

**МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ
ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ**

*Кваліфікаційна наукова
праця на правах рукопису*

ГОНЧАРОВ МИКОЛА ВІКТОРОВИЧ

УДК 340.12(477):004.738.-049.5

**ДИСЕРТАЦІЯ
ТЕОРЕТИКО-ПРАВОВІ ОСНОВИ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ
БЕЗПЕКИ В УКРАЇНІ**

Галузь знань 08 – Право

Спеціальність 081 – Право

Подається на здобуття наукового ступеня доктора філософії

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

_____ М. В. Гончаров

Науковий керівник:

доктор юридичних наук, професор,

Заслужений юрист України

Шевченко Анатолій Євгенійович

Ірпінь – 2023

АНОТАЦІЯ

Гончаров М. В. Теоретико-правові основи регулювання інформаційної безпеки в Україні. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 081 – Право. Державний податковий університет, Міністерство фінансів України. – Ірпінь, 2023.

Дисертація присвячена дослідженню теоретико-правових проблем регулювання сфери інформаційної безпеки в Україні, враховано особливості провадження правозабезпечувальних заходів у цій сфері з урахуванням додаткових зовнішніх загроз, пов'язаних з повномасштабним російським вторгненням 24 лютого 2022 року, проаналізовано стан правового забезпечення інформаційної сфери в окремих європейських країнах та Великобританії, визначено джерела загроз на напрямках доступу, володіння, розпоряджання масивами баз даних та іншими відомостями, віднесеними до різних рівнів правового і технологічного захисту.

Здійснений авторський теоретико-правовий аналіз чинної нормативної бази у сфері захисту інформації у межах цього дослідження засвідчив про тісне поєднання внутрішніх механізмів стабілізації встановленого порядку роботи з відомостями різних рівнів захисту та загальним підходом до забезпечення національної безпеки. Саме ця обставина є однією з основних при визначенні ролі і значення забезпечення належного рівня захисту сфери інформаційної безпеки як своєрідної кровоносної системи, завдяки якій відбувається взаємодія і координація дій між усіма складовими національної безпеки.

Сучасний стан суспільних відносин, насамперед між громадянином і державою, формується в умовах стрімкого розвитку цифрових технологій, коли практично всі сфери життя переведені в електронний формат спілкування. Без більшості діджиталізованих послуг майже неможливо уявити собі ситуації, які вимагають швидкого і точного вирішення. На цих рівнях особливої актуальності

набуває завдання належного захисту інформаційної сфери, оскільки механізми віддаленого доступу до баз даних, насамперед персональних і фінансових, перебувають під перманентною загрозою бути зламаними, а такими протиправними діями може бути завдано значних матеріальних збитків і моральної шкоди.

Дослідження теоретико-наукової і нормативної бази галузі захисту інформаційної сфери показало, що між цими складовими маєтся суттєвий розрив, який негативно впливає на загальний стан функціонування інформаційної складової у загальному механізмі національної безпеки. У зв'язку з цим виникла необхідність здійснити глибокий аналіз джерельної бази, опрацювати наукові і практичні підходи до розуміння як самого поняття «інформаційна безпека», так і інших, похідних понять (наприклад, загрози інформаційній безпеці, джерела загроз інформаційній безпеці тощо).

З опрацьованого матеріалу зроблено низку висновків, які ґрунтуються на результатах застосування методологічних інструментів наукового пошуку, і засвідчують постійний діалектичний зв'язок між матеріальною і духовною частинами загального поняття «інформаційна безпека». У цьому зв'язку опираємось на розлогий науковий доробок і багату нормативну базу, завдяки яким є можливість висловити авторське бачення проблематики забезпечення належного стану збереження інформації, а також продемонструвати критичне ставлення до оприлюднених відомостей з цього питання.

Посилання до історіографічних джерел сприяло розкриттю нових аспектів серед представлених наукових підходів до розуміння поняття «інформаційна безпека». Своєю чергою, коректне тлумачення семантичного значення системоутворюючих категорій при формуванні конкретного поняття (наприклад, джерела загроз інформаційній безпеці) є запорукою виведення логічного і правильного умовиводу, що є свідченням зрілості науковця і його здатності здійснювати теоретико-правові узагальнення у певній галузі юридичної науки.

Особливе місце відведено підбору методологічного інструментарію дослідження. Такий підбір здійснено на основі ексклюзивного значення сфери інформаційного забезпечення у взаємодії з іншими напрямками державного будівництва і національної безпеки. При цьому відзначаємо, що піднята проблематика має міждисциплінарний характер через закладену у ній правову і структурну природу: правова, економічна (технологічна) і морально-психологічна складові. За таких умов надзвичайного важливого значення надається філософсько-діалектичному методу з огляду на його гносеологічну природу, що сприятиме виведенню авторських висновків і суджень, які відзначатимуться послідовністю та поступальністю.

Застосування загально наукових методів дослідження забезпечить реалізацію завдань щодо найбільш повного і осяжного узагальнення наукового доробку і нормативної бази у сфері інформаційної безпеки, виведенню нових постійно діючих зв'язків між окремими елементами цілісного поняття «інформаційна безпека», а також пропозицій щодо підвищення ефективності профілактико-превентивних заходів на напрямках захисту інформаційного середовища України.

Комплексне застосування спеціально-наукових методів дослідження виведе нас на специфічні межі вузько-спеціалізованого підходу до розуміння загроз інформаційній безпеці крізь призму порівняльних, будівничих (моделювання) та інших маніпуляцій з формально визначеними складовими техніко-нормативного підґрунтя сфери інформаційної безпеки. Поряд з порівняльно-правовим будуть задіяні й інші інструменти наукової розвідки, а саме методи державно-правового моделювання, герменевтичний, спеціально-юридичний та ін.

Вирішуючи завдання дисертаційного дослідження, ми торкалися основ формування і розвитку державної політики у сфері інформаційної безпеки, а також здійснили поточний аналіз стану взаємодії наукової і практичної складових при виявленні і нейтралізації загроз базам даних та іншій інформації,

яка охороняється законом, і передбачає дотримання установленого порядку її використання.

Широке коло наукової інформації, що стосується досліджуваної проблематики, створило емпіричну базу, завдяки якій отримано авторські узагальнення і висновки стосовно чинних загроз інформаційній безпеці держави, а також скореговано процес дослідження у зв'язку з новими загрозами, що стали наслідком повномасштабної агресії росії проти України.

Напрацьовані матеріали виконали роль практичної основи наукової розвідки в частині розуміння пізнавального значення специфічної сфери професійної діяльності на напрямках захисту інформації в контексті виконання заходів з дотримання національної безпеки держави. Аксіологічні аспекти розкрито крізь призму розуміння механізмів взаємодії окремих складових у цілісному правовому механізмі, яким є національна безпека, представлених у поглядах знаних науковців і практиків з означеної сфери. Зроблено акцент на ролі і значенні застосування державних важелів впливу на провадження діяльності щодо формування у населення належного рівня медіакультури, усвідомленого і критичного ставлення до наявного інформаційного контенту, насамперед в умовах російської агресії проти України.

Окремий підрозділ присвячено правовій характеристиці нормативної бази у сфері інформаційної безпеки. Здійснено детальний аналіз чинного у цій сфері законодавства (законів і підзаконних нормативно-правових актів), опрацьовано понятійно-категоріальний апарат, досліджено семантико-етимологічну природу системоутворюючих понять, які виступають підґрунтям для формування логіко-структурних зв'язків між правовими явищами сфери інформаційної безпеки. Отримані в результаті таких дій відомості систематизовано у висновках і пропозиціях, які є свідченням новизни і практичної цінності виконаної роботи.

Особливого значення для дослідження ситуації, пов'язаної з розумінням ролі і значення інформаційної безпеки для реалізації завдань національної безпеки, набуває виокремлення джерел загроз інформаційній безпеці, їх

класифікація і пропозиції щодо своєчасного викриття і знешкодження деструктивних і ворожих кібератак, які здійснюються як з територій інших держав, так і мають внутрішнє медіапідґрунтя. Здійснено градацію джерел загроз інформаційної сфери з різних підходів, а саме з позицій фізичного походження контенту, соціально-особового напрямку (громадяни, особи, управлені на володіння і розпоряджання певним обсягом даних, технологічний аспект з урахуванням стану матеріально-технічного забезпечення засобів збереження інформації). При цьому особливу увагу приділено дослідженню і аналізу джерел загроз інформаційному середовищу з тих причин, що канали передавання відомостей на всіх рівнях становлять стійку і належним чином охоронювану сферу, що виступає кровоносною системою цілісного правового явища, яким є національна безпека України.

Проаналізований науковий доробок і нормативно-правова база з регулювання відносин у сфері використання, обміну, розпоряджання і збереження інформації спонукали до здійснення порівняльно-правового аналізу нормативно-правового забезпечення сфери інформаційного забезпечення країн Європейського Союзу та Великобританії. Вивчення показало, що вітчизняна сфера захисту інформації досить потужно протидіє протиправним зазіханням різної природи і походження, відзначається позитивний ефект від імплементації дієвих механізмів захисту інформації в українському медіапросторі. Відзначається необхідність створення спільних з європейськими країнами і Великобританією спільних координаційних центрів з вивчення медіаконтенту та визначення рівня деструктивності для функціонування демократичних принципів, на яких будується правова система зазначених країн, і відбувається реформування сфери інформації в Україні як державі-кандидату на вступ до європейської спільноти.

Як одне з чільних завдань дисертаційного дослідження виокремлено напрямок удосконалення інформаційної безпеки України. На основі чинних нормативно-правових актів різної юридичної сили здійснено теоретико-правове

вивчення особливостей правового регулювання інформаційної сфери у тих сегментах, які потребують підвищеної уваги і концентрації значних зусиль для збереження масивів інформації та інших відомостей, насамперед з обмеженим доступом. Здійснено посилення до конкретних напрямків посилення правового регулювання відносин інформаційної сфери, запропоновано застосування превентивно-профілактичного інструментарію для оздоровлення і суттєвого покращання ситуації на напрямках запровадження ефективного контролю за отриманням, зберіганням, використанням та володіння різними типами інформації.

Ключові слова : інформаційна безпека України, забезпечення інформаційної безпеки; національна безпека; державне управління; державна інформаційна політика; захист інформаційного простору; Україна; інформаційна агресія; інформаційні права людини; інформаційне право; інформаційне суспільство; штучний інтелект; права і свободи людини і громадянина; захист інформації; локалізація даних.

SUMMARY

Goncharov M. V. Theoretical and legal foundations of information security regulation in Ukraine. - Qualification scientific work in the form of a manuscript.

Dissertation for the degree of Doctor of Philosophy in the specialty 081 - Law. State Tax University, Ministry of Finance of Ukraine - Irpin, 2023.

The dissertation is devoted to the study of theoretical and legal problems of regulating the information security sphere in Ukraine, taking into account the peculiarities of law enforcement measures in this area, taking into account additional external threats associated with the full-scale Russian invasion on February 24, 2022, the author analyzes the state of legal support of the information sphere in certain European countries and the United Kingdom, identifies sources of threats in the areas

of access, possession, and disposal of database arrays and other information classified as different levels of legal and technological protection.

The author's theoretical and legal analysis of the current regulatory framework in the field of information protection within the framework of this study demonstrates a close combination of internal mechanisms for stabilizing the established procedure for working with information of different levels of protection and a general approach to ensuring national security. This circumstance is one of the main ones in determining the role and importance of ensuring an adequate level of protection of the information security sphere as a kind of circulatory system, thanks to which all components of national security interact and coordinate their actions.

The current state of social relations, primarily between citizens and the state, is shaped by the rapid development of digital technologies, when virtually all areas of life are transformed into electronic communication. Without most digitalized services, it is almost impossible to imagine situations that require a quick and accurate solution. At these levels, the task of proper protection of the information sphere becomes particularly relevant, since mechanisms for remote access to databases, primarily personal and financial, are under a permanent threat of being hacked, and such unlawful actions can cause significant material and moral damage.

The study of the theoretical, scientific and regulatory framework of the information sphere protection has shown that there is a significant gap between these components, which negatively affects the overall functioning of the information component in the overall national security mechanism. In this regard, it became necessary to carry out an in-depth analysis of the source base, to develop scientific and practical approaches to understanding both the concept of "information security" and other derivative concepts (e.g., threats to information security, sources of threats to information security, etc.).

From the material analyzed, a number of conclusions have been drawn which are based on the results of applying methodological tools of scientific research and which testify to the constant dialectical relationship between the material and spiritual

parts of the general concept of "information security". In this regard, we rely on an extensive scientific heritage and a rich regulatory framework, which make it possible to express the author's vision of the issues of ensuring the proper state of information security, as well as to demonstrate a critical attitude to the published information on this issue.

The reference to historiographic sources contributed to the disclosure of new aspects among the presented scientific approaches to understanding the concept of "information security". In turn, the correct interpretation of the semantic meaning of the system-forming categories in the formation of a specific concept (e.g., the source of threats to information security) is the key to drawing a logical and correct conclusion, which is evidence of the maturity of a scholar and his/her ability to make theoretical and legal generalizations in a particular area of legal science.

A special place is given to the selection of methodological tools for the study. This selection was made on the basis of the exclusive importance of the sphere of information support in interaction with other areas of state building and national security. At the same time, we note that the raised issues are interdisciplinary in nature due to their legal and structural nature: legal, economic (technological) and moral and psychological components. Under such circumstances, the philosophical-dialectical method is of utmost importance given its epistemological nature, which will facilitate the author's conclusions and judgments that will be characterized by consistency and progressiveness.

The use of general scientific research methods will ensure the realization of the tasks of the most complete and comprehensive generalization of scientific achievements and the regulatory framework in the field of information security, the derivation of new permanent links between individual elements of the integral concept of "information security", as well as proposals to improve the effectiveness of preventive and preventive measures in the areas of protection of the information environment of Ukraine.

The comprehensive application of special scientific research methods will lead us to the specific limits of a highly specialized approach to understanding threats to information security through the prism of comparative, construction (modeling) and other manipulations with formally defined components of the technical and regulatory framework of the information security sphere. Along with the comparative legal one, other instruments of scientific research will be used, namely methods of state and legal modeling, hermeneutic, special legal, etc.

In solving the tasks of the dissertation research, we touched upon the basics of the formation and development of state policy in the field of information security, and also carried out a current analysis of the state of interaction between scientific and practical components in identifying and neutralizing threats to databases and other information protected by law and involving compliance with the established procedure for its use.

A wide range of scientific information related to the studied issues has created an empirical basis, which has led to the author's generalizations and conclusions regarding the current threats to the information security of the state, as well as to the adjustment of the research process in connection with new threats resulting from Russia's full-scale aggression against Ukraine.

The materials developed have served as a practical basis for scientific research in terms of understanding the cognitive value of a specific area of professional activity in the field of information protection in the context of implementing measures to ensure the national security of the State. The axiological aspects are disclosed through the prism of understanding the mechanisms of interaction of individual components in the integral legal mechanism, which is national security, presented in the views of well-known scholars and practitioners in this area. The author emphasizes the role and importance of using state levers of influence on the implementation of activities aimed at forming an appropriate level of media culture among the population, a conscious and critical attitude to the available information content, especially in the context of Russian aggression against Ukraine.

A separate subsection is devoted to the legal characterization of the regulatory framework in the field of information security. A detailed analysis of the legislation in force in this area (laws and by-laws) is carried out, the conceptual and categorical apparatus is elaborated, and the semantic and etymological nature of the system-forming concepts which serve as the basis for the formation of logical and structural links between legal phenomena in the field of information security is investigated. The information obtained as a result of such actions is systematized in conclusions and proposals, which are evidence of the novelty and practical value of the work performed.

Of particular importance for the study of the situation related to understanding the role and importance of information security for the implementation of national security tasks is the identification of sources of threats to information security, their classification and proposals for timely detection and neutralization of destructive and hostile cyberattacks carried out both from the territories of other states and having a domestic media background. The author grades the sources of threats to the information sphere from different approaches, namely, from the standpoint of the physical origin of content, social and personal direction (citizens, persons authorized to own and dispose of a certain amount of data, technological aspect, taking into account the state of material and technical support of information storage facilities). Particular attention is paid to the study and analysis of the sources of threats to the information environment, since the channels of information transmission at all levels constitute a stable and properly protected sphere that acts as the circulatory system of the integral legal phenomenon, which is the national security of Ukraine.

The analyzed scientific heritage and the legal framework for regulating relations in the field of use, exchange, disposal and storage of information prompted a comparative legal analysis of the legal framework for information security in the EU and the UK. The study showed that the domestic information protection sphere is quite powerful in counteracting unlawful encroachments of various nature and origin, and a positive effect of the implementation of effective information protection mechanisms

in the Ukrainian media space is noted. The author notes the need to establish joint coordination centers with European countries and the United Kingdom to study media content and determine the level of destructiveness to the functioning of the democratic principles on which the legal system of these countries is based, and to reform the information sphere in Ukraine as a candidate state for accession to the European community.

