвиток». *Київ: Кабінет Міністрів України,* 2009, с.45. Вебайт: URL: https://www.kmu.gov.ua/document/12345 (дата звернення 28.10.2024).

249. Програма «Електронна Україна». *Київ: Національний інститут стратегічних досліджень,* 2003, с.120.

250. Програми інтеграції України у ЄС. Угода про асоціацію між Україною та Європейським Союзом. *Київ: Кабінет Міністрів України,*2014, с. 312.

251. Протокол про наміри між Україною та Європейським Союзом. *Київ: Міністерство закордонних справ України,* 1994. Вебсайт: URL: https://mfa.gov.ua/ua/ (дата звернення 28.10.2024).

252. Програма «eUkraine» (Задекларування наміру динамічного розвитку). *Київ: Кабінет Міністрів України,* 2005.с. 50. Вебсайт: URL: https://www.kmu.gov.ua/ua/ (дата звернення 28.10.2024).

253. Програма «eEurope*». Брюссель: Європейська комісія,* 2002, с. 40. Вебсайт: URL: https://europa.eu/elearning/europe (дата звернення 28.10.2024).

254. Проєкт «Зміцнення свободи медіа та створення системи Суспільного мовлення в Україні». *Київ: Рада Європи,* 2018, с. 65. *URL:* https://www.coe.int/en/web/kyiv/freedom-of-media-public-broadcasting (дата звернення 28.10.2024).

255. Проноза І. І. Гібридна російсько-українська війна як загроза європейській безпеці. *Політикус*, 2016. Вип. 1. С. 126-130. URL: http://nbuv.gov.ua/UJRN/polit_2016_1_30 (дата звернення 06.08.2022).

256. Прямухіна Н. В., Бойко Ю. В. Соціальні мережі як інструмент забезпечення державної безпеки. *Матеріали наукової конференції професорсько-викладацького складу, наукових працівників і здобувачів наукового ступеня за підсумками науково-дослідної роботи за період 2019–2020 рр. (квітень-травень 2021 р.)*, 2021. С. 280–282. Вебсайт. URL: https://goo.su/SeSAIqR (дата звернення: 17.08.24).

257. Радковець Ю. Погляди на створення системи інформаційної безпеки України та її Збройних Сил. *Наука і оборона*, 2014. № 1. С. 38−42.

258. Резолюція «Стратегічні комунікації Європейського Союзу як протидія пропаганді третіх сторін». *Страсбург: Європейський Парламент,* 2016. Вебсайт – URL: https://www.europarl.europa.eu/doceo/document/TA-8-2016-0441_EN.html (дата звернення 28.10.2024).

259. Резолюція про запобігання поширенню в Інтернеті інформації незаконного змісту, шкідливої для морального здоров'я суспільства. *Страсбург: Рада Європи,* 1996, с. 32. Вебсайт- URL: https://www.coe.int/en/web/cybercrime/internet-content-regulation (дата звернення 28.10.2024).

260. Регламент (ЄС) 2023/2854 від 13 грудня 2023 року про гармонізовані правила щодо справедливого доступу до даних та їх використання (Data Act). *Офіційний вісник Європейського Союзу, L 333,* 22 грудня 2023, с. 1 55. Вебсайт – URL: https://eur-lex.europa.eu/legal-content/UK/TXT/?uri=CELEX%3A32023R2854 (дата звернення: 28.10.2024).

261. Рекомендації з протидії пропаганді: тактичні, стратегічні, довгострокові (Центр аналізу європейської політики CEPA). *Сайт: Освіта медіа.*URL:http://osvita.mediasapiens.ua/trends/1411978127/recomendatsii_z_protidii_propagandi_taktichni_strategichni_dovgostrokovi_tsentr_analizu_evropeysko i_politiki_cepa (дата звернення: 16.10.2023).

262. Ржевська Н. Сучасна інформаційна політика: досвід США для України. *Політичні дослідження / Political Studies.* 2024. № 1(7). С. 68–85. https://doi.org/10.53317/2786-4774-2024-1-4 (дата звернення: 17.08.24).

263. Рибак М.І., Атрохов А.В. До питання про інформаційні війни. *Наука і оборона*, 1998. № 2. С. 65-68.

264. Романчук Ю. В. Міжнародне співробітництво у сфері інформаційної безпеки: концептуальний та регулятивний аспекти. Київ: *НАН України Інститут світової економіки і міжнародних відносин*, 2009. Автореф. дис. канд. політ. наук, спец.: 23.00.04.

265. Російська пропаганда. Сайт: Українська правда. URL: http://forum.pravda.com.ua/index.php?topic=786907 (дата звернення: 18.10.2023).

266. Ротар Н. Діджиталізація політичної участі громадян Європейського Союзу як інструмент подолання дефіциту демократії. *Історико-політичні проблеми сучасного світу.* 2022. № 45, с.163–175.

267. Рущенко І. П. Російсько-українська гібридна війна: погляд соціолога. Харків.2015. С. 268.

268. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки. URL: http://www.journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php (дата звернення 09.01.2022).

269. Світлична В.Ю. Інформаційна безпека: сутність та порядок реалізації. *Молодий вчений*, 2014. № 11. С. 97–100.

270. Семенченко А.І. Методологія стратегічного планування у сфері державного управління забезпеченням національної безпеки України. *Вид-во НАДУ*. Київ. 2008. С. 428.

271. Семенюк Н. Роль інформаційних технологій у стратегії протидії кіберагресії: український контекст. Київ, 2021. С. 312.

272. Семченко О. А. Забезпечення інформаційної безпеки держави. *ДНУ «Книжкова палата України»,* Київ 2015. С. 672.

273. Сенченко М. Запорука національної безпеки в умовах інформаційної війни. *Вісник Книжкової палати*, 2014. № 6. С. 3–9.

274. Ситник Г. П., Олуйко В. М., Вавринчук М. П. Національна безпека України. Київ, 2007.

275. Сливка В. Інформаційна війна проти України: міф чи реальність? URL: http://intkonf.org/slivka-vv-informatsiyna-viyna-proti-ukrayini-mif-chi-realnist/ (дата звернення 05.12.2022).

276. Служба безпеки України. *Служба безпеки України*: вебсайт. URL: https://goo.su/V0XtZ01 (дата звернення: 17.08.24).

277. Сопілко І. Роль доктрини інформаційної безпеки України в реалізації державної інформаційної політики України. *Журнал східноєвропейського права*, 2014. № 2. С. 36–42.

278. Соснін О. Неодмінна складова суверенітету: інформаційна культура суспільства в контексті інформаційної безпеки України. *Політика і час*, 2002. № 7. С. 33-40.