One of the main objectives of the dissertation research is to improve the information security of Ukraine. On the basis of existing legal acts of different legal force, the author made a theoretical and legal study of the peculiarities of legal regulation of the information sphere in those segments which require increased attention and concentration of significant efforts to preserve arrays of information and other data, primarily with limited access. The author makes reference to specific areas of strengthening the legal regulation of relations in the information sphere, and suggests the use of preventive and preventive tools to improve the situation and significantly improve the situation in the areas of introducing effective control over the receipt, storage, use and possession of various types of information.

Keywords: information security of Ukraine, information security; national security; public administration; state information policy; protection of information space; Ukraine; information aggression; information rights; information law; information society; artificial intelligence; human and civil rights and freedoms; information protection; data localization.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

1. Гончаров М. В. Сутність інформаційної безпеки в умовах розвитку сучасного суспільства. *Міжнародний науковий журнал «Інтернаука»*. Серія: «Юридичні науки». 2022. № 4. С. 77–82. URL: <https://www.inter-nauka.com/issues/law2022/4/8004>

2. Гончаров М. В. Тенденції наукових поглядів у сфері нормативно-правового забезпечення інформаційної безпеки України. *Науковий вісник Ужгородського національного університету*. Серія: «Право». 2022. № 70. С. 24–28. URL: <http://visnyk-pravo.uzhnu.edu.ua/article/view/257287/254189>

3. Гончаров М. В. Досвід нормативно-правового забезпечення інформаційної безпеки в країнах Європейського Союзу. *Наше право*. № 2. 2023. С. 144–150. URL: http://nashe-pravo.unesco-socio.in.ua/wp-content/uploads/archive/NP-2023-2/NP_2023_2_144.pdf

4. Andrii M. Blahodarnyi, Olha O. Barabash, Andrii V. Honcharov, Mykola V. Honcharov, Volodymyr A. Shatilo. Local Self-government in European Countries: General Characteristics, Comparison and Ukrainian Realities. *LEX LOCALIS - journal of local self-government* Vol. 21, No. 3, pp. 683-706, July 2023. URL: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85165207079&origin=resultslist&sort=plf-f> (Scopus).

які засвідчують апробацію результатів дисертації:

5. Гончаров М. В. До питання використання інформаційних систем та технологій у сучасному суспільстві. *Кібербезпека в Україні: правові та організаційні питання : матеріали всеукр. наук.-практ. конф., м. Одеса, 30 листопада 2018 р.* Одеса : ОДУВС, 2018. С. 94–95.

6. Гончаров М. В. Сутність інформаційної безпеки в умовах розвитку сучасного суспільства. *Кібербезпека в Україні: правові та організаційні*

питання: матеріали міжн. наук. практ. конф., м. Одеса, 22 листопада 2019 р. Одеса : ОДУВС, 2019. С. 4–5.

7. Гончаров М. В. Деякі аспекти дослідження інформаційної безпеки в діяльності держави. *Правова наука і державотворення в Україні у світлі сучасних глобалізаційних викликів: історія, теорія, практика (до 25-ї річниці Конституції України): матеріали Всеукраїнської науково-практичної конференції (м. Маріуполь – м. Кривий Ріг, 11 червня 2021 року)*. Маріуполь : ДонДУВС, 2021. С. 133–135.

8. Гончаров М. В. Деякі аспекти дослідження сутності інформаційної безпеки. *Інформація та документ у сучасному науковому дискурсі: матеріали VII Всеукраїнської дистанційної науково-практичної конференції. (Івано-Франківськ, 20 травня 2022 р.)*. Івано-Франківськ: ІФНТУНГ, 2022. С. 13–16.

9. Гончаров М. В. Концептуальні засади сутності інформаційної безпеки України. *Міжнародне право XXI століття: сучасність та майбутнє: Збірник тез доповідей Міжнародної науково-практичної конференції «Міжнародне право XXI століття: сучасність та майбутнє»*. (м. Ірпінь, 25 травня 2022 р.). Ірпінь: Державний податковий університет, 2022. С. 51–56.

10. Honcharov A.V., Honcharov M.V. Some aspects the conceptual study of regulatory and legal ensurement of information security. *The IX International Scientific and Practical Conference «Analysis of the problems of science and modern education»*, 06 – 08 March, 2023. Prague, Czech Republic. P. 77–80.

які додатково відображають результати дисертації:

11. Гончаров А. В., Гончаров М. В. Життєвий шлях, юридичні погляди та педагогічна діяльність В. Г. Кукольника (1765–1821). *Правовий часопис Донбасу*: Зб. наук. праць № 1(66). Кривий Ріг.: Донецький юридичний інститут МВС України, 2019. С. 13–18. URL: <https://ljd.dnuvs.in.ua/wp-content/uploads/2022/01/2-goncharov-goncharov.pdf>

ЗМІСТ

ВСТУП	3
РОЗДІЛ 1. ІСТОРИКО - МЕТОДОЛОГІЧНІ ОСНОВИ ДОСЛІДЖЕННЯ ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	16
1.1. Загальнотеоретичні основи дослідження поняття «інформаційна безпека».....	16
1.2. Методологія дослідження основ інформаційної безпеки	26
Висновки до розділу 1	41
РОЗДІЛ 2. ТЕОРЕТИКО-ПРАВОВЕ ОСМИСЛЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	44
2.1. Наукові погляди щодо поняття інформаційної безпеки та її закріплення в нормативно-правових актах	44
2.2. Аксіологічні аспекти та роль держави у забезпеченні інформаційної безпеки	65
2.3. Правова характеристика нормативної бази у сфері інформаційної безпеки	82
Висновки до розділу 2	99
РОЗДІЛ 3. АНАЛІЗ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ТА МІЖНАРОДНИЙ ДОСВІД З ПРОТИДІЇ ПОРУШЕННЯМ ВСТАНОВЛЕНОГО ПОРЯДКУ ПОВОДЖЕННЯ З ІНФОРМАЦІЄЮ	103
3.1. Джерела загроз інформаційній безпеці та їх класифікація	103
3.2. Досвід інформаційної безпеки в країнах Європи	117
3.3. Шляхи вдосконалення інформаційної безпеки в Україні	138
Висновки до розділу 3	161
ВИСНОВКИ	164
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	172
ДОДАТКИ	196

ВСТУП

Обґрунтування вибору теми дослідження. Актуальність теми дослідження визначається важливим значенням інформаційної сфери для задоволення не тільки потреб суспільства у передаванні і зберіганні відомостей, а й для виконання однієї з найважливіших функцій держави – забезпечення національної безпеки України. При цьому інформаційна галузь виконує двоєдине завдання: по-перше, задоволення потреб внутрішнього споживача і комунікація (у глобальному значенні цього поняття), по-друге, для захисту внутрішнього психологічного середовища від деструктивного впливу зовнішніх джерел загроз, насамперед з боку ворожої росії, а також убезпечення систем зберігання баз даних на всіх рівнях від протиправних посягань від усіх нелегітимних чинників.

На порядок денний виступає необхідність запровадження профілактико-превентивних заходів у контексті рішень Верховної Ради України і Європейського Парламенту, якими російську федерацію визнано країною-спонсором тероризму. У цьому зв'язку першочерговими видаються дії, спрямовані на створення інформаційного «залізного купола», якими би повністю держава-терорист була позбавлена найменших можливостей проникнення у медіапростір України, а особливо була позбавлена доступу і можливості втручання до будь яких відомостей, що стосуються сфери національної безпеки. Тому як одна з пропозицій, якою підсилюється актуальність і новизна дослідження, розглядається внесення доповнень до Конституції України, Закону України «Про інформацію» (стаття 7) в частині визначення імперативних вимог щодо недопущення контактів з російськими і дотичними до них джерелами інформації.

Саме тому це дослідження набуває значної теоретичної і практичної цінності, оскільки на шляху до повноправного членства України в ЄС, оборонному військовому блоці НАТО нашу державу очікують низка завдань, серед яких однією з ключових розглядається сфера інформаційної безпеки.

Говорячи про необхідність внесення поточних правок у чинне законодавство з питань інформаційної безпеки, потрібно адекватно оцінювати технологічний аспект, а саме діджиталізацію більшості сфер суспільного життя, що вимагає в недалекій перспективі докорінного перегляду галузевих нормативно-правових актів, які покладені в основу відносин використання баз даних і обміну інформацією.

Ще одним аспектом, яким підсилюється своєчасність викладених у дослідженні висновків і рекомендацій, є необхідність підвищення медіакультури і медіаосвіти громадян на фоні стрімкого впровадження інформаційних технологій у повсякденне життя. Сучасні виклики, які мають місце у відносинах при користуванні базами даних, і на їх фоні поширення зловмисної практики з протиправного заволодіння персональними, насамперед фінансовими даними споживачів інформаційних послуг, вимагають постійного моніторингу уповноваженими органами інформаційного середовища з метою своєчасної нейтралізації і усунення джерел подібних загроз.

З огляду на вищесказане, вкрай необхідним є провадження перманентних системних дій усіма суб'єктами інформаційних правовідносин, включаючи міжнародні інструменти правового захисту сторін партнерських угод з питань координації технологічно-правових заходів на всіх стадіях проходження інформації. Така державницька позиція передбачає швидку імплементацію міжнародних стандартів у сфері інформаційного забезпечення, ініціювання і активну участь у процесах гарантування цілісності і достовірності відомостей,

які використовуються як інструменти легалізації договірних відносин та інших дій, пов'язаних з настанням правових наслідків.

Крім того, актуальність теми наукової розвідки зумовлюється непередбачуваністю ситуації у зв'язку з необхідністю для України нарощувати економічний та інформаційний потенціал на фоні деструктивних дій російських загарбників, оскільки за таких умов перед державою і її союзниками з'являються все нові і нові загрози, насамперед у сфері інформаційної безпеки.

Для нашого дисертаційного дослідження обрано значний науковий масив філософсько-правового, економічного та соціального характеру, представлений такими вченими (перелік невичерпний), як: філософи Плутарх, Оуен Р.; вітчизняні та зарубіжні науковці: Біленчук П. Д., Білько С. С., Гнатюк С. Л., Григорчук М. В., Дзьобань О. П., Довгань О. Д., Золотар О. О., Косілова О. І., Кудін С. В., Ліпкан В. А., Логінов О. В., Новицька Н. Б., Ткачук Т. Ю., Тихомиров О. О., Француз. А. Й., Цимбалюк В. С., Шевченко А. Є., Ярема О. Г. та інші.

Висловлюємо щирю подяку науковцям, які здійснили вклад в опрацювання проблем, пов'язаних з забезпеченням інформаційної безпеки. У межах дослідження ми посилалися на результати їх доробку як підґрунтя для виведення авторських висновків і узагальнень.

У дисертаційному дослідженні маються посилання до публікацій представників європейської наукової, а саме Milton B.G., Laura Chappell, Palgrave Macmillan, яким засвідчуємо повагу і бажаємо подальших здобутків на науковій ниві.

Застосування методологічних методів дослідження обґрунтовано посиланнями і цитуванням праць таких науковців: Арістова І. В., Балинська О. М. Білозьоров Є. В., Братута О. Г., Волинка К.Г., Власенко В. П.,

Гусарев С.Д., Заяць Н. В., Кельман М. С., Костицький М. В., Онищук І. І., Перун Т. С., Сурмин Ю. П., Шигун М.М. та інші.

Емпіричною базою дослідження слугували Конституція України, закони України, міжнародні нормативно-правові акти, вітчизняне законодавство, а також доробок експертів у сфері інформаційної безпеки, оприлюднений на доступних медіаресурсах.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертаційне дослідження виконане у межах планових науково-дослідних тем у галузі природничих, технічних, суспільних і гуманітарних наук НАН України на 2019 – 2023 роки, затвердженими Постановою НАН України від 30 січня 2019 р. № 30, ґрунтується на положеннях Національної стратегії у сфері прав людини, затвердженої Указом Президента України від 24 березня 2021 року № 119/2021, Стратегії розвитку Державного податкового університету на 2022 – 2027 рр., затвердженої Вченою радою Державного податкового університету 30 червня 2022 р., протокол № 11. Тема дисертації пов'язана з науково-дослідною роботою кафедри теоретико-правових дисциплін Державного податкового університету «Забезпечення дії права в процесі реалізації державної політики» (номер державної реєстрації 0117U006224).

Тема дисертації затверджена Вченою радою Університету державної фіскальної служби України (28.11.2019 р. протокол №12) і уточнена Вченою радою Державного податкового університету (22.02.2023 р. протокол № 8).

Мета і завдання дослідження впливають з контексту теми наукової розвідки, що покладає обов'язок всебічно проаналізувати юридичне явище «інформаційна безпека» з позицій здійснення ефективних превентивно-профілактичних заходів для захисту медіапростору держави з урахуванням особливостей провадження такої діяльності в умовах російської агресії проти України.

Відповідно до поставленої мети сформульовано наступні **завдання**:

- встановити загальнотеоретичні основи дослідження поняття «інформаційна безпека»;
- обґрунтувати методологічний інструментарій дослідження;
- висвітлити наукові погляди щодо поняття інформаційної безпеки та її закріплення в нормативно-правових актах;
- з'ясувати аксіологічні аспекти та роль держави у забезпеченні інформаційної безпеки;
- надати правову характеристику нормативної бази у сфері інформаційної безпеки;
- визначити та класифікувати джерела загроз інформаційній безпеці;
- охарактеризувати досвід інформаційної безпеки в країнах Європи;
- визначити шляхи вдосконалення інформаційної безпеки в Україні.

Об'єктом дослідження для нашої наукової розвідки виступають суспільні відносини, що виникають в результаті становлення, функціонування та розвитку сфери інформаційної безпеки в структурі національної безпеки, з урахуванням особливостей її захисту в умовах повномасштабного російського вторгнення, глобальних діджиталізаційних процесів, що відбуваються на світовому інформаційному просторі.

Предметом дослідження є теоретико-правові основи регулювання інформаційної безпеки в Україні.

Методи дослідження. Актуальні методи дослідження винесено в окремий підрозділ, де зазначено науково-практичне значення кожного методу для вирішення завдань наукової розвідки. У тексті обґрунтовано аксіологічне і дослідницьке значення універсальних методів вивчення системи правових явищ у їх взаємодії на прикладі функціонування інформаційної складової у складі цілісного юридичного феномену «національна безпека». Доцільність

застосування кожного методу підтверджується цитуваннями науковців, які внесли вклад у дослідження проблематики, пов'язаної з нормативно-правовим регулюванням відносин щодо володіння, розпоряджання і доступом до інформації.

Відзначаючи дослідницьке значення застосування методологічних інструментів для досягнення мети наукової розвідки, необхідно акцентувати увагу на перманентному діалектичному зв'язку між загальнонауковими і спеціальними методами дослідження, що обумовлює логічну побудову процесу здійсненого теоретико-правового аналізу комплексного поняття «інформаційна безпека».

Щодо аксіологічного значення загальнонаукових методів: *філософсько-діалектичний метод* сприяв комплексному дослідженню структурних елементів юридичного феномену «інформаційна безпека» у їх постійній і безперервній взаємодії зі складовими у системі заходів забезпечення національної безпеки (підрозділи 1.1, 2.1, 3.1); завдяки застосуванню можливостей *системного підходу* досягнуто розуміння діалектичного поєднання світоглядної, пошукової, пояснювальної та прогностичної функцій у підходах до тлумачення результатів дослідження та виведення авторських висновків (підрозділи 1.1, 2.2., 2.3, 3.1, 3.3); *метод наукового спостереження*, як структурний елемент сфери емпіричного пізнання, забезпечить логічні зв'язки між визначеними особливостями предмета наукової розвідки та оціночними підходами у тлумаченні як окремих складових поняття «інформаційна безпека», так і ролі і значення цілісної системи захисту в контексті забезпечення національної безпеки (підрозділи 2.1; 2.3, 3.2, 3.3); дослідницьке значення *методів наукового аналізу, синтезу, індукції, дедукції, ідеалізації, формалізації та сходження від абстрактного до конкретного* тощо прослідковується в усіх підрозділах роботи, оскільки завдяки їх можливостям досягається вирішення завдань щодо вивчення

внутрішньої структури поняття «інформаційна безпека» на всіх рівнях її прояву при функціонуванні цілісного механізму «національна безпека» (підрозділи 1.1, 2.1, 2.2, 2.3, 3.1, 3.2, 3.3).

Спеціально-наукові методи для нашої наукової розвідки забезпечили можливість дослідження особливостей і специфіки об'єкта і предмета з урахуванням практичних аспектів і теоретичних положень, завдяки яким сформувалося цілісне юридичне явище «інформаційна безпека». Такими інструментами наукового пошуку обрано: *порівняльно-правовий метод* - сприяв здійсненню логіко-правового аналізу відомих наукових підходів до дослідження проблематики забезпечення інформаційної безпеки, а саме синтезовано семантичну основу побудови системоутворюючих понять шляхом порівняння їх звичаєвого і юридичного наповнення для вирішення завдань, пов'язаних із захистом інформаційного середовища держави (підрозділи 2.1; 2.3, 3.1, 3.3); *метод державно-правового моделювання* – забезпечить створення уявної моделі системи захисту сфери інформаційної безпеки з урахуванням нормативно-правового регулювання інших дотичних сфер, насамперед місця цієї складової у загальному контексті провадження заходів щодо забезпечення національної безпеки, а також прокладе паралелі до шляхів упровадження у вітчизняну сферу регулювання суспільних відносин в інформаційній сфері з урахуванням європейського досвіду (підрозділ 3.2, 3.3); *метод тлумачення правових норм* створить підґрунтя для коректного й уніфікованого розуміння системоутворюючих категорій, які формують поняття «інформаційна безпека», положень проаналізованої нормативно-правової бази з регулювання відносин у сфері використання інформації, а також виведене на авторські висновки щодо результатів обопільного впливу універсальних дефініцій на стан дотримання конституційного правопорядку у зазначеній галузі (підрозділи 2.2, 2.3, 3.3); *формально-юридичний метод* наукового дослідження надасть підстави для

формалізації міжпонятійних і міжгалузевих зв'язків між системоутворюючими поняттями, а також забезпечить коректне розуміння внутрішнього змісту досліджуваного поняття (інформаційна безпека) з зовнішніми аспектами їх проявлення у структурі актів правового регулювання цієї сфери (підрозділи 2.2, 3.2, 3.3); *спеціально-юридичний метод* забезпечив можливість досягнути описовості статусного значення інформаційної безпеки як об'єднувальної ланки усіх складових цілісного юридичного явища «національна безпека» шляхом використання загально прийнятої легітимної термінології, що, своєю чергою, стало підґрунтям для виведення авторських пропозицій щодо прогнозування варіантів розвитку превентивно-профілактичних заходів на всіх рівнях протидії протиправним зазіханням на встановлений порядок обміну і використання інформаційних баз даних (підрозділи 2.2., 3.1, 3.3); *герменевтичний підхід* сприяв виведенню домінуючої ролі аналітико-порівняльних аспектів при тлумаченні історичних етапів у розвитку системи захисту інформаційної сфери України, створив теоретико-правове підґрунтя для обранні найбільш ефективного способу тлумачення змісту і наповнення конкретних понять і категорій, що були використані для формування сучасної системи захисту інформаційного поля держави (підрозділи 1.1, 2.1, 2.2, 3.1).

Все вищезазначене створило сприятливі умови для визначення нормативного ареалу функціонування сфери інформаційної безпеки, забезпечило отримання достатньої теоретичної бази для дослідження внутрішніх складових і зовнішніх проявів механізмів захисту інформації на різних етапах вітчизняного державного будівництва.

Наукова новизна одержаних результатів полягає в тому, що представлене дослідження є логічним продовженням і доповненням доробку вітчизняних науковців у правничій сфері на напрямках забезпечення інформаційної безпеки України в надзвичайно складних історико-правових умовах. Значне ускладнення

вбачаємо у тому, що здійснення наукової розвідки відбувається на двох, протилежних за своїм інструментальним наповненням напрямках: конструктивний (в рамках реалізації євроінтеграційних процесів) та деструктивний (з протидії загарбницькій війні росії проти нашої держави).

Дисертація є однією з перших в українській юридичній науці комплексним теоретично-історичним дослідженням теоретико-правових основ регулювання інформаційної безпеки в Україні.

Основними науковими здобутками даної праці стали:

вперше:

- запропоновано та обґрунтовано впровадження періодизації процесів формування та становлення системи інформаційної безпеки держави за часовою ознакою;

- виокремлено джерела загроз, пов'язаних з повномасштабним вторгненням до України військ російської федерації, масованим проведенням інформаційно-психологічних спеціальних операцій (ІПСО), широкого проведення з боку росії дезінформаційних кампаній з метою посіяти паніку і капітулянтські настрої серед населення;

- розроблено класифікацію джерел загроз інформаційній безпеці держави на підґрунті територіального чинника (зовнішні, внутрішні, локальні загрози);

- запропоновано класифікацію інструментів регулювання відносин в інформаційній сфері на основі юридичної природи нормативно-правових актів (міжнародне законодавство, вітчизняна система законодавчих актів, підзаконні нормативно-правові акти і локальні акти органів влади і місцевого самоврядування);

удосконалено:

- системоутворюючі дефініції та ключові елементи категоріально-понятійного апарату: «інформаційна безпека», «джерела загроз інформаційній

безпеці», «правове регулювання інформаційної безпеки», «система превентивно-профілактичних заходів у сфері інформаційної безпеки». Авторські пропозиції на вказаному напрямку сприятимуть покращанню розуміння ролі і значення інформаційної складової в системі національної безпеки України, забезпечать умови для провадження подальших технологічних та право-регулюючих заходів, спрямованих на забезпечення позбавленого від протиправних зазіхань інформаційного поля, а також визначать нові завдання щодо протидії агресивним зовнішнім загрозам для утримання і стабілізації правочинного інформаційного середовища;

– методологічний інструментарій наукової складової у відносно новій галузі правової науки (інформаційному праві) з метою поширення спеціальних методів дослідження, які найбільш повно і об'єктивно відображають внутрішні процеси, що відбуваються як всередині механізмів функціонування інформаційної сфери суспільства, а також як складової збірного поняття «національна безпека»;

– окремі аспекти у підходах до розуміння джерел загроз інформаційній безпеці з урахуванням необхідності розроблення і впровадження у діяльність управлінських органів системних техніко-правових заходів стримування і протидії протиправним посяганням на встановлений порядок отримання, володіння, розпоряджання і використання інформації;

дістали подальшого розвитку:

– теорія та методологія інформаційного права та захисту інформаційної безпеки України в частині надання обґрунтованих пропозицій на доповнення оприлюдненого наукового доробку авторськими висновками щодо періодизації процесів становлення інформаційного права України, класифікації загроз інформаційній безпеці, виокремленні нових джерел загроз у цій сфері, а також

зміст заходів, спрямованих на профілактику і недопущення протиправних зазіхань на встановлений правовий порядок користування інформацією;

– теоретичні підходи до розуміння аксіологічного значення інформаційного права як однієї з основних складових комплексного механізму, який визначається як «національна безпека»;

– узагальнення досвіду європейських країн та Великобританії на напрямках розбудови і підтримання належного рівня інформаційної безпеки на своїх територіях, що сприяє подальшому вдосконаленню вітчизняної нормативної бази у сфері інформаційної безпеки, приведенню у відповідність до міжнародних вимог і правил чинних внутрішніх нормативно-правових актів, а також імплементації у нашу правову систему найбільш ефективних інструментів боротьби з порушеннями в інформаційній сфері.

Практичне значення одержаних результатів полягає в тому, що висновки та пропозиції, які містяться в роботі, можуть бути використані у:

- *науково-дослідній сфері* – як підґрунтя для подальшого дослідження теоретико-правових основ регулювання інформаційної безпеки в Україні (акт впровадження навчально-наукового інституту права Державного податкового університету від 15 лютого 2023 р.);

- *освітній діяльності* – для проведення різних форм занять зі здобувачами вищої освіти, при підготовці підручників, навчальних посібників, розробці лекційних курсів, робочих програм, навчально-методичних комплексів із дисциплін «Історія держави і права України», «Теорія держави і права», «Історія учень про державу і право», «Історія українського права», «Історія України» (акт впровадження навчально-наукового інституту права Державного податкового університету від 15 лютого 2023 р.);

Особистий внесок здобувача. Дисертація є самостійною, завершеною науковою працею. Сформульовані в ній положення, узагальнення, висновки,

рекомендації та пропозиції обґрунтовано на підставі самостійно проведених досліджень.

У науковій статті *Local Self-government in European Countries: General Characteristics, Comparison and Ukrainian Realities*, опублікованій разом із А. Благодатним, Ольгою Барабаш, Андрієм Гончаровим, Володимиром Шатіло, автором висвітлено проблеми місцевого самоврядування у сфері інформаційної безпеки в Україні та деяких європейських країнах.

У тезах доповіді «Some aspects the conceptual study of regulatory and legal ensurement of information security», опублікованій разом із А. Гончаровим, автором висвітлено основи концептуального дослідження нормативно-правового забезпечення інформаційної безпеки.

У статті «Життєвий шлях, юридичні погляди та педагогічна діяльність В. Г. Кукольника (1765–1821)», опублікованій разом із А. Гончаровим, здобувачем висвітлено юридичні погляди В. Г. Кукольника у сфері інформаційної безпеки.

Ідеї та розробки, що належать співавторам, разом з якими були опубліковані наукові статті та тези доповіді, в дисертації не використовувалися. Для аргументації окремих положень дисертації використовувалися наукові праці інших учених, на які зроблено посилання.

Апробація результатів дослідження. Основні положення дисертації обговорювались на засіданні кафедри теоретико-правових дисциплін Державного податкового університету. Результати дослідження були оприлюднені на: Всеукраїнських науково-правових конференціях «Кібербезпека в Україні: правові та організаційні питання» (м. Одеса, 30 листопада 2018 р.), «Кібербезпека в Україні: правові та організаційні питання» (м. Одеса, 22 листопада 2019 р.), «Правова наука і державотворення в Україні у світлі сучасних глобалізаційних викликів: історія, теорія, практика (до 25-ї річниці

Конституції України)» (м. Маріуполь – м. Кривий Ріг, 11 червня 2021 р.), VII Всеукраїнській дистанційній науково-практичній конференції «Інформація та документ у сучасному науковому дискурсі» (м. Івано-Франківськ, 20 травня 2022 р.), міжнародній «Міжнародне право XXI століття: сучасність та майбутнє». (м. Ірпінь, 25 травня 2022 р.), міжнародній The IX International Scientific and Practical Conference «Analysis of the problems of science and modern education» (Prague 06 – 08 March 2023).

Публікації. Основні наукові результати дисертації викладені у 11 наукових публікаціях, серед яких 3 наукові статті, опублікованих у фахових юридичних виданнях України, затверджених МОН України, 1 наукова праця у виданні, яке включено до наукометричної бази Scopus, 6 тез доповідей на міжнародних та всеукраїнських науково-практичних конференціях та 1 публікація, яка додатково відображає результати дисертаційного дослідження.

Структура та обсяг дисертації. Дисертаційна робота складається зі вступу, трьох розділів, що містять вісім підрозділів, висновків, списку використаних джерел. Загальний обсяг дисертації становить 201 сторінки, із яких основного тексту – 171 сторінка. Список використаних джерел містить 240 найменувань на 24 сторінках. 3 додатки розміщуються на 6 сторінках.

РОЗДІЛ 1

ІСТОРИКО - МЕТОДОЛОГІЧНІ ОСНОВИ ДОСЛІДЖЕННЯ ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Загальнотеоретичні основи дослідження поняття «інформаційна безпека»

Запорукою успішного дослідження будь-якого правового явища є побудована на законах логіки правильна стратегія наукового пошуку, яка має ґрунтуватись на аксіоматичних і дискусивних аргументах, висловлених теоретиками і практиками у конкретній галузі права. Саме такий підхід гарантуватиме належний рівень фаховості результатів наукової розвідки і надаватиме пояснення авторського розуміння і особистого вкладу здобувача у розроблення предмету наукового дослідження.

Початковим етапом нашої роботи розглядаємо глибоке вивчення генези юридичного феномену «інформаційна безпека» як матеріального підґрунтя для подальшого визначення тих особливостей зазначеного явища, які вимагають подальшого розроблення на напрямках дотримання належного рівня національної безпеки. Особливого значення така робота набуває в умовах воєнного нападу росії на Україну, який розпочався 24 лютого 2022 року.

Дослідження цілісного поняття «інформаційна безпека» вимагає застосування комплексного підходу до розуміння значення (семасіології) кожного терміну, який його формує («інформація і безпека»). При цьому необхідно зауважити, що термін «інформація» застосовується не як системоутворююча складова, а вживається для означення якісної характеристики базового елемента, тобто категорії «безпека», що розкриває галузеве

спрямування і змістовне наповнення заходів, та створює відповідне поле нормативно-правового регулювання.

Для розуміння об'єктивного змісту цілісного поняття «інформаційна безпека» ми послуговуватимемося можливостями окремих методологічних інструментів (в основному, аналізу, синтезу та ін.), які сприятимуть вивченню глибинних діалектичних зв'язків між визначеними категоріями, що його формують.

Термін «інформація» (лат. *informatio*) – це відомості, про які-небудь події, чиюсь діяльність тощо [1].

Сучасний тлумачний словник української мови надає дещо ширше тлумачення цього терміну, а саме: інформація – це відомості про навколишній світ, процеси, які в ньому відбуваються, про події, ситуації...[2].

Чинним законодавством, зокрема Законом України «Про інформацію», подається офіційне тлумачення цього терміну: «інформація – будь які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» [3].

Згідно з Законом України «Про доступ до публічної інформації» [4] поняття «інформація» наділене дещо ширшими ознаками і з урахуванням кола користувачів його визначено крізь призму публічності, тобто подається як відомості, сформовані представниками органів влади і місцевого самоврядування при виконання ними службових обов'язків, зафіксовані в будь якій матеріальній формі.

Здійснений авторський юридичний аналіз нормативної бази у галузі інформаційної безпеки показав, що термін «інформація» отримав уніфіковане застосування в багатьох сферах суспільного життя. Також його цінність засвідчується широким використанням в усіх галузях юриспруденції, оскільки

згідно з обсягом закладеного у ньому поняття набуває властивостей впливати на конкретні правовідносини, надаючи їм упереджувально-профілактичного змісту.

Термін «безпека» - стан, коли кому-, чому-небудь ніщо не загрожує [5].

Детальне дослідження семантичного значення цього терміну в інших джерелах (словниках) показало, що він отримав аналогічне тлумачення. Це означає, що за змістом та етимологією він не викликає наукового різнобачення і сприймається однаково в усіх сферах застосування.

Законодавством України подано офіційне тлумачення стану захищеності людини і природи у навколишньому середовищі. Для юридичного фахового аналізу легітимного розуміння сутності цього елементу («безпека») в структурі чинників, якими визначається найширше поняття відсутності небезпеки, посилаємося до положень Конституції України [6], де статтею 3 найвищою соціальною цінністю визнаються людина, її недоторканість і безпека, життя, здоров'я, честь і гідність.

Статтею 17 Основного Закону забезпечення інформаційної безпеки розглядається у контексті пріоритетних завдань держави як складова системи захисту державного суверенітету і національної безпеки.

У Конституції України відведено особливу роль інституту Президента, який відповідно до покладених на нього обов'язків забезпечує національну безпеку та державну незалежність (стаття 106), що включає в себе заходи щодо утвердження достатнього рівня інформаційної безпеки.

Про виключне значення досліджуваного терміну для науковця говорить те, що в Основному Законі його ужито 36 разів. Принагідно потрібно зауважити, що відособленого застосування цього терміну в законодавстві ми не виявили, проте наданням йому ознак галузево-орієнтованого характеру досягається повне розуміння змісту, який апріорі закладається у наповнення заходів у конкретній сфері життя суспільства.

Положеннями Закону України «Про національну безпеку України» [7] вводяться поняття воєнної, громадської і державної безпеки, що формує цілісне поняття «національна безпека», і розглядається як узагальнююча категорія в системі провадження заходів із захисту державного суверенітету, цілісності і неподільності території, встановлених конституційних гарантій демократичного вектора розвитку суспільства, а також створення ефективних механізмів нейтралізації джерел загроз українській державності.

Законом України «Про основи національної безпеки України» основна компонента державного суверенітету подається у широкому поєднанні з усіма сферами життєдіяльності суспільства, що засвідчує здатність розкривати всі аспекти змісту заходів, що вживаються для дотримання конституційного правопорядку з урахуванням зовнішніх чинників (міждержавного спілкування).

У розумінні положень коментованого Закону «національна безпека – захищеність...і забезпечення свободи слова та інформаційної безпеки, кібербезпеки та кіберзахисту...при виникненні негативних тенденцій до створення потенційних або реальних загроз національним інтересам [8].

Вибірковий аналіз чинного законодавства і оприлюдненого наукового доробку показав, що термін «безпека», як і «інформація», має міжгалузеве застосування, оскільки завданням усіх сфер правоохоронної і правозабезпечувальної діяльності є створення умов, що позбавлені і не допускають настання будь-яких негативних чи загрозливих наслідків як від природного середовища, так і від діяльності людей. Уважаємо, що саме з таких позицій потрібно оцінювати наукове супроводження процесів розроблення, удосконалення, оновлення й адаптації до європейських стандартів законодавства України, у тому числі й тих нормативно-правових актів, де йдеться про інформаційну безпеку.

На цьому етапі доцільно більш детально зупинитися на історичних аспектах цього юридичного феномену, проаналізувати економіко-соціально-правові передумови необхідності розвивати інструменти зі знешкодження, пригнічення і повного подолання загроз, що пов'язані з протиправним, деструктивним впливом зовнішніх інформаційних ресурсів, а також внутрішніх чинників, які загрожують національній безпеці держави.

З метою забезпечення комплексного підходу до виконання завдань нашого наукового дослідження звертаємося до джерельної науково-практичної бази у сфері інформаційної безпеки України. Це означає, що емпіричною базою для такого аналізу слугуватимуть опрацьовані нами джерела без градації на галузеву приналежність.