279. Соціологічна група «Рейтинг». Громадська думка щодо інформаційної безпеки в умовах війни (2021–2024): підсумковий звіт. *Вебсайт – URL:* https://ratinggroup.ua (дата звернення 07.12.2024).

280. Степаненко В. В., Кириченко О. В., Демченко В. С. Гібридна війна: загроза національній безпеці України. *Інститут національної безпеки.* Київ: 2015. С. 24-35.

281. Стратегія інформаційної безпеки від від 28.12.2021 №685. *Офіційний вебпортал: Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/685/2021#n14 (дата звернення 11.09.2023).

282. Стратегія кібербезпеки України, затверджена Указом Президента України від 14 серпня 2021 року № 447/2021. Офіційний вебпортал: сайт Президента України. URL: https://www.president.gov.ua/documents/4472021-39681 (дата звернення 11.09.2023).

283. Суббот А. Інформаційна безпека суспільства. *Віче*, 2015. № 8. С. 29-31.

284. Сучасна гібридна війна: нові форми агресії. *Сайт: Ракурс.* URL: http://ua.racurs.ua/1063-suchasna-gibrydna-viyna-ta-yiyi-vidobrajennya-u-virtualniy-realnosti-chastyna-2 (дата звернення 17.01.2022).

285. Тарасюк А. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи. *Фенікс.* Київ. 2020. С. 400.

286. Теракти в містах влаштувала росія – МЗС. *Сайт: Факти.* URL: http://fakty.ictv.ua/ua/ukraine/polituka/20150224-1543464/ (дата звернення 05.06.2023).

287. Турчак А. В. Основні засади державної політики забезпечення інформаційної безпеки в Україні. *Інвестиції: практика та досвід*, 2019. № 11. С. 123-127.

288. У СБУ заявили, що російські канали застосовують проти телеглядачів «25-й кадр». *Сайт: ТСН.* URL:http://tsn.ua/politika/u-sbuzayavili-scho-rosiyski-kanali-zastosovuyut-protiteleglyadachiv-25-y-kadr-350517.html (дата звернення 14.11.2022).

289. Указ Президента України «Про рішення Ради Національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». *Офіційний вебпортал: Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/ show/685/2021#n7 (дата звернення 05.08.2023).

290. Указ Президента України від «Про рішення Ради національної безпеки і оборони України» від 31 жовтня 2001 року з питання «Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки». *Офіційний вебпортал: Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/1193/2001#Text (дата звернення 05.08.2023).

291. Уповноважений із захисту державної мови. *Уповноважений із захисту державної мови*: вебсайт. URL: https://goo.su/4bM1i (дата звернення: 17.08.24).

292. Фань Ч. Правове забезпечення інформаційної безпеки в системі сучасної міжнародної співпраці. *Наукові праці МАУП*, 2012. Вип. 4 (35). С. 110–115.

293. Федорук О. Концептуальні засади формування системи забезпечення національної інформаційної безпеки. *Вісник соціально-економічних досліджень*, 2013. Вип. 2 (1). С. 182–188.

294. Фомін О. Сутність поняття «інформаційна безпека». URL: defpol.org.ua/site/index.php/en/publikaci/doc_download/25 (дата звернення 05.05.2023).

295. Харченко Л.С., Ліпкан В.Л., Логінов О.В. *Інформаційна безпека України: Глосарій*. Київ , 2004. С. 136.

296. Хімей В. Основні сучасні проблеми інформаційної безпеки України. *Теле та радіожурналістика*, 2014. Вип. 13. С. 127–132.

297. Холод О. Види соціально-комунікаційних технологій. *Наукові праці Національної бібліотеки України ім. В. І. Вернадського*, 2011. Вип. 32. С. 7-20. URL: http://nbuv.gov.ua/UJRN/npnbuimviv_2011_32_1 (дата звернення 10.10.2023).

298. Хоружий Г. Війна Росії проти України. Російська пропаганда як складова «Гібридної війни». *Освіта регіону*, № 4, 2016. URL: http://social-science.com.ua/article/1392 ((дата звернення 10.10.2023).

299. Христенко В. Є. Маніпулювання свідомістю в умовах гібридної війни: психологічний аспект. *Монографія. Харків: Вид-во НУЦЗУ,* 2018. с. 44.

300. Центр протидії дезінформації. *Центр протидії дезінформації*: вебсайт. URL: https://goo.su/bPTh3 (дата звернення: 17.08.24).

301. Цимбалюк В. С., Бабінська А. В. Правове регулювання інформаційної безпеки в Україні: проблеми теорії та практики. *Адміністративне право і процес*. 2014. № 2 (8). С. 22–30. URL: http://applaw.net/index.php/journal/issue/view/18/4-8-2014-pdf (дата звернення 06.12.2023).

302. Чмельов В. О. Форми і засоби ведення інформаційної боротьби. Матеріали круглого столу «Актуальні проблеми забезпечення національної безпеки України». *Національний Університет внутрішніх справ.* Київ. 2006.

303. Чубарова Е., Шадур А. Інформаційна гібридна війна Росії проти України: особливості та наслідки. *Політологічні читання*. 2017. № 1. С.202-207.

304. Шаповалов О. Інформаційна безпека та кіберзахист України: сучасний стан та перспективи. Київ, 2018. С. 189.

305. Шевчук П. Інформаційно-психологічна війна Росії проти України: як їй протидіяти. *Демократичне врядування. Науковий вісник*. 2014. Вип. 13. С. 15–26.

306. Шиманова-Стефанишин О. Інформаційна політика в Україні у контексті українсько-російських відносин: політологічний аналіз.. *Російсько-українська війна: історія та сучасність : кол. моногр. наук. ред. Олег Полянський ; упоряд. Олег Полянський, Руслана Труба*. Львів : Растр-7, 2023. С. 123–136.

307. Шлемкевич Т. В. Інформаційне протистояння як один із головних аспектів ведення «гібридної війни». *Матеріали міжрегіональної науково-*

практичної конференції «Національна і регіональна безпека в умовах інформаційної війни». Івано-Франківськ, 2018. С. 182–187.

308. Шотурма Н. В. Інформаційні війни в інтернет-просторі. *Матеріали ІІ Міжнародної наукової конференції «Освіта і наука у мінливому світі: проблеми та перспективи розвитку» (Дніпро, 27-28 березня 2020 р.).* Дніпро, 2020. С. 91-92.

309. Шотурма Н. В. Особливості інформаційної безпеки в інтернет-просторі. *Матеріали Міжнародної наукової конференції «Безпека в сучасному світі» (Дніпро, 27-28 вересня 2019 р.).* Дніпро, 2019. С. 55-56.