О. Д. Довгань, Т. Ю. Ткачук, досліджуючи історичні аспекти та джерела оприлюднення перших згадувань про інформаційну безпеку, зазначають: «Проблематика інформаційної безпеки та її забезпечення у різних аспектах висвітлювались у наукових працях Плутарха, Сенеки, Платона, Макіавеллі, Гроція, а також інших вітчизняних та зарубіжних дослідників» [9, с. 80].

Як вбачається з наведеної вище цитати, логічним висновком є те, що сфера інформаційної безпеки ще в ранні часи набула дуалістичного характеру. Причиною цьому, на наш погляд, є те, що вказані вчені мали визначні досягнення не тільки в юриспруденції, а й у філософії. Тому виведені ними узагальнення поєднують у собі юридичну і філософську компоненту.

О. О. Золотар, досліджуючи першоджерела інформаційної безпеки, зазначає, що «початок історії захисту інформації вчені пов'язують з появою можливості фіксації інформаційних повідомлень на твердих носіях, тобто з винаходом писемності, а першим видом інформації, що підлягала захисту, вважають державну таємницю» [10, с. 140].

На думку науковця, майже одночасно з винайденням писемності були відкриті методи і способи захисту інформації, а саме шифрування і приховування. Як приклад О. О. Золотар наводить історичний факт, що засвідчує спосіб захисту інформації від стороннього доступу і поширення. Такий випадок відомий як перший шифрований текст, прихований під рецептом глазури при нанесенні її на вироби гончарства (Месопотамія, 2000 років до н. е.).

Відомі наукові погляди щодо розуміння та формування парадигми інформаційної безпеки мають в основі широку палітру філософського знання, що сягає своїм корінням глибокої давнини. Філософи минувшини завжди досліджували причини і джерела загроз, намагалися домогтися стабільного миру та процвітання. За таких умов трансформувалися підходи до розуміння інформації. Питання безпеки особи, суспільства, держави та отримання достовірної інформації цікавили мислителів Стародавнього світу. Щоправда, вказана проблема розглядалася переважно в контексті війни й миру [11, с. 40].

Плутарх, древньогрецьких філософ-мораліст, письменник, історик, у своїх працях наводить звичай: кожного, хто входив до сисситії (трапезної), «...старший, вказуючи на двері, попереджав: «Жодне слово з них не виходить» [12, с. 181].

О. Курбан, досліджуючи генезу інформаційного впливу в XVIII столітті на прикладі боротьби за незалежність мешканців північноамериканських колоній, зазначає: «У своїй боротьбі колоністи використовували соціальні мережі (товариства «Сини свободи», «Кореспондентські комітети»), застосовували образні символи («дерево свободи», стереотипи та лозунги «Воля або смерть»). Вони дуже активно застосовували дієві акції, тогочасні медіа, чутки, маніпуляцію» [13, с. 30].

О. П. Дзьобань, досліджуючи наукову спадщину Томаса Гоббса та Еммануїла Канта, зазначає, що «наукове обґрунтування проблеми національної

безпеки взагалі, й інформаційних її аспектів зокрема, в сучасному розумінні й певні напрямки її вирішення містяться у працях вказаних науковців» [14, с. 41].

О. Павленко, вивчаючи генезу інформаційної безпеки, здійснила аналіз історичних джерел виникнення і розвитку цієї галузі права, і запропонувала його поділ на етапи:

I етап – до 1816 року – характеризується використанням природно виникаючих засобів інформаційних комунікацій. Для цього періоду основним завданням збереження відомостей полягало в недопущенні сторонніх осіб до володіння інформацією про факти, майно, події тощо, які мали для людини чи колективу людей важливе, а в окремих випадках – життєве значення.

II етап – починаючи з 1816 року – пов'язаний з початком використання штучно створюваних технічних засобів електро- і радіозв'язку. Поряд з використанням досвіду попереднього періоду застосовувалися такі інструменти захисту інформації, як «перешкодостійке кодування повідомлення (сигналу) з подальшим декодуванням прийнятого повідомлення (сигналу)».

III етап – починаючи з 1935 року – пов'язаний з появою засобів радіолокацій і гідроакустики. У цей період головним напрямком у сфері захисту інформації було забезпечити приймальні пристрої радіолокаційних систем «активними маскуючими і пасивними імітуючими радіоелектронними перешкодами».

IV етап – починаючи з 1946 року – пов'язаний з винаходом і впровадженням у практичну діяльність електронно-обчислювальних машин (комп'ютерів). Для даного етапу характерним виступало фізичне обмеження доступу сторонніх осіб до устаткування, на якому зберігалася інформація.

V етап – починаючи з 1965 року – обумовлений створенням і розвитком локальних інформаційно-комунікаційних мереж. Завданнями інформаційної

безпеки зазначеного періоду були забезпечити ефективне збереження інформації шляхом фізичного захисту джерел (носіїв) інформації.

VI етап – починаючи з 1973 року – пов'язаний з використанням надмобільних комунікаційних пристроїв з широким спектром завдань. З урахуванням технологічних проривів загрози інформаційній безпеці ставали дедалі серйознішими, що вимагало розроблення відповідних систем захисту від несанкціонованого втручання (хакерства) у порядок використання інформаційних ресурсів. У цей час починає формалізуватися інформаційне право як нова галузь міждержавної правової сфери.

VII етап – починаючи з 1985 року – пов'язаний зі створенням і розвитком глобальних інформаційно-комунікаційних мереж з використанням космічних засобів забезпечення [15].

Колектив науковців, серед яких А. Б. Тоцький, О. І. Тимошенко, А. М. Гуз, вважають, що історія охорони і захисту інформації на території сучасної України також сягає ще додержавних часів. Першим видом інформації, яку потрібно було охороняти, була військова інформація. Спочатку охорону такої інформації забезпечував князь, потім особа, яку він призначав особисто. Війна була на той час головним і загальновизнаним способом ведення зовнішньої політики будь-якої держави, тому захист військової інформації був головним у політиці князів Олега, Ігоря, Святослава, Ярослава та княгині Ольги. Князі, йдучи в похід, намагалися приховати інформацію про кількість війська і напрям головного удару. Ворог не міг адекватно реагувати на небезпеку, а заздалегідь розпущені чутки, перебільшення і неправдива інформація ще більше призводили до паніки [16, с. 11].

У контексті сказаного вище доцільно навести озвучений результат наукової розвідки колективу у складі В. М. Петрик, А. М. Кузьменко, В. В. Остроухов, які віднайшли одне з первинних документальних свідчень про

застосування інформації з метою обману ворогів при провадженні воєнних дій. Науковці зазначають, що до XIII ст. належить один з перших історичних прикладів масштабного застосування дезінформації у воєнних цілях. Пов'язаний цей приклад із вторгненням монголів до Угорщини у 1241 р. [17, с. 56]. Монголи розбили військо угорців та їх союзників на річці Шайо і при цьому серед трофеїв виявили королівську печатку. Хан Батий наказав підготувати наказ угорською мовою від імені короля Бели про припинення опору, скріпивши його захопленою королівською печаткою. Цей документ розіслали в різні частини ще не завойованої країни, що сприяло введенню в оману угорської армії.

Окремо слід вирізнити напрацювання у цій галузі права закордонних науковців, яких ми вибірково зачитуємо.

Так, Роберт Оуен уважав, що «тільки звільнення народів від приватновласницького ярма й об'єднання їх в один союз покладе край насильству й уможливить забезпечення безпеки [18, с. 375]. На думку відомого філософа й економіста, справжній безпековий стан як вселюдська гармонія можливий лише за умови організованого виховання населення при застосуванні інформаційних інструментів виховного характеру.

Ю. М. Канигін та В. І. Кушерець вважають, що «суспільство з великим запізненням починає осмислювати політичні, економічні, соціальні, військові, психологічні та інші наслідки глобальної інформатизації» [19, с. 35].

Вважається, що одними з перших проблеми комп'ютерної інформаційної безпеки усвідомили і зробили впевнений крок до їх вирішення державні відомства США в кінці 60-х років XX століття, коли комп'ютери коштували великих грошей, а інтернет зароджувалася з нечисленних, виключно військових і наукових інформаційних мереж [20, с. 17].

Українська історія також зберегла свідчення про факти використання інформації як для доведення до відома ворога неправдивих відомостей, та і для

організації протидії внутрішнім загрозам щодо недопущення витоку секретної інформації.

Так, у матеріалах раніше згадуваного доробку авторського колективу за участі А. Б. Тоцького, О. І. Тимошенко, А. М. Гуз, знаходимо відомості про те, що у Запорізькій Січі та державі Богдана Хмельницького вироблені були своєрідні форми захисту військово-політичної інформації. Хмельницький широко використовував дезінформацію. В спогадах польських урядовців та військових часто зустрічається рядки на кшталт «одне думає, про інше пише», «наміри його жодним чином не можна зрозуміти». Хмельницький зазначав у жовтні 1648 р.: «А військова справа така: коли мисль буде йти на війну, щоб тої мислі ніхто не відав і недруг би остерігався» [16, с. 14].

Основною метою зловмисників завжди буває порушення складових інформаційної безпеки – доступності, цілісності або конфіденційності [21].

С. О. Лисенко: Серед останніх новацій із-за кордону варто зазначити, що 15 липня 2016 року німецький уряд затвердив план «Біла книга» з питань оборонної політики та безпеки, в тому числі інформаційної. В ній чітко вказано, що Російська Федерація стала реальною загрозою, що шкодить існуючому міжнародному порядку та європейській безпеці. У першу чергу, це пов'язано з агресією проти України.

Поточним підсумком до вищесказаного є те, що сучасний стан і розуміння значення інформаційної безпеки нерозривно пов'язані з тими наріжними каміннями, на яких виникла і ґрунтується державна політика у сфері забезпечення як національного, так і міжсуб'єктного спілкування з дотримання межових знаків, встановлених як допустимі норми освідомлення з приватно-державними процесами конкретних національних утворень.

Показовими у цій ситуації є висновки, озвучені С. О. Лисенко за результатами дослідження історичних аспектів інформаційної безпеки як сфери

спеціальних правовідносин. Науковець зазначає, що в ситуації, що склалась, правомірно «задекларована необхідність підвищення загальної інформаційної захищеності всього блоку НАТО... [22, с. 42]. При цьому науковець відзначає надзвичайну потребу у створенні Європейської ПРО, а також висловлюється про необхідність удосконалення механізмів захисту інформаційного поля. Такий підхід можна пояснити необхідністю створення оновленої системи захисту інформації між країнами НАТО в зв'язку з загарбницькою політикою російської федерації проти України.

Як вбачається з вищенаведеного, інформація не існує відособлено від людського середовища і має конкретну мету, з якою впливає на суспільство. Здійснене авторське дослідження підтвердило науково-практичну тезу про те, що на різних етапах розвитку суспільства рівень інформаційного впливу на людей напряду залежав від розвитку інструментів інформаційного впливу. Саме для розв'язання окремих завдань нашого дослідження ми торкнулися генезуальних проблем у підходах до розуміння правової природи інформаційної безпеки. На наш погляд, фундаментальними засадами виникнення у зародковому стані понять, які сьогодні визначені як інформаційна безпека, є звичаєве право, елементи якого у процесах розвитку цивілізації набули загальнообов'язкового характеру для їх учасників на підґрунті запровадження нормативно-правового регулювання цієї сфери.

1.2 Методологія дослідження основ інформаційної безпеки

Специфічна природа інформаційної безпеки вимагає обрання і застосування особливих методів наукового дослідження і полягає в імплементації фахового знання про такі методи й інструменти пізнання правової реальності, закономірності розвитку і функціонування правових механізмів, а

також їх застосування для об'єктивного відтворення правової природи досліджуваних явищ і процесів при формуванні понятійно-категоріального апарату. Тому здійснений авторський пошук показав, що викристалізовування та зміцнення нормативно-правового підґрунтя правої науки в галузі інформаційної безпеки здійснювалось поетапно і послідовно. Законодавець і представники науки інформаційного права й інформаційної безпеки своєчасно і більшою мірою адекватно реагували на виклики у найбільш вразливих сферах життя суспільства і держави.

Процес нормативно-правового регулювання правовідносин в означеній сфері права супроводжувалося активізацією наукових досліджень, що мали на меті реалізацію завдань з розбудови методології науки інформаційного права й інформаційної безпеки. Суспільно-економічна ситуація в державі і національна політика вимагали постійної роботи на напрямках посилення національної безпеки, що є підставою стверджувати, що об'єктивізація методологічного інструментарію для дослідження правової структури інформаційної безпеки відбувається на перетині різних галузевих правових наук. На нашу думку, саме такий підхід сприяв максимальному збагаченню і удосконаленню методологічного інструментарію цієї сфери.

Відомо, що система інструментів наукового дослідження обрамлюється поняттям «методологія», тобто об'єднує концепції і парадигми вивчення окремих правових явищ з метою розвитку правової науки.

У науковому середовищі, високо оцінюючи значення інших суспільних наук, вважають, що питання методології наукового пізнання у їх системності і взаємозв'язку закономірно стають одними з провідних на загальному фоні сучасної науки.

Для розв'язання завдання нашої наукової розвідки ми обрали низку методологічних інструментів, якими намагатимемося піддати додатковому

вивченню окремі аспекти значимості правового явища «інформаційна безпека» у діалектичному зв'язку з іншими складовими процесу державотворення. Дану проблематику розроблятимемо послуговуючись загально відомими методами наукового дослідження з урахуванням особливостей, якими характеризуються напрямки впливу інформаційної безпеки на стан формування і здійснення заходів у сфері національної безпеки.

Для надання нашій роботі ознак науковості, опираємося на узагальнене розуміння сутності авторського наукового доробку, який отримуємо завдяки виконанню основних критеріїв, одним з яких є дослідження обраного об'єкта – суспільних відносин у сфері забезпечення інформаційної безпеки.

Згідно з Універсальним словником-енциклопедією науково-дослідна праця – це систематичне й цілеспрямоване вивчення об'єктів, у котрих використовуються засоби й методи науки та яке завершується формуванням знань про об'єкт, що вивчається [23].

Оцінюючи науковознавче значення методології, не викликає сумніву, що для вирішення конкретно обраних проблем нового наукового знання необхідно застосовувати комплексно увесь інструментарій сучасної формальної логіки, але домінуюча роль належить методології науки, оскільки в її основі лежать не лише логіка та гносеологія, але і вся філософія.

Розв'язуючи завдання цього наукового дослідження, усвідомлюємо, що зроблені висновки не будуть позбавлені дискусійності і викличуть певний рівень критичних зауважень. Поряд з цим ми не відмежовуватимемось від оприлюдненого логіко-правового підходу в сфері сприйняття дії і гіпотетичних результатів застосування окремих методів дослідження до виведення авторських узагальнень з піднятої проблематики.

При обранні комплексу відповідних методів та способів отримання, перевірки, узагальнення та викладення наукових знань ми виходимо з того, що

такий підхід забезпечить повномірне висвітлення науковознавчої складової у загальному контексті чинного нормативно-правового забезпечення інформаційної безпеки України. Беремо до уваги також те, що методологія як наука є надзвичайно гнучкою і завдяки розробкам представників різних галузей права постійно оновлюється й удосконалюється. І це при тому, що основне логіко-семантичне наповнення методологічних інструментів залишається константою, не змінюється у своїй внутрішній сутності, слугуючи підґрунтям для формування нових поглядів і розкриття чи додаткового пояснення об'єктивно існуючих правових явищ з огляду на предметно-галузеве спрямування дослідження.

Отже, під час проведення дослідження нормативно-правового забезпечення інформаційної безпеки не доцільно використовувати найбільш широкий інструментарій сучасної наукової методології, а не задовільнятися лише власне правознавчими методами. На думку Т. С. Перуна, «комплексне застосування методів уможливорює досліджувати проблеми у єдності їх соціального змісту і юридичної форми, здійснювати системний аналіз вказаних праць [24].

На думку науковця, найбільш повному результату для досягнення цілей дослідження необхідно комплексно застосовувати діалектичний, компаративний, структурно-функціональний, історичний та інші методологічні інструменти, що сприятиме всебічному вивченню нормативно-правового забезпечення інформаційної безпеки, а також уможливить використання дослідницьких якостей логічного, історико-соціологічного та порівняльно-правового методів наукової розвідки.

Теоретико-методологічна основа сучасного знання про інформаційну безпеку характеризується діалектичним поєднанням відособлених елементів взаємовпливом об'єктивних чинників, що набувають детермінантних ознак для

певних рівнів здійснення заходів з підтримання достатнього рівня національної безпеки. На цьому етапі говоримо про необхідність застосування діалектичного методу наукового дослідження як універсального інструменту через його здатність мати всеохоплюючий вплив на всі події і явища, що забезпечує можливість пізнання окремих процесів у їх сукупності, перманентному чи тимчасовому взаємозв'язку і розвитку. Завдяки гносеологічній природі цього методу відбувається поступальний, прогресивний рух від незнання до знання.