310. Шульга В. І. Сучасні підходи до трактування поняття інформаційна безпека. 2015. URL: http://www.economy.nayka.com.ua/?op=1&z=5514 (дата звернення 06.06.2023).

311. Ядро російських топ-сайтів. «Про що і як пишуть кремлівські медіа?». URL: https://imi.org.ua/monitorings/yadro-rosijskyh-top-sajtiv-pro-shho-i-yak-pyshut-kremlivski-media-i39750 (дата звернення 28.10.2024).

312. Яремчук М. О. Конфлікт та Кібербезпека: Виклики та Сценарії Розвитку. *Кібербезпека в сучасному світі: актуальні виклики*. Одеса, 2022.

313. Ященко В. А. Інформаційна свідомість як фактор війни Росії проти України. 2022. С. 9-17.

314. Archive "Networks for People and their Communities: Making the Most of the Information Society in European Union". *European Commission*, Brussels, 1996. URL: http://aei.pitt.edu/8692/ (дата звернення 07.12.2023).

315. Administrative law governing the activities of law enforcement agencies under Martial Law / Y. Holodnyk et al. *Ius Humani. Revista de Derecho*. 2024. Volume 13, Issue 1. P. 50–67. https://doi.org/10.31207/ih.v13i1.344 (date of application: 17.08.24).

316. Allison R. Russian «deniable» intervention in Ukraine: how and why Russia broke the rules. *International Affairs*. 2014. Vol. 90. No. 6. P.1255−1297.

317. Applebaum A. Twilight of Democracy: The Seductive Lure of Authoritarianism. New York: Doubleday, 2020, p. 224.

318. Avery G., Cameron F. The Enlargement of the European Union. *Sheffield: Sheffield Academic Press.* 1998. P. 198. URL: https://books.google.com.ua/books?id=NU07cD6NEJQC&pg=PA158&lpg=PA158 (дата звернення 06.12.2023).

319. Balancing Interests: Criminal Proceedings & Private Life Interference Under Martial Law in Ukraine / O. Babikov et al. *German Law Journal*. 2024. P. 1–25. https://doi.org/10.1017/glj.2024.12 (date of application: 17.08.24).

320. Basic Documents UNESCO 1989-1995. *News Communication Strategy. Document C II-96/WS/2.* Paris: UNESCO, 1995. 109 p. URL: https://communication.biu.ac.il/files/communication/shared/qstl__castell_d1_3-21.1-80.pdf (дата звернення 06.06.023).

321. Basko A., Nestertsova-Sobakar O., Kaliman M. Interaction between Local Governments and the Police in Ensuring the Vital Functions of the Region and Creating a Secure Environment Under Martial Law: Legal and Economic Aspects. *Baltic Journal of Economic Studies*. 2024. Volume 10, Issue 1. P. 11–19. https://doi.org/10.30525/2256-0742/2024-10-1-11-19 (date of application: 17.08.24).

322. Batiuk O., Puzanov A. Objectives and Functions of the National Guard of Ukraine as a Subject of Ensuring State Security Under Martial Law. *Право і суспільство*. 2024. № 1, Т. 2. С. 374–380. https://doi.org/10.32842/2078-3736/2024.1.2.56 (дата звернення: 17.08.24).

323. Berezovska-Chmil, O., Kotsur, V., Kuprii, T., Semenets-Orlova, I., Drakokhrust, T., Skliar, N. Security issues on the European continent in conditions of Russia's aggression against Ukraine. https://doi.org/10.24857/rgsa.v17n6-026 (дата звернення 06.06.2023).

324. Bērziņš J. Russia's new generation warfare in Ukraine: Implications for Latvian Defense Policy. *Policy Paper*. 2014. Vol. 2. P. 2002−2014.

325. Bey H. The information war. *Virtual Futures*. 1994. P. 2.

326. Biliusov, Yevhen; Chyzhov, Denys; Osaulenko, Andriy; Perelyhina, Raisa; Derevianko, Serhii. International institution in the mechanism for the

protection of human rights and freedoms in the national security context. *Revista Cuestiones Políticas*, Volume 40, Number 73. July – December, 2022: pp. 108–127.

327. Bogdana Cherniavska, Serhii Shevchenko, Vasyl Kaletnik, Hryhorii Dzhahupov and Tetiana Madryha. Information Warfare in the World and Information Security Issues in the Context of the Russian-Ukrainian War. *Review of Economics and Finance*, 2023, 21, 916-922. DOI:https://doi.org/10.55365/1923.x2023.21.100 (дата зверненя 06.12.2023).

328. Building the European Information Society for Us All. *First Reflections of the High Level Group of Experts. Interim Report.* Brussels, 1996. URL: https://books.google.com.ua/books/about/Building_the_European_information_society.html (дата звернення 06.12.2023).

329. Brown H. Star Spangled Security: Applying Lessons Learned Over Six Decades Safeguarding America. *Washington, DC: Brookings Institution Press*, 2012, p.44.

330. Clarke, R. A., & Knake, R. K. The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats. *Penguin Press.* 2019. P. 162.

331. Cohen R. Negotiating Across Cultures: International Communication in an Interdependent World. *Washington, DC: United States Institute of Peace Press*, 1991, P.102-115.

332. Diem G. N. American Foreign Policy I: Sixteen Key Shaping American Foreign Policy. URL: http://www.amforeignpolicy.bravepages.com/AFP7.html (дата звернення 06.12.2023).

333. Dovhan O. V. Political Internet Discourse as a Source of Data for Linguistic Analysis. *Закарпатські філологічні студії*. 2023. Вип. 31. С. 162–169. https://doi.org/10.32782/tps2663-4880/2023.31.29 URL: https://goo.su/S9PTftj (дата звернення: 17.08.24).

334. Dovhan O. V. Political Internet discourse: Features of text analysis in the context of machine learning. *Науковий вісник Міжнародного гуманітарного університету. Сер. Філологія.* 2023 № 63. С. 40–47.

https://doi.org/10.32782/2409-1154.2023.63.9 URL: https://goo.su/6UhJIJv (дата звернення: 17.08.24).

335. Dr. Andrew Rathmell. Information Warfare: Implications for Arms Control. *Bulletin of Arms Control*, N 29 April 1998.

336. Ensuring National Security under Martial Law Conditions: Legal Regulation, Threats, Cooperation and Directions for Improvement / A. Nosach et al. *Khazanah Hukum*. 2024. Volume 6, Issue 1. P. 46–62. https://doi.org/10.15575/kh.v6i1.33936 (date of application: 17.08.24).

337. Europe and Global Information Society. *Recommendations of the High-Level Group on the Information Society to the Corfu European Council (Bangemann Group). European Commission.* 1994. URL: http://aei.pitt.edu/1199/1/info_society_bangeman_report.pdf (дата звернення 06.12.2023).

338. Friedman, A., & Singer, P. W. Cybersecurity and Cyberwar: What Everyone Needs to Know. *Oxford University Press*, 2014. pp. 43-46.

339. Gaddy J. Russia's Virtual Economy. *Washington, DC: Brookings Institution Press*, 2002, pp.60-64.

340. Fukuyama F. The End of History and the Last Man. *New York: Free Press,* 1992, pp. 202-205.

341. Giles, K. *Russia's* "Hybrid Warfare": How the Kremlin is Reinventing War in the 21st Century. *The Atlantic Council,* 2015. 180 p.

342. Green Paper. Living and Working in the Information Society: People First. *European Commission, Brussels,* 1996. URL: https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:1996:0389:FIN:EN:PDF (дата звернення 07.12.2023).

343. Haponenko V. Institutional Counteraction to Informational Warfare in Ukraine. *Political Technologies of Information War: Domestic and World Aspects*: monograph. Head of the author's team S. Bulbeniuk. Kyiv: KNEU, 2024. P. 128–141. *ResearchGate*: website. URL: https://goo.su/L9eH92 (date of application: 17.08.24).

344. Heras M. Russian Information Warfare: A Reality that Must be Faced, 2017.

345. Herpen, M. van. Putin's Propaganda Machine: Soft Power and Russian Foreign Policy. *Rowman & Littlefield,* 2015. 204 p.

346. Hoffman, F.G. Hybrid Warfare and Challenges. *Joint Force Quarterly, 2011.*

347. Huntington S.P. The Clash of Civilizations and the Remaking of World Order. *New York: Simon & Schuster,* 1996. P. 368.

348. Hybrid Warfare. Ryan C. Maness. Cyber Strategy: The Evolving Character of Power and Coercion, 2019.

349. Hybrid Warfare. URL: http://www.gao.gov/assets/100/97053.pdf (дата звернення 07.12.2023).

350. Information Warfare and International Security. *NATO Science and Technology Committee, Draft General Report.* 06 October 1999.

351. Jakub Kalenský. Ukraine's Struggle with Information Warfare: A Triumph of Resolve, 2018.

352. Johnson J. Morality and Contemporary Warfare. *New Haven: Yale University Press,* 1999, P.14.

353. Jonsson O., Seely R. Russian full-spectrum conflict: An appraisal after Ukraine. *The Journal of Slavic Military Studies,* 2015. Vol. 28. No. 1. P. 1–22.

354. Laswell H.D. National Security and Individual Freedom. *New York: McGraw-Hill,* 1950, P. 21-24.

355. Libicki M. What is Information Warfare? *Washington, D.C.: National Defence University Press, 1995.* URL:https://www.researchgate.net/publication/235038698_What_Is_Information_Warfare (дата звернення 07.12.2023).

356. Kant I. Perpetual Peace: A Philosophical Sketch. *Königsberg: Friedrich Nicolovius,* 1795, p. 96.

357. Kaufmann D. The Worldwide Governance Indicators Project: Answering the Critics. *World Bank Policy Research Working Paper*, No. 4149, 2007, p.16.

358. Kaplan M. The Balance of Power in International Relations: Metaphors, Myths, and Models. *Princeton: Princeton University Press*, 1968, P. 24-30.

359. Katzenstein P. J. The Culture of National Security: Norms and Identity in World Politics. *New York: Columbia University Press*, 1996, p. 54.

360. Keohane R. O. After Hegemony: Cooperation and Discord in the World Political Economy. *Princeton: Princeton University Press,* 1984, p. 117-120.

361. Kimberly Martineau. Ukraine's Cyber Resilience: A Pivotal Point in History, 2022.

362. Kremer J.-F., Müller B. Cyberspace and International Relations: Theory, Prospects and Challenges. *Springer Science & Business Media,* 2013. P. 284.

363. Lucas Kello. The Virtual Weapon and International Order, 2017.

364. Maurer T., Janz S. "The Russia-Ukraine Conflict: Cyber and Information Warfare in a Regional Context". *The International Relations and Security Network*, 2014. Vol. 17. URL: https://www.files.ethz.ch/isn/187945/ISN_184345_en.pdf (дата звернення 07.12.2023).

365. Marchuk V. Ukraine’s European Integration in the Political Dimension of Central and Eastern Europe. *Ivano-Frankivsk: Vasyl Stefanyk Precarpathian National University*, 2024, p. 250.

366. Marchuk V., Dudkevych V., Melnychuk V. European Integration of Ukraine: Political and Security Practices. *Ivano-Frankivsk: Vasyl Stefanyk Precarpathian National University*, 2024, p. 230.

367. Mearsheimer J. J. The Tragedy of Great Power Politics. New York: W. W. Norton & Company, 2001, P. 114-118.

368. Michalack M. M. The New Security Agenda. *London: Routledge*, 2002, pp. 164-182.

369. Morgenthau H. In Defense of the National Interest: A Critical Examination of American Foreign Policy. *New York: Alfred A. Knopf,* 1951, p.115.

370. National Security Act of 1947. *Discover U.S. Government Information*: website. URL: https://goo.su/zN8t6 (date of application: 17.08.24).

371. National Security Strategy. *The White House*: website. URL: https://goo.su/Ei5kXB (date of application: 17.08.24).

372. Nye J. S. Soft Power: The Means to Success in World Politics. *New York: PublicAffairs,* 2004, p. 91-93.

373. Nimmo B., Feldstein S. "The Anatomy of Russian Information Warfare: The Crimean Operation, a Case Study". 2014.

374. Organizational and legal principles of information security of enterprises in the conditions of martial law in Ukraine / B. Melnychenko et al. *Scientific Bulletin of National Mining University*. 2024. Issue 1. P. 167. https://doi.org/10.33271/nvngu/2024-1/167 *EBSCO*: website. URL: https://goo.su/cjfza (date of application: 17.08.24).

375. Peculiarities of Public Service Under the Legal Regime of Martial Law / O. Salmanova et al. *International Journal of Religion*. 2024. 5(5), P. 494–500. https://doi.org/10.61707/12kx3b52 *International Journal of Religion*: website. URL: https://goo.su/EMkph (date of application: 17.08.24).

376. Rasmussen M. "Russia's Information Warfare: A Western Perspective". 2015.

377. Rid T., Buchanan B. "Attributing Cyber Attacks". 2015.

378. Rid, T. Cybкer War Will Not Take Place. *Oxford University Press,* 2013.

379. Seddon M. "Documents Show How Russia’s Troll Army Hit America". *BuzzFeed*, 2014. URL: https://www.buzzfeednews.com/article/maxseddon/documents-show-how-russias-troll-army-hit-america (дата звернення 07.12.2023).