Л. Булавін вказує, що діалектичний метод надає дослідникові можливість вивчати всі явища довколишнього світу в «їхньому взаємозв'язку та взаємодії, в їхньому розвитку і еволюції шляхом переходу кількості в якість, обумовленого боротьбою внутрішніх протилежностей, закладених у цих явищах» [25, с. 4]. Наведе судження науковця, хоч і не пов'язане з дослідженням проблем правового характеру, повномірно відображає сутність і дослідницькі можливості цього методу наукового пошуку.

М. В. Костицький, досліджуючи філософські та методологічні проблеми права, акцентує увагу на значному дослідницькому потенціалі діалектики і її категорій. На думку науковця, категорії діалектики є універсальними логічними формами мислення, в яких відображені ті загальні властивості, відношення і зв'язки, які існують в об'єктивній реальності. Без понять і категорій пізнання дійсності було б неможливим [26, с. 13]

М. С. Кельман, визначаючи підходи щодо методології, вказує, що у цьому зв'язку виникають питання, з одного боку, про використання загальних знань про безпеку при дослідженні соціальних проблем, вивчення яких у логіко-гносеологічних аспектах може призвести до отримання нового, так і до поглиблення раніше отриманого знання, а з іншого – при виробленні та прийнятті управлінських рішень з проблем забезпечення безпеки [27, с. 42–43].

Ми підтримуємо висловлену науковцем думку, оскільки при формуванні категоріально-понятійного апарату конкретної галузі права використання універсальних методологічних інструментів (діалектичного, логічного, інформаційного, системного, структурно-функціонального та інших методів) розширює межі і глибину наукового пошуку.

Основним джерелом істинності і послідовності у викладенні авторських висновків виступає системний підхід, який, за висловлюванням І. І. Онищука, забезпечує «єдність методологічної інтеграції та диференціації з домінуванням тенденції об'єднання, збирання методологічного комплексу [28].

Підводячи підсумок висловлених науковцем думок, необхідно відзначити прихильність до об'єднавчого застосування наукознавчих методів з поясненням функцій окремо взятого методологічного інструменту. Так, наприклад, І. І. Онищук вважає, що світоглядна функція відіграє первинну роль у системному підході, оскільки є підґрунтям для формування світогляду людини, здатність до відкриття трактується основною функцією евристичного методу, для пояснення процесів і явищ головною відзначається здатність розкривати їх внутрішню сутність і структуру у межах застосування пояснювального методу, можливість формулювати очікувані варіанти розвитку ситуації розглядається основною для прогностичного методу.

Значення системного підходу визначається не лише встановленням певним логічним порядком проведення логічних операцій. Головною його рисою виступає методологічність, тобто використання його не стільки як способу представлення світу, а і як методу його пізнання. В цьому полягає його методологічна функція, коли системність у пізнавальному процесі працює як принцип, метод і теорія [29, с. 304].

Водночас доцільно погодитися з А. Б. Качинським у висновках про значення всебічного дослідження причин виникнення суспільно загрозливих

явищ, а також ролі людини у цих процесах, де він надає оцінку загальнонауковому пізнанню як інструменту реалізації такого завдання. Науковець вважає, що «...від результатів залежить соціальна оцінка і активна державна політика в галузі забезпечення інформаційної безпеки» [30, с. 13–14].

Стає зрозумілим, що до переліку дотичних питань соціальної практики з високим відсотком ймовірності можна причислити проблему інформаційної безпеки, вирішення теоретичного і прикладного значення якої передбачає, насамперед, достатньо широке, повномірне загальнонаукове усвідомлення в формально-логічному об'єднанні висновків:

– по-перше, теоретико-прикладне розв'язання завдань у сфері дотримання інформаційної безпеки структурується в чітку науково-практичну площину на напрямках наукових досліджень щодо вироблення і виконання заходів з забезпечення належного рівня інформаційної безпеки як форми управління соціальною сферою;

– по-друге, завдяки застосуванню наукових методів дослідження загроз сфері інформаційної безпеки можна здійснити науковий прогноз щодо результатів переведення теоретичних умовиводів у практичну площину, що однозначно сприятиме поширенню загальних якостей економіко-правової категорії «безпека» на більш конкретне юридичне явище, яким є «інформаційна безпека»;

– по-третє, завдяки діалектичним якостям загальнонаукових і спеціально-наукових методів дослідження, які притаманні інструментам наукового аналізу і синтезу, у межах теоретико-методологічного супроводження процесів сфери інформаційної безпеки відбувається поділ і поєднання гуманітарних, природничих, технічних та інших знань, які акумулюють в собі загальні характеристики всіх структурних елементів соціального середовища,

забезпечуючи відповідний і необхідний баланс для їх нормального функціонування і розвитку.

Досліджуючи методологічне забезпечення науки «інформаційне право», І. П. Арістова концентрується на «важливості взаємодії усіх галузей юридичної науки, оскільки це дозволяє досліджувати предмет однієї із галузей юридичної науки (наприклад, науки «Інформаційне право») [31, с. 13]. При цьому науковець відзначає домінуючу роль вченого, який, здійснюючи дослідження у сфері інформаційного права, не має права обмежуватись виключно вивченням правових механізмів чи іншої проблематики лише спеціальними методами. Вчений зобов'язаний враховувати ті нерозривні зв'язки між наукою «інформаційне право» та юридичною наукою в цілому, які виступають об'єктивним підґрунтям для пояснення всіх правових подій і явищ.

Для продовження курсу на дотримання логічної послідовності при верифікації авторських висновків щодо предмета наукової розвідки ми покладаємо нашу роботу в русло загальної лінії науки, тобто проаналізуємо вплив загальнонаукових і спеціально-наукових методів дослідження.

Застосовані нами загальнонаукові методи (емпіричні і теоретичні) відображатимуть головні завдання дослідження, оскільки узагальнюють результати оприлюдненого наукового доробку з позицій системного застосування принципів і прийомів, що відображають наскрізний зв'язок між всіма правовими явищами, об'єднаними категорією «юриспруденція». Такий підхід обґрунтовуватиме посилення до наукових здобутків у різних галузях науки, оскільки методологічним інструментам, віднесеним до цієї категорії, притаманні характеристики абстрактності, відсутності чіткого галузевого розмежування і регламентації.

Надаючи тлумачення сутності методів юридичної науки, Ю. Скиба розуміє загальнонаукові методи як такі, що мають «загальнонауковий характер і

використовуються в усіх або у низці галузей, та спеціальні, як методи, що використовуються у певній галузі і не виходять за її межі й використовуються у кожній науці в різних співвідношеннях» [32, с. 53].

На цьому етапі доцільно обрати, на наш погляд, найбільш ефективні для нашого дослідження методологічні інструменти і проаналізувати їх пізнавальне значення.

Застосування методу наукового спостереження як складової сфери емпіричного дослідження в структурі загальнонаукових методологічних прийомів сприятиме виокремленню особливостей і наданню правової оцінки окремим аспектам, які мають місце у процесах нормативно-правового регулювання сфери інформаційної безпеки. Компетентне узагальнення законотворчої діяльності, що стосується місця і ролі інформаційної безпеки в системі заходів з посилення національної безпеки, сприятиме виведенню авторських обґрунтованих висновків щодо ефективності і своєчасності прийняття і впровадження відповідних норм і правил.

В. В. Ковальчук та Л. М. Моїсєєв вважають, що «спостереження стає методом тоді, коли воно не обмежується тільки констатацією, описом фактів, а має наукове пояснення, класифікацію» [33, с. 132].

Можливості порівняльного методу застосовуватимемо при аналізі ефективності і якості прийнятих законодавчими актами рішень у сфері забезпечення інформаційної безпеки. Такі логічні операції здійснюватимемо щодо міжнародних правових актів, які відповідно до Конституції України є частиною національного законодавства держави (стаття 9 Основного Закону).

Компаративістський підхід також використовуватимемо при логіко-правовому аналізі оприлюднених наукових позицій, тобто здійснимо порівняння семантичного і мисленнєвого наповнення дефініцій окремих елементів в структурі заходів з захисту інформаційної безпеки, а також порівняємо

теоретико-правове значення чинних норм права у цій галузі з аналогічними нормами європейського законодавства.

Є. В. Павліченко та М. І. Голинська, оцінюючи значення порівняльно-правового методу для правової науки, зазначають, що порівняльно-правові дослідження є надзвичайно важливими для юридичної науки та для її розвитку, вони тісно пов'язані з міжнародним публічним і приватним правом, з галузевими юридичними науками, для яких формується інформація для теоретичних узагальнень на рівні, вищому за національний, а також відіграє важливу роль у процесі міжнародної уніфікації та гармонізації права [34, с. 20].

Значну увагу приділимо аналітико-правовій діяльності на основі застосування методів, що віднесені до теоретичного способу дослідження, якими є аналіз, синтез, індукція, дедукція, ідеалізація, формалізація, сходження від абстрактного до конкретного тощо. Переконані, що завдяки застосуванню системи інструментів теоретичного рівня зможемо дослідити внутрішню структуру складного правового феномена, яким є інформаційна безпека, ґрунтуючись на законах логіки і діалектики вивести закономірності взаємодії його структурних елементів і механізмів, якими вони приводяться в дію.

За допомогою можливостей прийому наукового аналізу, який виступає підґрунтям аналітичного методу наукового дослідження, цілісне правове явище «інформаційна безпека» буде поділено на структурні елементи, що надасть можливість вирізнити нові характерні ознаки обраного предмета наукової розвідки. Закладений в основі цього методу алгоритм дій розкриє не тільки внутрішню структуру предмета дослідження, а й прояснить порядок діалектичних зв'язків між ними і способи взаємодії.

Колектив науковців, серед яких Шевченко А. Є., Француз А. Й., Кудін С. В. вважають, що концептуальне конструювання сучасної системи забезпечення інформаційної безпеки містить певну складність унаслідок своєї

багатоаспектності та передбачає розробку як теоретико-методологічних питань, так і нормативно-правового механізму, основних напрямів, форм і методів реалізації відповідних нововведень [35, с. 51].

Метод наукового синтезу прокладе для нас зворотні процеси, за допомогою яких ми здійснимо мисленнєве поєднання виокремлених структурних елементів поняття «інформаційна безпека», а послідовність їх приєднання відкриє нові аспекти в підходах до уточнення чи спростування усталених висновків щодо функціональних можливостей цього поняття у загальній системі категоріального апарату правової науки, які об'єднуються поняттям «національна безпека».

О. Г. Братута визначає сутність синтезу як засобу теоретичного пізнання полягає у створенні нового наукового знання про явище як цілісний об'єкт на основі знання, попередньо отриманого певним способом [36, с. 14].

Завдяки можливостям індуктивного методу ми намагатимемося вивести нове знання з результатів аналітико-синтетичного поділу (поєднання) окремих структурних елементів поняття «інформаційна безпека». На підставі виведених узагальнень буде розроблено пропозиції на напрямку удосконалення чинного законодавства у сфері захисту інформаційного простору України.

Суворо дотримуючись законів логіки при побудові авторських умовиводів за результатами застосування вищевказаних методологічних інструментів, вийдемо на рівень дедуктивних узагальнень, які ґрунтуватимуться виключно на отриманих нами авторських висновках.

У зв'язку з наведеним, метод формалізації сприятиме обґрунтуванню авторських висновків щодо необхідності прийняття нових норм чи внесення і доповнення до чинного законодавства з метою усунення можливостей для спекуляцій щодо дублювання господарським правом нормативної бази інших галузей права.

А. Є. Конверський зазначає: «У науці термін «формалізація» має кілька значень: 1) метод логіки, який полягає в застосуванні формалізованої мови до вивчення предмета логіки; 2) процес кодування засобами формально-логічної теорії фрагментів наукових теорій чи самих теорій; 3) відображення понять логічної семантики у поняттях логічного синтаксису [37, с. 52].

Послугуючись можливостями методу ідеалізації, ми намагатимемося на підґрунті чинного нормативно-правового середовища у сфері національної безпеки запропонувати нову, позбавлену прогалин у правовому регулюванні систему захисту інформації на всіх рівнях її функціонування.

У розумінні методологічної науки ідеалізація – це спосіб логічного моделювання, завдяки якому створюються ідеалізовані об'єкти. Ідеалізація спрямована на процеси мислимої побудови можливих об'єктів. Межі ефективності ідеалізації визначаються практикою [38].

Метод сходження від абстрактного до конкретного обумовить підстави для введення в правове поле ідеалізованих (мисленнєво-створених авторами) конструкцій у сфері інформаційної безпеки як гіпотетично можливих шляхів удосконалення системних механізмів функціонування цього юридичного феномену.

О. В. Закаленко та О. В. Большакова характеризують метод сходження від абстрактного до конкретного як універсальний і здатний вивчати окреслену систему явищ, тому що кожна, на перший погляд, не причетна до розвитку система при ближчому розгляді завжди виявляється чи частиною чи етапом більш широкої і складної системи, що знаходиться у процесі розвитку [39 с. 113].

Наступним етапом у виконанні завдань нашого дослідження стане застосування спеціально-наукових методів (порівняльно-правовий, державно-правового моделювання, тлумачення правових норм, формально-юридичний, спеціально-юридичний та ін.).

Порівняльно-правовий (порівняльний, компаративний) метод у межах нашого дослідження використаємо для визначення змісту та сутності структурних елементів поняття «інформаційна безпека», виокремлення їх характеристик, аналізу чинних правових норм, які регулюють цю сферу правовідносин, а також для виявлення особливостей і окремих аспектів їх взаємодії з метою подальшого напрацювання можливих напрямів удосконалення законодавства України і сфери його застосування.

Х. Юркевич, оцінюючи значення порівняння при дослідженні правових явищ, вважає, що «у загальному розумінні порівняльно-правовий метод – це метод вивчення правових систем різних держав шляхом зіставлення однойменних правових норм, інститутів, принципів тощо та практики їх застосування» [40, с. 157].

Порівняльно-правовий метод, на думку В. М. Шаповала, виступає також і як метод емпіричних досліджень, тобто на рівні техно-юридичного дослідження, коли розкриваються техніко-конструктивні та інші техніко-юридичні риси подібності (єдності) і розходження змісту й форми тих чи інших правових інститутів різних правових систем...[41, с. 53]. У контексті нашого дослідження такі можливості зазначеного методу можна обґрунтовано екстраполювати на сферу інформаційної безпеки, тобто для вивчення загальних закономірностей розвитку конкретного правового явища у розумінні оцінки ефективності чинного законодавства у зазначеній сфері, а також його оновлення і удосконалення.

Завдяки можливостям методу державно-правового моделювання ми створимо уявну модель системи захисту сфери інформаційної безпеки з урахуванням нормативно-правового регулювання інших дотичних сфер, насамперед місця цієї складової у загальному контексті провадження заходів щодо забезпечення національної безпеки.

М. М. Шигун зазначає, що моделювання є одним із найбільш вживаних методів пізнання дійсності. Він займає чільне місце серед інших філософських методів наукових досліджень, активно застосовується в усіх видах людської діяльності при її плануванні, веденні, оцінці результатів. Моделювання є основним методом набуття знань в усіх сферах діяльності як при навчанні в освітніх закладах, так і при самопідготовці [42, с. 203].

Використання методу тлумачення правових норм сприятиме більш чіткому розумінню внутрішнього змісту правової бази, якою регулюються правовідносини у сфері інформаційної безпеки, а також прокладе шлях до презентації авторського розуміння системи взаємодії між структурними елементами, які отримали офіційне визначення в джерелах права.

У контексті сказаного доцільно дослухатися думки М. В. Котенка, який зазначає, що «під способом тлумачення в правовій літературі розуміють систему прийомів, засобів та правил здійснення з'ясування змісту та смислу правової норми в результаті їх застосування в інтелектуально-вольовій діяльності суб'єктів права, забезпечують всебічність та комплексність здійснення тлумачення норм права, визначають офіційний або неофіційний характер тлумачення правових норм, зумовлені змістом правової норми та професійним рівнем суб'єктів тлумачення норм права; забезпечують результативність тлумачення правових норм в цілому, а їх застосування відображається в змісті акту тлумачення норм права, що має індивідуально визначений характер» [43, с. 64].

Колектив науковців, серед яких А. Є. Шевченко, А. В., Старостюк, М. В. Кармаліта, вважають, що значну кількість методів, які використовує теорія держави і права в процесі вивчення державно-правових явищ, можна представити у вигляді наступної системи: філософські методи, загальнонаукові методи, приватнонаукові методи та приватноправові [44, с. 6].

Для визначення місця і ролі цілісного юридичного явища «інформаційна безпека» в системі вітчизняного державного будівництва звернемося до можливостей формально-юридичного методу наукового дослідження. Такий підхід сприятиме вивченню взаємозв'язків між внутрішнім змістом правових норм у галузі захисту інформаційного простору держави та зовнішнім їх відображенням у нормативно-правових актах, які встановлюють порядок і межі застосування інструментів превентивної і поточної (перманентної) діяльності управнених органів.