380. Shlapak, D.A., Johnson, M.W. Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of the Baltics. *Rand Corporation,* 2016.

381. Singer, P. W., Friedman, A. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. *Crown.* 2014. P. 124.

382. Slobodianiuk A., Vonsovych S., Bezerovska-Chmil O., Nykorovych Y., Halipchak V. "Political aspects of decision-making". *AD ALTA: Journal of Interdisciplinary Research, Web of Science.* The Czech Republic, 2023, Volume 13, Issue 2, Page 23-26.

383. Snyder T. The Road to Unfreedom: Russia, Europe, America. *New York: Tim Duggan Books,* 2018. P. 41-43.

384. Sobakar A. O., Nestertsova-Sobakar O. V. Information Security of the Activities of Law Enforcement Bodies of Ukraine Under the Conditions of the Legal Regime of the Martial State. https://doi.org/10.30525/978-9934-26-442-9-24 *Izdevniecība "Baltija Publishing"*: website. URL: https://goo.su/51EgZjd (date of application: 17.08.24).

385. State Policy in the Field of Employment: Legal Problems and Prospects in the conditions of Martial Law / D. Shvets et al. *Scientific Bulletin of National Mining University*. 2024. № 2. P. 185–193. https://doi.org/10.33271/nvngu/2024-2/185 (date of application: 17.08.24).

386. StopFake.org. Analytical reports on countering Russian propaganda and disinformation. Website – URL: https://stopfake.org (date of application: 28.10.24).

387. StopFake.org. Analytical review of information threats in social networks and the media space of Ukraine (2021–2024). Website – URL: https://stopfake.org (date of application: 28.10.24).

388. The National Security Strategy of the United States of America. Washington, 2006, 54 p.

389. Tumber H., Webster F. Journalists under fire: Information war and journalistic practices. *Sage.* 2006. P. 192.

390. Vaintraub M. Professional Competence Development of Teaching Staff in Higher Education Institutions under Martial Law. *Educational Challenges*. 2024.

Volume 29, Issue 1. P. 204–213. https://doi.org/10.34142/2709-7986.2024.29.1.14 URL: https://goo.su/680ucMV (date of application: 17.08.24).

391. Vorotin V. Y. Public Management of Risks and Threats in the Conditions of the Martial Law of the European State. *The Future of Risk Management*. 2024. Chapter 19. https://doi.org/10.5772/intechopen.1004455 *IntechOpen*: website. URL: https://goo.su/BqCIEM (date of application: 17.08.24).

392. Waltz K. N. Theory of International Politics. *Reading, MA: Addison-Wesley Publishing Company*, 1979, p. 54-66.

393. Watts, C. Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News. *Harper Collins*. 2018.

394. Wendt A. Social Theory of International Politics. *Cambridge: Cambridge University Press*, 1999, p. 429.

395. Wolfers A. "National Security" as an Ambiguous Symbol. *Political Science Quarterly*, Volume 67, Issue 4, 1952, P. 481–502.

ДОДАТКИ

Додаток А

Список публікацій здобувача за темою дисертації та відомості про апробацію результатів дисертації

Статті у наукових фахових виданнях України:

1. Галіпчак В. Інформаційна війна як складова гібридної війни в умовах російьскої агресії. *Вісник Прикарпатського університету. Політологія.* 2023. №15. С. 26-32.

URL: http://politicus.od.ua/index.php/2023-ukr?id=64

2. Галіпчак В. Інституційні чинники інформаційної політики євроінтеграції України: безпековий вимір. *Політикус.* 2023. №3. С. 97-102.

URL: http://politicus.od.ua/index.php/2023-ukr?id=64

3. Галіпчак В. Безпека інформаційного простору україни в умовах російської агресії на сучасному етапі: основні завдання та виклики. *Науковий журнал «Регіональні студії»,* 2023. №34. С. 81-85.

URL: http://regionalstudies.uzhnu.uz.ua/index.php/34

4. Галіпчак В. Трансформація інформаційного простору України під впливом російськоїагресії: зміни та виклики. *Політикус.* 2023. №4. С. 26-31.

URL: http://politicus.od.ua/index.php/2023-ukr?id=65

5. Галіпчак В. Державно-правовий механізм інформаційної безпеки України в умовах російської агресії. *Політикус.* 2023. №5. С. 19-24.

URL: http://politicus.od.ua/index.php/2023-ukr?id=66

6. Галіпчак В. Сучасні виклики та стратегії забезпечення інформаційної безпеки України в умовах російської агресії: перспективи та завдання. *Науковий журнал «Регіональні студії».* 2023. №35. С. 65-70.

URL: http://regionalstudies.uzhnu.uz.ua/index.php/35

Статті у періодичних наукових виданнях інших держав, включених до міжнародних наукометричних баз Scopus/Web of Science:

7. Slobodianiuk A., Vonsovych S., Bezerovska-Chmil O., Nykorovych Y., Halipchak V. Political aspects of decision-making . *AD ALTA: Journal of Interdisciplinary Research. Web of Science. The Czech Republic.* 2023. Volume 13. Issue 2. Page 23-26.

URL: https://www.magnanimitas.cz/ADALTA/130236/papers/A_04.pdf

Список публікацій здобувача, які додатково відображають наукові результати дисертації:

8. Галіпчак В. Здійснення інформаційної політики євроінтеграції. Безпека інформаційного суспільства ЄС. *Прикарпатський вісник НТШ. Думка.* 2021. №5. С. 21-24.

URL:https://pnu.edu.ua/wp-content/uploads/2021/04/Програма-звітної-конференції-викладачів-за-2020-рік-2.pdf

9. Галіпчак В. Державно правовий механізм забезпечення інформаційної безпеки. *Матеріали ІІІ Всеукраїнської науково-практичної конференції «Політичні процеси сучасності: глобальний та регіональний вимір» (м.Івано-Франківськ, 27-28 травня 2021р.).* Івано-Франківськ: Прикарпатський національний університет імені Василя Стефаника, 2021.

URL:https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/56376/1/Збірник%20Конференції%2027-28%20травня%202021%20%28Івано-Франківськ%29.pdf

10. Галіпчак В. Основні методологічні засади поняття національної безпеки: інформаційий вимір. *POLITIA. Вісник наукових робіт молодих вчених.* Івано-Франківськ: ЯРИНА, 2023. Вип. 5. С. 192–225.

URL:https://kpip.pnu.edu.ua/wp-content/uploads/sites/121/2023/04/politia-5.pdf

11. Галіпчак В. Державно-правовий механізм здійснення інформаційної безпеки: агенти іметоди впливу. *Матеріали Всеукраїнської науково-практичної конференції « Теоретичні та практичні аспекти політичного розвитку в Україні і світі в умовах повномасштабної російсько-української війни (пам'яті Любомири Мандзій)» (м.Львів, 10 травня 2023р.).* Львів: Львівський національний університет імені Івана Франка, 2023. С. 40-42.

URL:https://filos.lnu.edu.ua/wpcontent/uploads/2023/05/Conf_Program_May23.pdf

12. Галіпчак В. Роль інституційних механізмів у запезпеченні інформаційної безпеки: аспекти управління та взаємодії. *IX Міжнародна науково-практична конференція «Практичні та теоретичні питання розвитку науки та освіти» (м. Львів, 29-30 жовтня 2023 року).* Львів: Львівський науковий форум, 2023р. С. 35-37.

URL:http://www.lviv-forum.inf.ua/save/2023/29-30.10/Збірник.pdf

13. Галіпчак В. Вплив інформаційних технологій на захист національних інтересів в Україні: виклики та можливості. *X Міжнародна науково-практичніа конференція «Пріоритетні шляхи розвитку науки і освіти» (м. Львів, 29-30 листопада 2023 року).* Львів: Львівський науковий форум, 2023р. С. 70-73.

URL:http://www.lviv-forum.inf.ua/save/2023/29-30.11/Збірник.pdf

Додаток Б

Нормативно-правова база забезпечення інформаційної безпеки України

Назва документа	**Дата прийняття**	**Основні положення**
Закон України "Про основи національної безпеки України" [239]	19 червня 2003 року	Визначає основні принципи та пріоритети забезпечення національної безпеки України, зокрема в інформаційній сфері.
Закон України "Про інформацію"[235].	2 жовтня 1992 року (зі змінами)	Регулює відносини, пов'язані із створенням, отриманням, використанням, поширенням та захистом інформації.
Закон України "Про доступ до публічної інформації" [91].	13 січня 2011 року	Встановлює порядок доступу до інформації, яка перебуває у володінні суб'єктів владних повноважень, та забезпечує прозорість і відкритість їхньої діяльності.
Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" [97]	5 липня 1994 року	Визначає організаційно-правові основи захисту інформації в інформаційно-телекомунікаційних системах.
Указ Президента України "Про рішення Ради національної безпеки і оборони України щодо введення воєнного стану"[245]	24 лютого 2022 року	Регулює правові аспекти функціонування держави в умовах воєнного стану, зокрема в інформаційній сфері.
Стратегія кібербезпеки України [282].	14 серпня 2021 року	Визначає завдання щодо забезпечення кібербезпеки України, зокрема в умовах гібридних загроз.
Національна програма інформатизації України [206].	4 лютого 1998 року	Визначає напрями розвитку інформаційної інфраструктури та впровадження інформаційних технологій.

**Джерело: оформлено автором за даними, на які посилаються вище.*

Додаток В

Основні інституції та органи, відповідальні за інформаційну безпеку України станом на 07.12. 2024р.

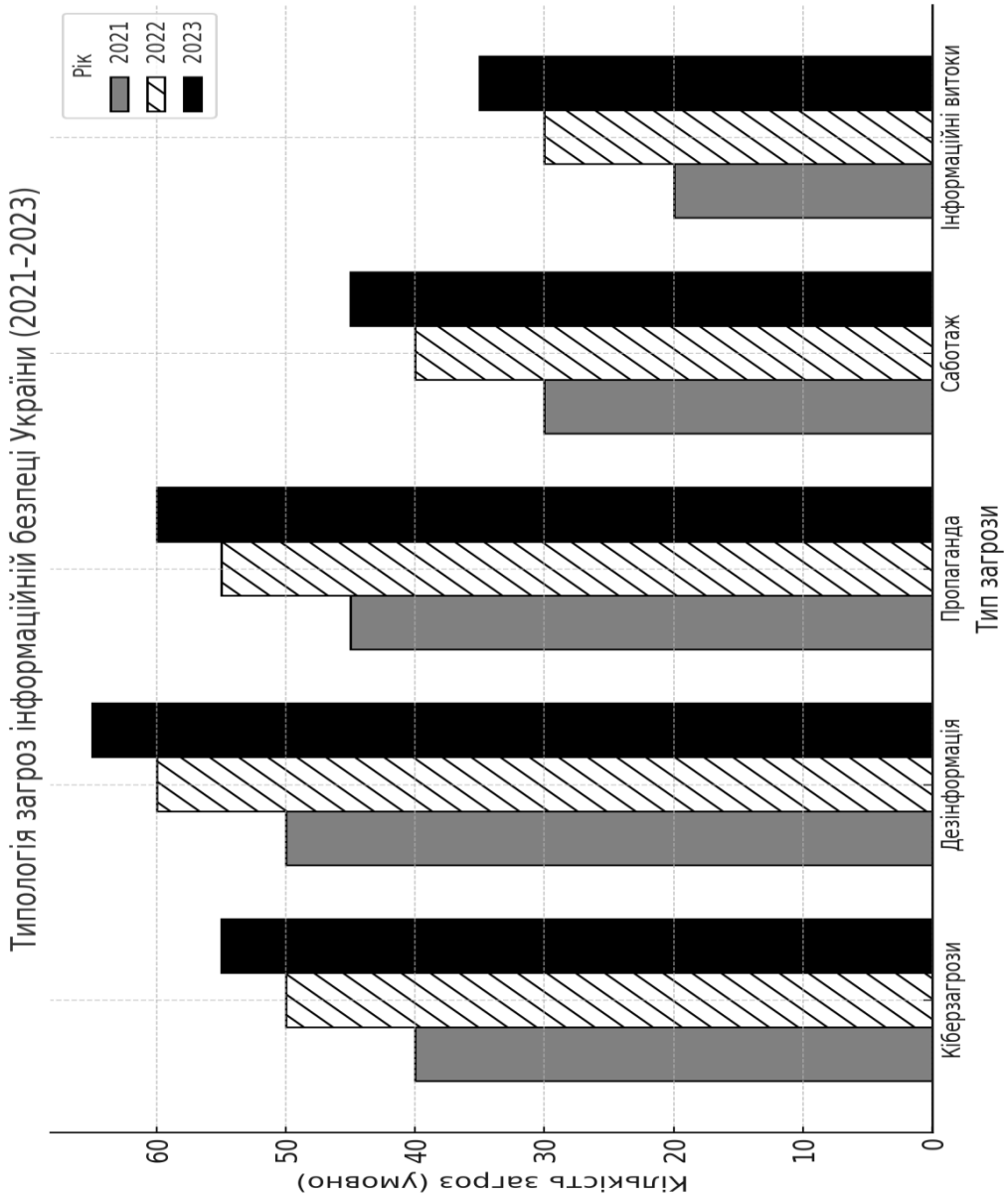
Інституція	**Функції**	**Значення**
Рада національної безпеки і оборони України (РНБО)	Визначає основні напрями державної політики у сфері національної та інформаційної безпеки. Координує діяльність органів виконавчої влади з питань національної безпеки та оборони, зокрема інформаційного захисту.	Є центральним органом прийняття стратегічних рішень у сфері інформаційної безпеки.
Служба безпеки України (СБУ)	Здійснює заходи щодо протидії інформаційним загрозам, включаючи виявлення, попередження та ліквідацію інформаційних атак та кіберзагроз.	Основний орган із забезпечення контррозвідувальних заходів в інформаційному просторі.
Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку)	Забезпечує захист інформаційних систем державних органів, створення та експлуатацію захищених телекомунікаційних мереж.	Відповідає за технічний захист інформації та підтримку кібербезпеки.
Міністерство оборони України	Організовує інформаційно-психологічний захист у військовій сфері, зокрема захист даних у збройних силах.	Забезпечує інформаційну складову національної оборони.
Міністерство цифрової трансформації України	Розробляє цифрові стратегії, координує впровадження електронного урядування, відповідає за формування національного цифрового середовища.	Головний координатор цифрових реформ, спрямованих на зміцнення інформаційної безпеки.
Національний центр кібербезпеки	Аналізує загрози кібербезпеці, координує дії органів виконавчої влади у сфері протидії кіберзагрозам.	Центральний орган із моніторингу та протидії кіберзагрозам.