Сутність спеціально-юридичного методу наукового пізнання полягає в описі явищ державно-правової діяльності за допомогою юридичної термінології, висвітленні дійсності соціальних суб'єктів з погляду юридичних моделей поведінки, з позиції законного або протиправного, обов'язкового або можливого

Завдяки застосуванню цього методу отримаємо можливість дослідити неузгодженості у підходах до розуміння внутрішнього змісту механізмів, задіяних у сфері захисту інформаційної безпеки, а також визначити причини, які вносять дисбаланс у наукове розуміння цього юридичного феномену.

У межах нашого наукового доробку виникне питання щодо вивчення особливостей семантико-лексичного змісту задіяного категорійно-понятійного апарату, що уможливиться лише при умові застосування відповідних методологічних інструментів, яким є метод герменевтики. Використання можливостей цього інструмента дослідження сприятиме опрацюванню історико-правових аспектів формування основ розуміння суспільно-економічних підстав запровадження інструментів захисту інформаційного поля з позицій генези цієї правової конструкції. Такий підхід забезпечить можливість встановлення діалектичних зв'язків між первинними проявами усвідомленої необхідності у професійному захисті інформації і нинішнім станом нормативно-правового регулювання інформаційної безпеки.

На думку І. Онищука, герменевтичний підхід у правовій сфері ґрунтується на сукупності принципів і методів тлумачення й інтерпретації юридичних текстів, а останні можуть мати форму як нормативно-правових, так і інших правових документів, а також наукових монографій та інших письмових праць вчених [46, с. 38].

Як зазначає О. М. Балинська, герменевтичний підхід у науковому пізнанні правового моніторингу передбачає «розуміння» його знакового мислення, а також вміння передати це значення у загальнодоступних термінах (пояснювати, тлумачити) [47 с. 47–48].

Здійснений логіко-правовий аналіз місця і ролі інформаційної безпеки в системі цілісного правового явища «національна безпека» виводить нас на рівень теоретико-правового узагальнення, де йдеться про поєднання внутрішніх механізмів її функціонування. За таких умов ми застосуємо синергетичний підхід, який передбачає дослідження процесів самоорганізації та становлення нових упорядкованих елементів і систем різної правової природи, спрямованих на забезпечення конституційного правопорядку в державі.

Висновки до розділу 1

Результати аналітико-практичного дослідження генези цілісного правового феномену «інформаційна безпека» показали, що питання інформаційного здоров'я в комплексному розумінні були на порядку денному майже всіх державних утворень з часів усвідомлення необхідності утримувати від стороннього доступу різнопланові відомості з окремих сфер життєдіяльності суспільства. Найбільш виразною з позицій доступу до ґрунтового юридичного аналізу є сфери безпеки і захисту. Підтвердженням такого висновку є те, що історичні джерела зафіксували факти поширення неправдивої інформації під час

провадження воєнних дій на ранніх етапах державотворення. Тобто у ті далекі часи правителі держав розуміли значення вербальної і невербальної інформації для реалізації своїх планів.

Іншим аспектом функціонування цієї сфери є створення належного морально-психологічного клімату в державах з метою забезпечення дотримання населенням нормативно встановленого порядку в усіх сферах життєдіяльності.

Аксіологічне значення наведеного матеріалу вбачаємо у тому, що з позицій фахового дослідження чітко вимальовується роль неписаного (звичаєвого) права, в якому, як ми переконані, містяться підвалини, що упродовж віків слугувати основою для розвитку інституту інформаційної безпеки у тому вигляді, в якому він функціонує у наші дні.

Поточним підсумком в частині розуміння ролі і значення методологічної складової для результатів нашого дослідження є наступне: з позиції методології юридичної науки парадигма інформаційної безпеки має складну структуру, яку утворюють елементи: методологія правозастосування, Законодавство України, систематика норм права, пояснення правової норми, порядок реалізації положень закону, правова політика держави у сфері безпеки інформації, медіакультура і медіаетика при застосуванні законодавства, яке врегульовує питання повноти доступу громадян до джерел інформації, тактико-стратегічні напрями діяльності суб'єктів забезпечення безпеки при користуванні інформацією, ефективність застосування законодавства, правозастосовна експертиза відомчих нормативно-правових актів, що врегульовують відносини у сфері інформаційної безпеки. На нашу думку, будь який з перелічених структурних елементів цілісного комплексу інформаційної безпеки може слугувати об'єктом окремого наукового дослідження.

Робимо передбачення у тому, що обрані методологічні інструменти для вирішення завдання нашої наукової розвідки сприятимуть фаховому

дослідженню глибинних складових процесів здійснення заходів на напрямках захисту інформаційного простору України. Застосування методологічних прийомів дозволить більш повно і всебічно розкрити роль інституту інформаційної безпеки у розвитку наших уявлень про систему заходів із забезпечення інформаційної гігієни українського медіа, публічно-правового і приватно-правового інтелектуального простору, означити нові аспекти в його структурі та елементному складі.

У подальших розділах ми зосередимося на розробленні шляхів удосконалення механізму впливу інформаційного права та інформаційної безпеки на сферу суспільних відносин для приведення їх до належного нормативного забезпечення та зміцнення правопорядку в державі.

РОЗДІЛ 2

ТЕОРЕТИКО-ПРАВОВЕ ОСМИСЛЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Наукові погляди щодо поняття інформаційної безпеки та її закріплення в нормативно-правових актах

Дослідження проблем у сфері організації та провадження заходів з захисту інформаційного поля України набуває надважливого значення. Як складова національної безпеки держави, сфера інформації справляє потужний вплив на всі сторони функціонування суспільства. Деструктивний вплив на загальну ситуацію в державі, насамперед на сферу захисту інформації, справила повномасштабна російська агресія, яка розпочалася 24 лютого 2022 року. Саме тому інформаційну безпеку держави ми визначаємо як матеріальне підґрунтя морального здоров'я української нації і підсистем життєзабезпечення, яке потребує посиленої уваги та постійного контролю з боку органів, наділених необхідним обсягом повноважень. У зв'язку з цим заходи, спрямовані на підтримання належного рівня інформаційної безпеки, мають тривати безперервно, своєчасно і ефективно реагувати на будь-які прояви недружнього чи зловмисного втручання в моральний клімат чи матеріальну площину вітчизняного державного будівництва.

Водночас, здійснений нами теоретико-правовий аналіз нормативно-правового забезпечення інформаційної безпеки держави показав, що має місце значний розрив між наукою і практикою в процесах організації упереджувальних та превентивних дій на напрямках нейтралізації агресивних проявів у цій сфері.

Оцінюючи стан інформаційної захищеності України за весь період незалежності, необхідно зазначити, що науковці і практики внесли значний

вклад в розбудову інструментів ефективної протидії спробам завдати шкоди суспільству і державі у всіх відомих формах несанкціонованого втручання в економіку, науку, сферу управління, військову справу, суспільну свідомість.

Розглядаючи інформаційну безпеку держави як цілісну систему захисту відомостей незалежно від форми, в якій вони зберігаються, ми вирізняємо основні загрози цієї сфери, серед яких чільне місце займає протиправне оприлюднення, несанкціоноване використання, руйнування, знищення і зміна легітимних записів у державних чи інших реєстрах, які мають у електронній формі, і захищені законом від зловмисного втручання.

Порушення встановленого порядку доступу до інформації порушує принципи її охорони і збереження, тобто конфіденційність, цілісність і доступність з боку осіб, наділених необхідним обсягом повноважень.

Проте, на теперішній час стан захищеності прав і охоронюваних законом інтересів людини, держави і суспільства у сфері інформації України підтверджує висновок про недостатній рівень правового регулювання й забезпечення інформаційної безпеки. Мають місце непоодинокі випадки недотримання чи застосування певних обмежень таких прав без належного правового обґрунтування. Профільні норми, що врегульовують правовідносини у сфері інформаційної безпеки, демонструють суперечності, неузгодженість правових механізмів їх реалізації тощо.

Як видається, така ситуація склалася з причин недостатнього рівня взаємодії і поєднання зусиль теоретиків права і законотворців на напрямках науково-практичного супроводження сфери правового забезпечення інформаційної безпеки та інших системних прорахунків. Саме тому ми утверджуємось в думці про необхідність кардинальної зміни вектора правового впливу на всю галузь інформаційної безпеки як комплексне поняття, яке функціонує завдяки діалектичному зв'язку між наукою і практикою. Досягнення

порозуміння між теоретиками і практиками права у сфері дотримання належного рівня інформаційного захисту держави стане тим чинником, яким буде усунено диспропорційність між науковими розробленнями і формалізацією імперативних складових (прийняття законів), що регулюють правовідносини в означеній сфері.

На нашу думку, саме такий підхід може стати головною ланкою у перманентному перебігу подій, якими прокладається шлях до досягнення достатнього рівня правопорядку в сфері інформаційної безпеки, що відповідає конституційним гарантіям, передбачених статтею 17 Конституції України [6], відповідно до якої найважливішими функціями держави, окрім забезпечення державного суверенітету і національної безпеки, є організація належного рівня інформаційної безпеки.

Вітчизняні науковці не полишали поза увагою проблеми, пов'язані з організацією сфери інформаційної безпеки України. Такі тенденції започатковані в 90-і роки минулого століття, проте мали, в основному, узагальнюючий характер у межах організації заходів у сфері захисту національних інтересів, позбавлення України статусу імпортозалежної держави як в технологічній сфері, так і на інших напрямках міжнародного співробітництва.

Понад три десятиліття Української незалежності характеризуються інтенсивним дослідженням цієї галузі. Науковим розвідкам з даної проблематики притаманна широка осяжність висвітлення питань інформаційної безпеки. Водночас відзначається відсутність єдиної наукової концепції інформаційної безпеки, що говорить про недостатній рівень теоретико-практичної розробленості теми.

Загальна тематика досліджень на напрямку використання інформаційних технологій в науковій літературі представлена технологічними і гуманітарними пропозиціями щодо вирішення проблем на напрямках забезпечення інформаційної безпеки. Поряд з здійсненням технологічних заходів, що

передбачає програмно-технічне супроводження процесів функціонування інформаційної безпеки, гуманітарний підхід визначає інформаційну безпеку як міждисциплінарну складову наукового знання, виокремлюючи юридичні, соціологічні і психологічні аспекти зазначеного соціально-правового явища.

Спрямування державної політики щодо питань, пов'язаних з організацією і проведенням заходів у сфері налагодження ефективного застосування інструментів інформаційної безпеки з позицій економіко-правового змісту, спонукало до всебічного глибинного наукового дослідження особливостей загально-методологічних основ функціонування цілісного процесу інформаційної безпеки. Таке завдання потребувало виведення закономірностей розвитку інформаційної сфери як основи матеріального і морального аспектів життєдіяльності суспільства, розроблення шляхів і способів використання інструментів інформаційної сфери з метою реалізації основних соціально-політичних завдань України, серед яких європейський вектор розвитку та набуття членства в НАТО. При цьому головним елементом парадигми інформаційної безпеки, на наше переконання, виступає інформаційний гуманізм, що покликаний гарантувати повномірну захищеність об'єктів інтелектуального надбання.

Слід зауважити, що поняття «інформаційна безпека» широко використовується в наукових публікаціях, навчальній і публіцистичній літературі, в нормативних документах різного рівня.

Водночас, вектор нашого дослідження вимагає здійснити авторський теоретико-правовий аналіз оприлюдненого наукового доробку на напрямку визначення основних якісних елементів, змісту і сутності ємнісного міждисциплінарного поняття, яким є інформаційна безпека держави. У контексті вищесказаного наводимо наукові погляди та підходи до тлумачення феномену «інформаційна безпека». При цьому не будемо вдаватися до дослідження

етимології складових цього поняття, оскільки воно містить загальновідомі категорії, які не потребують приведення до однакового розуміння. У поточному підсумку до цієї частини підрозділу подаємо авторське визначення цього поняття.

Логіко-правовий аналіз опрацьованого масиву інформації показав, що вихідне поняття «інформаційна безпека» отримало визначення на підґрунті тих завдань, які покладав перед собою дослідник з огляду на галузеве спрямування дослідження. Такі підходи видаються нам надто дискусивними, оскільки не відображають внутрішню природу цього ємнісного соціально-економічного явища, яке містить у собі економічні, соціальні та правові складові. Тобто при визначенні дефініції цього поняття з вузько дисциплінарних позицій відбувається невинуватене редуціювання його міжгалузевої природи, залишаються поза увагою ті якісні характеристики, завдяки яким воно отримало значне поширення в різних сферах суспільного життя.

У контексті зазначеного вище наводимо судження Г. М. Сашука, який визначає інформаційну безпеку країни як «стан захищеності життєво важливих інтересів особистості, суспільства та держави від зовнішніх і внутрішніх загроз» [48]. Свої висновки науковець обґрунтовує особливостями сучасного стану правового регулювання відносин в Україні, робить акцент на недостатній визначеності і не сформованості системи цінностей та інтересів суспільства, вказує на те, що існує низка невідповідностей між бажаннями та інтересами різних соціальних груп і професійних спільнот. Така ситуація, на думку науковця, призводить до політичної і соціальної нестабільності. Саме з причини відсутності порозуміння і збалансованості поглядів у суспільстві щодо національних пріоритетів, цілей та інтересів, не забезпечується досягнення належного рівня узгодженості в діях між зацікавленими державними органами

щодо організації та підвищення стану резистентності національної та інформаційної безпеки.

Наведене утверджує нас в думці про полігалузеву природу поняття «інформаційна безпека», оскільки воно, як було сказано вище, покладає завдання щодо нормативного регулювання всієї системи суспільних відносин. Своєю чергою це означає, що базовим елементом цієї системи виступають загальнообов'язкові правила, встановлені нормативно-правовими актами.

Компаративістський метод наукового дослідження відсилає нас до здійснення теоретико-правового аналізу інших підходів до визначення поняття «інформаційна безпека» і ролі цього інституту в житті суспільства.

Першим практичним кроком до розкриття завдань цього підрозділу розглядаємо необхідність пояснення соціально-правової природи поняття «інформаційна безпека» крізь призму суспільних відносин, всередині яких функціонують інструменти захисту інформаційного середовища. На думку окремих науковців таким середовищем є суспільні відносини у різних сферах.

Так, В. С. Цимбалюк та А. В. Бабінська вважають, що «під інформаційною безпекою України слід розуміти стан захищеності її національних інтересів в інформаційній сфері, що визначаються сукупністю збалансованих інтересів особи, суспільства та держави [49].

Співзвучні судження знаходимо у науковому доробку О. А. Ніщименко, який розуміє це поняття як «стан захищеності національних інтересів України в інформаційній сфері, що складаються з сукупності збалансованих інтересів особи, суспільства та держави від внутрішніх і зовнішніх загроз, що відповідає принципу забезпечення національної безпеки в інформаційній сфері» [50, с.19].

В цілому, такі визначення мають право на життя, оскільки охоплюють всеузагальнюючі ознаки ємнісного явища «інформаційна безпека» як

інструменту впорядкування суспільних відносин на всіх рівнях, у тому числі й захисту від стороннього протиправного впливу.

Л. О. Кочубей [51, с. 221-222] при дефініції інформаційної безпеки, окрім загальних елементів, які ми зустрічаємо у визначеннях цитованих вище науковців, звертається до морально-психологічних аспектів, а саме «...деструктивних думок і дій, що призводять до негативних відхилень на шляху стійкого прогресивного розвитку названих суб'єктів».

Оцінюючи правове і логічне наповнення наведеного наукового розуміння сутності поняття «інформаційна безпека», вважаємо доцільним внести авторське розуміння вкладених термінів, що його пояснюють. На наш погляд, аналізована дефініція не в повній мірі розкриває сутність поняття «інформаційна безпека», оскільки використані базові елементи (деструктивні думки, негативні відхилення), що відтворюють внутрішню будову цього економіко-правового явища, мають превалюючий літературно-публіцистичний зміст, що не може позиціонуватися як достатнє пояснення складних економіко-правових явищ.

Критичне ставлення справляє ототожнення словосполучень «життєво важливі інтереси» з «інформаційною озброєністю держави, суспільства, особистості». Порівнювані поєднання вживаних слів відзначаються надто широким змістом і лише віддалено відображають дотичні поняття, які можуть застосовуватися як допоміжні, уточнююче-описові категорії.

Дещо інші підходи до оцінки змісту і ролі інформаційної безпеки в структурі національної безпеки держави зустрічаються в науковому доробку С. С. Єсімова [52, с. 75]. Характеризуючи інститут інформаційної безпеки в системі інформаційного права, науковець включає до сфери його впливу всі сфери життя суспільства, які регулюються організаційними, правовими, технічними інструментами, що відповідають за забезпечення інформаційно-комунікаційного комплексу держави. Говориться про систему інформаційних

ресурсів, інформаційно-комунікаційну інфраструктуру, ринок інформаційної продукції та послуг, систему масової освіти, підготовку кадрів для цієї сфери тощо.

Позитивно оцінюючи наукові здобутки С. С. Єсімова, вважаємо за доцільне висловити авторське критичне ставлення до оприлюдненого розуміння поняття «інформаційна безпека». Перше, що знижує враження від аналізованого визначення, є надмірне нагромадження структурних елементів сфери суспільного життя в одному узагальненні. Такий підхід надто розмиває межі цілісного інформаційного середовища, невиправдано поділяючи на окремі складові. Більше того, застосовуючи спосіб подріблення цілісного інституту «інформаційна безпека», науковець фактично покладає себе в залежність соціально-філософських понять, перелік яких є невичерпним.

На нашу думку, презентоване С. С. Єсімовим визначення поняття «інформаційна безпека» не повністю відповідає основним критеріям, якими можна пояснити поняття, тобто лаконічності, дотримання логічного змісту, послідовності обґрунтування і вирізнення відмінних ознак тощо.

Для надання нашій розвідці необхідного рівня науковості звертаємося до інших, представлених у значній кількості визначень поняття «інформаційна безпека».

Інформаційна безпека, на думку Б. О. Кормича, «виступає як захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування і розвитку людини, всього суспільства та держави [53, с. 89].

Колектив науковців (І. Громико і Т. Саханчук) висловлюються про те, що «інформаційна безпека України – це захищеність державних інтересів, за якої забезпечується запобігання, виявлення і нейтралізація внутрішніх і зовнішніх інформаційних загроз, збереження інформаційного суверенітету держави і

безпечний розвиток міжнародного інформаційного співробітництва» [54, с. 130 - 134].

В. С. Цимбалюк розуміє інформаційну безпеку «як стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації» [55, с. 204].

На думку Р. А. Калюжного, інформаційна безпека – це вид соціальних інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності» [56, с. 234-244].

С. Ф. Гуцу вважає, що інформаційна безпека – «це стан захищеності потреб в інформації особи, суспільства й держави, при якому забезпечується їхнє існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз» [57, с. 35].

А. О. Нашинець-Наумова висловлюється про те, що «інформаційну безпеку України можна інтерпретувати як сукупність життєво важливих умов функціонування суб'єктів (людини, суспільства, держави) в інформаційній сфері та суб'єктивних (правових політичних, інформаційних наукових, оперативно-розшукових) можливостей їх усвідомлення й контролю» [58, с. 4,].

Проте найбільш ємнішим і таким, що, на нашу думку, достатньою мірою відповідає вимогам до пояснення процесів і явищ, вважаємо визначення поняття «інформаційна безпека» від Л. С. Харченко: «інформаційна безпека – це складова національної безпеки, процес управління загрозами і небезпеками державними і недержавними інституціями, окремими громадянами, за якого забезпечується інформаційний суверенітет України» [59, с. 65].

Окремо слід звернути увагу на судження Н. С. Мороз [60, с. 136], яка пояснює явище інформаційної безпеки крізь призму діалектичного розвитку, застосовуючи категорію «динамічність». Цю характерну особливість науковець

розглядає як важливу ознаку, оскільки вона постійно перебуває у динаміці, розвивається, а отже й постійно трансформується для потреб суб'єктів інформаційної сфери.

Для більш осяжного розуміння поняття «інформаційна безпека» звертаємо увагу на наукові погляди О. Г. Яреми та С. С. Єсімова. На думку науковців, інформаційна безпека має складну структуру і саме через це «структурна складність пояснюється предметною безліччю правовідносин, що виникають під час забезпечення захищеності інтересів особистості, суспільства та держави в інформаційній сфері» [61, с. 247-248].

Представники сучасної правової науки, у тому числі О. Кісілевич-Чорнойван, зауважують, що «інформаційна безпека – це складова частина національної безпеки, яка, по-перше, відображає стан захищеності життєво важливих інтересів особи, суспільства і держави, за якого зводиться до мінімуму нанесення шкоди через неповність, несвоєчасність та недостовірність інформації або негативного інформаційного впливу через негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації», і, по-друге, «стан захищеності інформаційного середовища/простору загалом, який забезпечує його формування, використання і розвиток і інтересах громадян, організацій, держави» [62, с. 13].

Н. С. Грабар [63] інформаційну безпеку розглядає крізь призму її захищеності від несанкціонованого втручання, знищення і перетворення, а також створення умов, за яких буде досягнуто достатнього рівня захищеності інформаційних ресурсів, що виключає порушення їх нормального функціонування.

О. П. Дзьобань, О. Г. Данільян, та М. І. Панов висловлюють думку про те, що «інформаційна безпека – це безпека об'єкта від інформаційних загроз або

негативних впливів, пов'язаних з інформацією, на нерозголошення даних про той чи інший об'єкт, що є державною таємницею» [64, с. 165].

У зв'язку з наведеним вище зауважимо, що більшість з представлених дефініцій поняття «інформаційна безпека» певним чином виокремлюють складові механізму цього юридичного явища, застосовуючи такі характеристики, як «здатність захистити», «стан захищеності» тощо, тобто акцентують увагу на потенційній здатності управнених суб'єктів на забезпечення достатньо захищеного режиму для передавання і обміну інформацією.

Пізнавальний досвід вивчення правової реальності засвідчує про те, що для розвитку сфери інформаційної безпеки як частини суспільного життя важливого значення набувають не лише результати наукових розвідок, а й організаційні напрямки, які заохочують до пошуків найбільш оптимальних шляхів для їх досягнення.

Грунтуючись на проаналізованих наукових матеріалах, наводимо авторське визначення поняття «інформаційна безпека», яку розуміємо як діалектичну єдність всіх складових суспільного життя, якими забезпечується правомірне володіння, користування і поширення відомостей з різним рівнем доступу.

Не викликає суперечливих суджень те, що належно організована інформаційна безпека обумовлює певний рівень захисту особи, суспільства і держави від деструктивної, ворожої і шкідливої інформації, протиправного контенту, а також здійснює протекціоністську функцію для убезпечення учасників інформаційної сфери від негативного впливу на їх свідомість, що перешкоджає природному розвитку особи, становить загрозу суспільству і державі.

Як вбачається з основних завдань на напрямках дотримання інформаційного «здоров'я» держави, саме стан функціонування системи захисту моральної і матеріальної складових сучасного суспільства здатен забезпечити

належний рівень інформування та виховання особи, розбудови суспільства та держави, достатню захищеність інформаційної інфраструктури, включаючи ІТ-сферу, серверне обладнання та відомості, що внесені до державних реєстрів.

У контексті сказаного доцільно згадати висновки Р. І. Проданюка, який розуміє належний рівень інформаційної безпеки як діяльність «однієї із соціальних інституцій контролю за підтриманням інформаційної рівноваги, функція якої полягає в підтримання екологічності інформаційного простору» [65, с. 87].

Наведене вище покладає перед управлінськими органами завдання щодо практичного застосування норм і правил у сфері інформаційної гігієни, які виступають обов'язковими для виконання усіма членами суспільства. За таких обставин вирізняємо проблемну ситуацію у сфері забезпечення інформаційної безпеки. Говориться про стан нормативно-правового регулювання механізмів функціонування системи інформаційної безпеки.

О. Д. Довгань і Т. Ю. Ткачук вважають, що ефективності інформаційного законодавства в цілому серйозно шкодить «відсутність у нормативно-правових актах з питань забезпечення інформаційної безпеки єдиних для всіх джерел правового регулювання відповідних засадничих нормативних умов» [66, с. 86–87]. Адже інформаційна безпека держави «є інтегральною характеристикою стану економічної системи, що передбачає характеристику стану низки підсистем – взаємопов'язаних структурних складових: макроекономічну, інвестиційну, інноваційну, фінансову, соціальну, зовнішньоторговельну, енергетичну, продовольчу, демографічну безпеку. Водночас інформаційна безпека є складовою системи більш високого рівня – національної безпеки.

Питання природи і змісту інформаційної безпеки автор розкриває у статті «Сутність інформаційної безпеки в умовах розвитку сучасного суспільства», в якій зазначає, що питання сутності інформаційної безпеки в умовах розвитку

сучасного суспільства є одним із головних для України, яке тісно пов'язане з вирішенням таких питань, як захист суверенітету і територіальної цілісності країни, забезпеченням її економічної безпеки... [67].

Поряд із юридичними конструкціями, правилами та прийомами викладення положень законодавчих та інших нормативно-правових актів одним із основних засобів юридичної техніки розглядаємо відповідну термінологію (категоріально-понятійний апарат).

Полісистемність і різновекторність у підходах до розуміння поняття «інформаційна безпека» виступають підґрунтям для дефініції і пояснення суто інформаційно-безпекових понять, що є вкрай необхідним для ефективного провадження наукової і нормативно-законотворачої діяльності. У цьому зв'язку необхідно вказати на відсутність як однотипного підходу до розуміння системоутворюючих категорій, та і відсутність законодавчого визначення ключових понять сфери інформаційної безпеки.

С. М. Луценко пропонує інформаційне забезпечення – це комплексний, цілеспрямований процес доведення інформаційних матеріалів, створених у сфері документального, фактографічного і концептуального обслуговування, до безпосередніх виконавців розробки з урахуванням їх інформаційних потреб і наявних інформаційних ресурсів (методів, засобів і т.д.) [68, с. 41–45].

Д. О. Хом'яков [69, с. 183], розглядаючи стан нормативно-правового регулювання сфери інформаційної безпеки, вказує на необхідність створення відповідної нормативно-правової бази, яка набуває особливого значення при формуванні сучасної та ефективної системи захисту інформаційної безпеки, оскільки без належного правового підґрунтя неможливо розробити єдину концепцію національного масштабу, а отже й ефективно здійснювати заходи із забезпечення національної безпеки.

Прикладом такої ситуації є те, що поняття «безпека інформації» не набуло формального визначення, хоча вживається в деяких законодавчих актах (Закон України «Про основи національної безпеки»). Даним Законом згадане поняття визначається як базове у підходах до розуміння системної сутності безпеки інформації, яка, не маючи офіційного визначення, позиціонується як невід’ємна складова національної безпеки України.

У статті «Тенденції наукових поглядів у сфері нормативно-правового забезпечення інформаційної безпеки України» автор зазначає, що «нормативно-правове забезпечення є більш широким поняттям порівняно з нормативно-правовим регулюванням...» оскільки нормативно-правове регулювання може позиціонуватись як складова забезпечення інформаційної безпеки [70, с. 26].

Наукове дослідження генези інформаційної безпеки як інституту права показало, що поняття «інформаційна безпека» не набуло достатнього рівня уваги з боку законотворців, оскільки нині нечинним Законом України «Про основи національної безпеки України» від 2003 р. даний термін не був офіційно сформульований. Водночас, це поняття побіжно згадується у загальному тлумаченні поняття «національна безпека», яка розглядається як «захищеність життєво важливих інтересів людини і громадянина, суспільства і держави..., забезпечення інформаційної безпеки...» Як бачимо, в коментованому Законі поняття «інформаційна безпека України» не використовується, а законодавець застосовує термін «національна безпека України в інформаційній сфері».

На наш погляд, поняття «інформаційна безпека» і «національна безпека України в інформаційній сфері» можуть сприйматися як синоніми, оскільки відображають однопорядкові завдання на напрямку реалізації завдань із захисту України в найширшому розумінні цього поняття.

Законами України «Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки» [71] та «Про електронні комунікації» [72] подаються різні за змістом визначення поняття «інформаційна безпека».

У розумінні положень Закону України «Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки» інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [71].

Відповідно до положень Закону України «Про електронні комунікації» інформаційна безпека розглядається крізь призму захисту цілісності та можливості протидіяти протиправному використанню (безпека мереж і послуг – здатність електронних комунікаційних мереж і послуг протистояти діям, що становлять загрозу доступності, цілісності чи конфіденційності таких мереж і послуг, а також даних, що зберігаються, передаються чи обробляються, та пов'язаних із ними послуг, що надаються або доступ до яких здійснюється через електронні комунікаційні мережі чи послуги) [72].

Різноманітність законодавця у підходах до визначення поняття «інформаційна безпека» створює певні складнощі, насамперед для законотворчої діяльності в інформаційній галузі, а також на напрямках застосування встановлених правил для користування інформацією та її носіями.

Водночас, з урахуванням реалій російської агресії проти України перед країною покладається завдання щодо прийняття нових, удосконалення чинних нормативно-правових актів, що передбачено положеннями для України як кандидата на вступ до Європейського Союзу.

Аналізуючи стан дотримання нормативно-правового регулювання інформаційної безпеки в Україні, Ю. Є. Максименко зазначає, що «інформаційну безпеку України становлять три структурні елементи: інформаційна безпека у сфері прав і свобод людини і громадянина; інформаційно-психологічна безпека; інформаційно-технічна безпека [73, с. 117].

Вивчення окремих документів, якими регулюються відносини у сфері інформаційної безпеки, дає підстави для висновку про необхідність удосконалення інформаційного законодавства. Українські науковці активно включилися в цей процес, про свідчать численні наукові розвідки з наведеної проблематики.

Наукові розвідки на напрямках фахового аналізу сфери інформаційної безпеки відображені у доробку вітчизняних вчених, серед яких: О. О. Золотар, В. А. Ліпкан, А. Ю. Нашинець-Наумова, О. О. Тихомиров, О. А. Заярний, О. В. Олійник, С. О. Лисенко та інші.

Так, В. А. Ліпкан висловлюється про те, що «інформаційна безпека України є органічною складовою національної безпеки, відтак її розгляд є необхідним для формування базових знань та уявлень про національну безпеку [74, с. 194].

Ситуація, пов'язана із заходами на напрямках забезпечення інформаційної безпеки в структурі національної безпеки, фактично перебуває у стані перманентного трансформування. Ми у своїх висновках виходимо з того, що інформаційна безпека досягається провадженням виваженої і раціональної державно-правової політики у сфері національної безпеки, що є проявом функціонування поліаспектної системи державних і економічних заходів, насамперед щодо перманентного забезпечення превентивно-профілактичних впливів на протиправне поширення деструктивних відомостей в економічній, соціальній, оборонній та інших сферах суспільного життя.

О. В. Олійник [75 с.132] вважає, що умовами розвитку системи нормативно-правового регулювання відносин у сфері інформаційної безпеки виступають своєчасні та впорядковані дії законотворців, спрямовані на постійне вдосконалення технологічних і правових механізмів протидії загрозам в інформаційній сфері.

О. О. Золотар [76, с. 178–179] зазначає, що правове регулювання може розглядатись лише як складова забезпечення інформаційної безпеки з тієї причини, що сама інформаційна безпека є природною і невід’ємною властивістю її об’єктів.

С. О. Лисенко вважає, що систематизація норм інформаційної безпеки повинна відбуватись згідно з переліченими конституційними засадами, повністю позбавляючись складних процедур, зайвих перепон та найбільш узгодженою системою норм [77, с. 160].

На сьогодні одним із найважливіших напрямів розвитку стратегії нормативно-правового забезпечення інформаційної сфери України виступає завдання щодо її приведення до найвищих стандартів управління та відповідності новітнім викликам для інформаційної безпеки в умовах російської агресії.

Аналіз чинної законодавчої бази у сфері інформаційної безпеки України показав, що регулювання цього елементу національної безпеки відбувається на нормативному підґрунті, визначеному Конституцією України і профільними Законами України: «Про інформацію», «Про науково-технічну інформацію», «Про Національну програму інформатизації», «Про Концепцію Національної програми інформатизації», «Про поштовий зв’язок» тощо.

Нормативне наповнення згаданих законів спрямоване на регулювання конкретних видів правовідносин, а саме дотримання належного рівня інформаційної безпеки, протидії протиправному використанню баз даних, захист

відомостей, що віднесені до державної таємниці, охорона інформаційних ресурсів, конфіденційної та обмеженої у сторонньому доступі інформації. Все зазначене обрамлюється положеннями Доктрини безпеки особистості, держави, суспільства тощо.

Теоретико-правовий аналіз чинного законодавства України у сфері безпеки інформації засвідчує кількісну перевагу тих нормативно-правових актів, якими регулюється інформаційно-технічний сегмент у складі цілісного поняття «інформаційна безпека». Дещо менш активно представлено приватно-правові компоненти, а саме інформаційно-психологічний та безпека інформації у відношенні до прав і свобод громадян. На нашу думку, такий дисбаланс обумовлений пріоритетним ставленням до технологічних інструментів, якими забезпечується зберігання та передавання інформації, а також своєчасна протидія протиправним проявам на напрямках використання і поширення відомостей певної категорії.

Оновлення системи інформаційної безпеки та підтримання працездатного стану сфери комунікації, упевненого економічного поступу уможливлюються за умови впровадження новітніх інструментів правового регулювання нормативної бази цієї складової національної безпеки. Такі події мають об'єктивний характер, оскільки економіко-політичні процеси, що відбуваються в Україні, сягають усіх сфер життя суспільства, насамперед інформаційної безпеки як гаранта об'єктивного і стабільного середовища передавання даних як всередині держави, так і на міжнародному рівні.

Такі трансформаційні процеси мають відбуватись з урахуванням конкретної суспільно-політичної ситуації, що має місце в глобальному і державному масштабах, забезпечувати здатність технологічних інструментів захисту інформації ефективно протистояти будь-яким джерелам загроз, найперше з боку країни-агресора.