**Джерело: оформлено автором за даними [13].*

Додаток Г

Типологія загроз інформаційній безпеці України

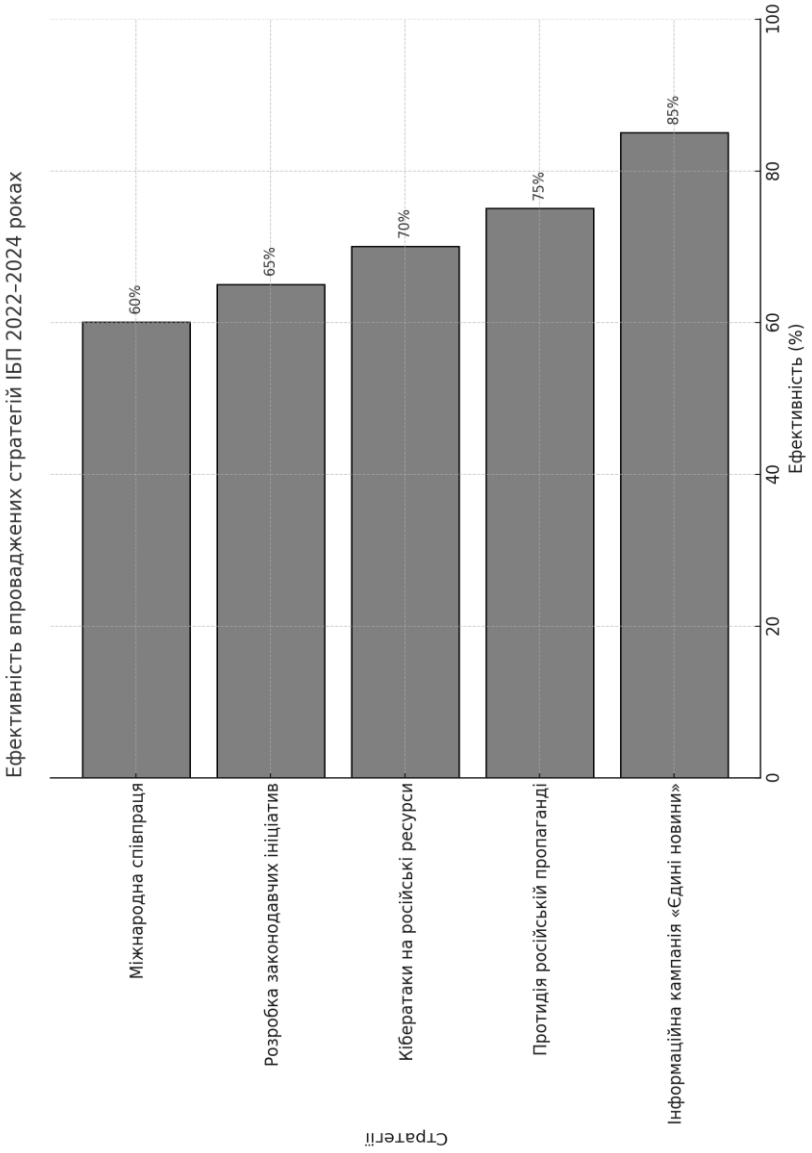
Нижче подано графічне відображення типології загроз інформаційній безпеці України за період 2021–2023 рр.



**Джерело: створено автором за допомогою онлайн сервісу Datawrapper.de згідно з даними [114;77; 115; 116].*

Додаток Д

Нижче подано приклади та графічне відображення ефективності впроваджених стратегій ІБП за період 2022–2024 рр.

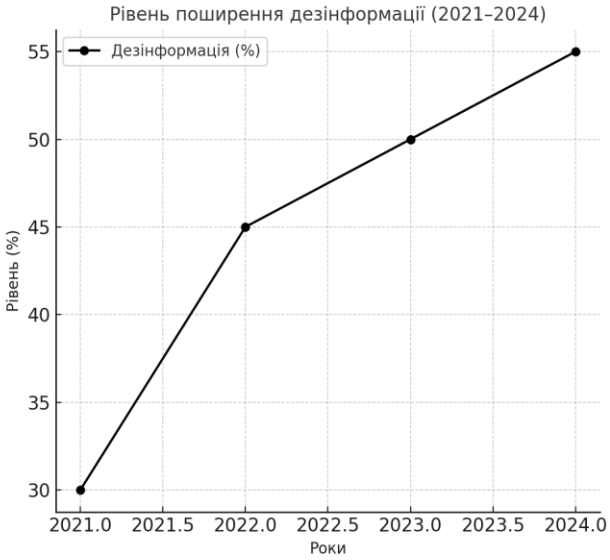


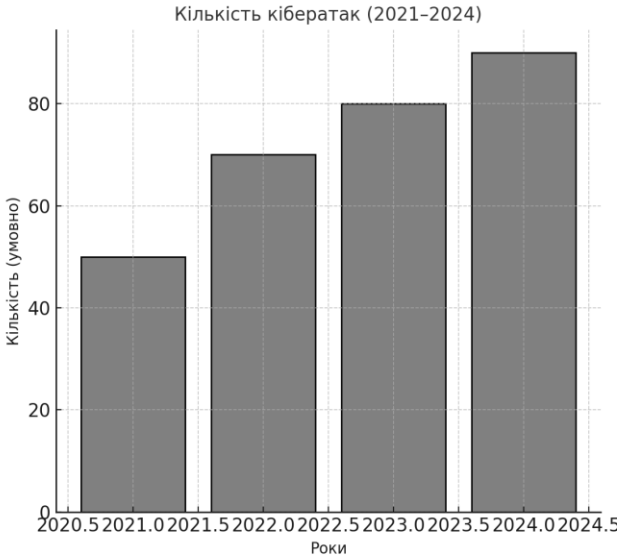
Ефективність кожної стратегії оцінювалася на основі аналітичних звітів та експертних оцінок за період 2022–2024 років. Показник ефективності наведено у відсотках.

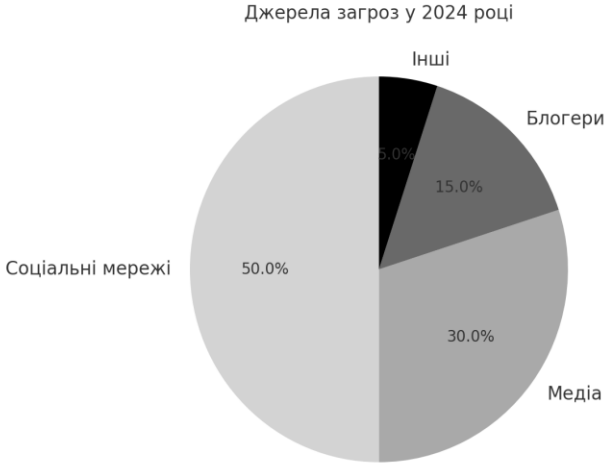
**Джерело: створено автором за допомогою онлайн сервісу Datawrapper.de згідно з даними [63;201; 386].*

Додаток Е

Статистичні дані щодо стану інформаційного простору України за період 2021–2024 рр., включаючи поширення дезінформації, кількість кібератак та джерела загроз



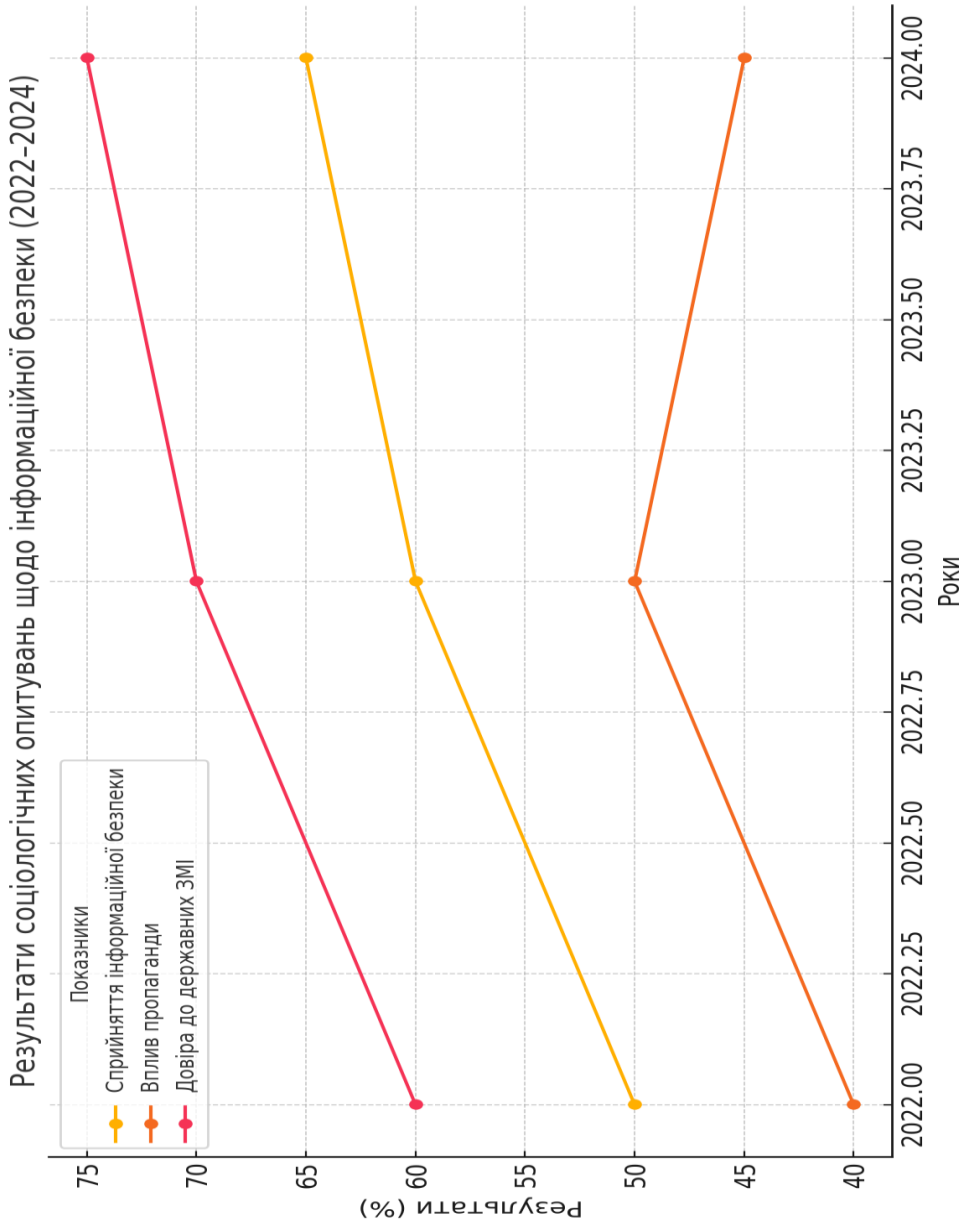




**Джерело: створено автором за допомогою онлайн сервісу Datawrapper.de згідно з даними [63;127; 387].*

Додаток Є

Результати соціологічних досліджень громадської думки щодо сприйняття інформаційної безпеки, впливу пропаганди та рівня довіри до державних ЗМІ в умовах війни за період 2022–2024 рр.



**Джерело: створено автором за допомогою онлайн сервісу Datawrapper.de згідно з даними [208; 126; 279; 62;63].*