Саме з цих причин говоримо про необхідність розроблення та впровадження нових стандартів нормативно-правового регулювання сфери інформаційної безпеки, в основу яких мають бути покладені найбільш ефективні зразки інструментів захисту інформаційного простору України. Як було вже сказано дещо раніше, така діяльність має провадитись з урахуванням нинішніх інформаційних загроз, які набувають все більш вишуканих і завуальованих форм руйнації морального і психологічного клімату в державі.

Забезпечуючи суверенітет і територіальну цілісність України, з огляду на реалізацію конституційних положень щодо незмінності державного курсу на злиття з Європейським Союзом, необхідно в подальшому розвивати інструменти захисту інформаційного середовища держави у тісній взаємодії з дружніми країнами при якісній і своєчасній протидії деструктивному впливу з боку внутрішніх джерел загроз, а також нейтралізації зовнішніх ворожих впливів.

На наш погляд, одним з основних недоліків нормативно-правового забезпечення інформаційної безпеки залишається проблема уніфікації законодавчого регулювання цієї сфери. Так, будучи поміщеними у різні нормативно-правові акти, однотипні поняття отримують неоднакове визначення, що ускладнює системну взаємодію між управненими органами на напрямках їх застосування.

Водночас необхідно зазначити, що значна частина нормативної бази у сфері інформаційної безпеки відзначається декларативністю, що значно ускладнює їх практичне застосування в конкретних ситуаціях. Такий висновок робимо з опрацьованого масиву документів різної юридичної сили, якими врегульовуються відносини у сфері інформаційної безпеки.

На наше переконання, визначальними принципами на напрямках розвитку системи інформаційної безпеки України мають стати:

- доступність, прозорість і зрозумілість нормативної бази з регулювання цього типу правовідносин;
- ефективність і надійність правових інструментів захисту оспорюваного, порушеного чи невизнаного права на володіння інформацією чи розпоряджання нею;
- підтримка державою громадянських інститутів і суспільних утворень з метою залучення якнайширшого кола осіб до участі в процесах державотворення на напрямках посилення інформаційної безпеки України;
- створення умов для реальної участі суб'єктів інформаційного права в процесах нормотворення шляхом законодавчого закріплення такої можливості;
- забезпечення більш високої прозорості і відкритості правових механізмів, які беруть участь у реалізації прав учасників інформаційної сфери незалежно від форми власності;
- підвищення ефективності контролю з боку громадянського суспільства за процесами внесення змін до інформаційного законодавства, а також результатами застосування правових механізмів з убезпечення інформаційної сфери.

Отже, якщо розглядати правові основи нормативно-правового забезпечення інформаційної безпеки в нашій країні, то до пріоритетних напрямів можна, на наш погляд, віднести: створення якісної нормативно-правової бази; провадження системного моніторингу стану інформаційної безпеки України; запровадження дозвільних процедур у сфері надання інформаційних послуг як інструменту контролю за дотриманням правил інформаційної гігієни; адаптація до світових стандартів захисту інформаційної сфери, покращання та вдосконалення інформаційної інфраструктури з урахуванням джерел загроз інформаційній безпеці; запровадження освітніх програм у закладах освіти для

виховання і навчання основам користування інформацією у відповідності до реального стану справ у сфері інформаційної безпеки України.

Через збільшення недружнього і ворожого впливу на інформаційне середовище України, що включає в себе розпорошування я і нівелювання вітчизняних моральних цінностей, національної культури та української ідентичності, необхідно посилити роботу над створенням конкурентоздатного вітчизняного медіа контенту. Залишаються актуальними завдання щодо підвищення резистентності інформаційних та комп'ютерних ресурсів, задіяних у системі державного управління, фінансовій сфері, банківському секторі, енергетичній, транспортній галузях, а також інших внутрішніх та міжнародних контрагентів.

Розв'язана країною-агресором повномасштабна війна справила деструктивний вплив на сферу інформаційної безпеки, де проявились слабкі місця і справжні прогалини у механізмах правового регулювання відносин у сфері інформаційної безпеки. Все це зумовлює необхідність якнайшвидшого перепрофілювання управнених державних структур на встановлення надійного заслону проникненню в медіапростір України ворожого інформконтенту, а також прискорює виконання «домашнього завдання» для України як майбутнього члена Європейського Союзу та Організації Північно-атлантичного договору (НАТО).

Ефективна реалізація стратегічних пріоритетів, основних засад і завдань з боку держави у галузі інформаційної безпеки вимагає оновлення нормативно-правових механізмів, удосконалення організаційних підходів до управління сферою інформаційної безпеки, її належного кадрового забезпечення на умовах залучення до роботи високоінтелектуальних, патріотично налаштованих і грамотних спеціалістів. Таке завдання уможливорюється виконанням комплексу законодавчих і практичних заходів, спрямованих на усунення суперечностей,

неврегульованості, конфлікту інтересів між суб'єктами-учасниками сфери передавання і володіння інформаційними ресурсами, а також за умови подолання корупційних проявів на всіх рівнях державного управління.

Тому, при удосконаленні стратегії національної безпеки, можливого розробленні доктрини з питань комплексного забезпечення всіх складових цього юридичного явища, важливим елементом являється інформаційна безпека держави, яка є інструментом захисту національних інтересів в інформаційній сфері.

Отже, інформаційна безпека – це такий стан захищеності правовими інструментами інформаційного середовища, при якому мінімізуються будь які прояви протиправного заволодіння, використання чи розпоряджання інформацією з порушеннями встановленого порядку.

2.2 Аксіологічні аспекти та роль держави у забезпеченні інформаційної безпеки

Враховуючи процеси демократичного розвитку і поширення на значну частину суспільних відносин електронних видів комунікації (діджиталізації), наша держава пройшла низку стадій, етапів, а також рівнів, завдяки логіко-юридичному аналізу яких можна прослідкувати процеси становлення системи захисту інформаційної складової у загальній структурі національної безпеки в Україні. Не дивлячись на встановлені розмежування в розрізі наділення компетенцією управлінських органів у сфері інформаційної безпеки, мають місце непоодинокі факти конфлікту інтересів. Така ситуація стала можливою з причини відсутності чітких службових інструкцій, якими мають бути роз'яснені межі контролюючого і управлінського впливів, оскільки відповідними

законодавчими і підзаконними нормативно-правовими актами не деталізуються механізми дозволеного втручання у сферу інформаційної безпеки.

Водночас, комплексний підхід до дослідження інституту інформаційної безпеки вимагає всебічного опрацювання його структурних елементів як цілісного правового явища. Межові орієнтири такої наукової розвідки практично неможливо передбачити з огляду на поліаспектний характер інструментального впливу його складових на суспільне середовище як у самій державі, так і при зносинах з іншими країнами.

Така постановка питання розкриває нові аспекти у підходах до оцінки ролі і значення інформаційної безпеки як одного із стабілізаторів у сфері дотримання належного рівня національної безпеки. При цьому особливу увагу потрібно зосередити на специфічній складовій цього процесу, що пов'язана зі збереженням, утворенням, поширенням ціннісних результатів життєдіяльності суспільства. Говоримо про аксіологічну функцію інформаційної безпеки як інструмента філософсько-правового характеру, що регулює ці питання, і охоплює найширше коло матеріальних і нематеріальних правовідносин.

Аксіологія (від давньогрец. *ἀξία* – цінність – теорія цінностей) – теорія цінностей, ...досліджує системи або множини взаємопов'язаних цінностей [78].

К. В. Горобець зазначає, що «останнім часом у зв'язку з нарощуванням практичного потенціалу аксіологічних досліджень під цінностями розуміють не лише категорії належного, а й значущості, корисності для людини» [79, с. 83].

У статті «Аксіологічний підхід у кримінальному праві: зміст та значення» науковець дійшов висновку про те, що у кримінальному праві застосування аксіологічного підходу, безперечно, повинно базуватися на універсальних методологічних засадах, що вироблені філософією, однак водночас ці засади підлягають поглибленню, уточненню, адаптації та специфікації з урахуванням предмета в метода кримінального права, його завдань і функцій [80, с. 224].

Коментуючи наведене вище судження необхідно зазначити, що кримінальне право слугує тим бар'єром, який найбільш ефективно відпрацьовує на всіх напрямках збереження сфери національної безпеки, до якої структурно належить інформаційна безпека. На нашу думку, саме інструменти кримінального права і кримінального процесуального права є найбільш дієвими на напрямках упередження і нейтралізації протиправних посягань на встановлений інформаційний правовий режим в Україні, оскільки в них закладено найвищу ступінь державного примушування до виконання встановленого законом порядку.

С. А. Калінін, досліджуючи значення цінностей матеріального і нематеріального характеру, вказує: «Як учення про цінності, взяті у контексті світоглядного розуміння людини, аксіологія дозволяє характеризувати ієрархію цінностей, що склалися стосовно конкретного світогляду й антропології, описувати їх зміст стосовно конкретної цивілізації, взятої у певному історичному часі» [81, с. 270].

В. М. Брижко, вивчаючи систему цінностей у сфері інформаційного права, зазначає, що «у загальному аспекті аксіологія у юридичній сфері передбачає вивчення реалій і цінностей у життєдіяльності людини, суспільства і держави з метою раціонального впорядкування суспільних відносин на основі легалізації положень щодо стосунків, виконання яких забезпечується нормами законів та підзаконних нормативних актів. Основними поняттями у юридичній аксіології є «інформаційна культура» та «правова культура»...[82, с. 28].

Термін «інформаційна культура» для науковця позиціонується як «частина загальної культури і як один з найважливіших аспектів культурних досягнень взагалі. Вона має такі загальні риси як нерозривний зв'язок людини з природою і суспільством та можливості щодо її інформаційно-творчої діяльності» »...[82, с. 29].

Правова культура, за визначенням В. М. Брижка, - це система цінностей правових традицій і правових ідей, прийнятих членами певної спільності (державної, релігійної, етнічної), які використовують її для забезпечення упорядкування суспільних відносин. Правова культура людини визначається в умінні і навиках користуватися правом та законом з орієнтацією життєдіяльності на приписи світових правових стандартів, що визначають досягнення цивілізації у проблемах цінностей [82, с. 32].

Є. М. Мануйлов та О. П. Дзьобань вказують, що «на даному етапі розвитку людства соціальний суб'єкт вступив у нову фазу, де основним предметом праці є інформація і знання, знаряддям праці – інформаційні технології та засоби комунікації, а саме суспільство поступово стає інформаційним. Звернення суспільної свідомості до проблем інформаційної безпеки пов'язано з новими особливостями життя у сучасному суспільстві» [83, с. 75].

Суть проблем, пов'язаних із забезпеченням інформаційної безпеки людини й суспільства, полягає у тому, що інформаційна сфера щодня розширюється дедалі більше і більше, як в обсязі, так і в сучасних засобах обробки інформації [84].

Оцінюючи значення інформації для визначення рівня «інформаційного здоров'я» суспільства, треба мати на увазі, що наявність значного чи надмірного обсягу різнопланових відомостей не свідчить про їхню користь і позитивний вплив на об'єкти (людей). У такому разі вирішальне значення має наповнення (контент) інформаційного середовища на напрямках утвердження загальнолюдських моральних цінностей і дотримання належного рівня національної безпеки.

Б. Мільтон зазначає, що «інформації не може бути занадто багато, просто існує величезна кількість непотрібної інформації, яка змушує суб'єкта знати менше, аніж він знав до її отримання. Інформація – всього лише сировина, а

рішення приймаються на основі знань, мудрості, інтуїції й розуміння, тобто продуктів її переробки» [85].

Структура системи державного управління вибудована в такий спосіб, що саме на державу покладається обов'язок забезпечити життєздатні умови для народу країни, адже згідно з положеннями статті 3 Конституції України людина визнається найвищою соціальною цінністю. Тому, окрім обов'язку зберегти життя і здоров'я людини, держава несе повну відповідальність за стан справ в усіх сферах суспільного буття, якість наданих послуг та збереження допустимого рівня інформування населення.

В умовах активізації реформ в Україні відзначаються певні труднощі щодо реалізації функцій держави в окремих сферах життя суспільства. Сфера національної безпеки не є винятком із загального стану речей, інформаційних та інших відносин. Разом з тим, процеси правотворення і державного будівництва понад десятиліття потребують залучення до них науковців, проаналізувати доробок минувшини і у такий спосіб привести сферу інформаційної безпеки до належного рівня упорядкованості і готовності протидіяти зовнішнім і внутрішнім джерелам загроз.

У контексті цього підрозділу дослідження важливо з'ясувати теоретико-правовий зміст категорії «забезпечення інформаційної безпеки» та проаналізувати підходи українського законодавця до процесів приведення інформаційного середовища до достатнього рівня захисту від протиправного втручання. Це дасть змогу комплексно та ґрунтовно проаналізувати структуру механізму на напрямках забезпечення інформаційної безпеки держави, виявити причини його недостатньої дієвості загалом та окремих його елементів у процесуальній діяльності щодо охорони і захисту сфери національної безпеки.

Здійснений авторський теоретико-правовий аналіз наукового доробку з цієї проблематики показав, що науковцями пропонуються різні, більшою мірою

галузеві підходи до розуміння і дефініції поняття «забезпечення інформаційної безпеки». На наш погляд, саме зазначена обставина є причиною фахових дискусій щодо структури та обсягу елементів цього юридичного феномену.

Мультикомпонентність досліджуваного поняття зумовлює необхідність розпочати аналіз з ключового елементу (забезпечення), оскільки саме цим поняттям охоплюється комплекс заходів, що вживаються на виконання завдань інформаційної безпеки.

У Словнику української мови термін «забезпечення» пояснюють як створення надійних умов для здійснення чого-небудь, гарантування чогось; - захист, охорона кого, що-небудь від небезпеки [1].

Якщо проаналізувати юридичні й економічні категорії, які містять лексему «забезпечення», то можна відзначити окремі відмінності при її трактуванні. З позиції права, це – діалектичне поєднання заходів і засобів, створення умов для ефективного функціонування чогось та/або нормального перебігу процесу. Для потреб економіки, це – діяльність зі створення засобів та застосування їх у логічній послідовності і певному порядку. У науковій літературі, зазвичай, за основу беруть широке тлумачення поняття «забезпечення», що поєднує всі зазначені вище аспекти, однак акцентують увагу на його діяльнісних складових.

В. А. Предборський вважає, що «діяльність із забезпечення безпеки як соціальний феномен стосовно подання протиріч між об'єктивною реальністю – небезпекою і потребами особи, соціальних груп, суспільства та держави на засадах попередження, локалізації та обмеження» [86, с. 13].

Пропонуючи концепцію двовимірності діяльності із забезпечення безпеки, учений далі вказує на горизонтальний (діяльність щодо дотримання безпеки людини, підприємницької структури, територіальної одиниці, держави тощо) і вертикальний (утвердження наукової, економічної, політичної технічної безпеки тощо) виміри [86, с. 14].

Слід зауважити, що В. А. Предборський зробив такі висновки, досліджуючи сферу економічної безпеки держави. Проте, на нашу думку, їх можна екстраполювати на сферу інформаційної безпеки, оскільки у представленій класифікації застосовано підходи, що повномірно відповідають заходам з протидії загрозам як об'єктивного характеру (економічні, військові, технічні тощо), так і суб'єктивного характеру (неправдиві відомості, дезінформація, протиправне втручання в систему акумулювання і зберігання баз даних тощо).

За результатами дослідження сектору безпеки України, яке було проведене Службою безпеки України упродовж 2005 - 2007 років, підготовлено монографічне дослідження «Правові засади інформаційної безпеки України», в якому її автори формулюють визначення понятійно-категоріального апарату у сфері державної безпеки.

Так, фахівці у сфері державної безпеки визначають поняття «забезпечення державної безпеки» як спеціальний вид діяльності у сфері національної безпеки, що здійснює система державних органів і військових формувань, використовуючи комплекс правових, організаційних, режимних, контррозвідувальних, оперативно-розшукових, службово-бойових і військових заходів, спрямованих на захист об'єктів державної безпеки [87, с. 56].

Необхідно вказати, що в основу представленої дефініції покладено поширений у юридичній науці підхід до розуміння категорії «забезпечення» як діяльності з реалізації заходів, проте воно не знайшло свого багатоаспектного відображення в українському законодавстві. Разом з тим, не дивлячись на значний часовий період, який відділяє наші реалії від оприлюднення СБУ результатів дослідження, пропоноване визначення не втратило актуальності, а навпаки, - набуло надто важливого значення під час російської агресії проти України.

Ми, ґрунтуючись на проведеному аналітико-правовому дослідженні окремих елементів структури національної безпеки, вважаємо, що при визначенні поняття «забезпечення інформаційної безпеки» потрібно виходити з найбільш широкого узагальнення якісних характеристик цього процесу. Такий підхід сприятиме повномірному висвітленню тих якостей, які, по-перше – розкриють сутність механізму взаємодії його складових; по-друге – відмежують його від інших суміжних процесів з подібним елементним наповненням.

О. О. Тихомиров, досліджуючи сферу інформаційної безпеки України, пропонує застосування методологічного інструменту, який уможлиблює розглядати її як своєрідну діяльність, в якій держава є активним учасником і відповідальною за стан дотримання належного рівня протидії інформаційним загрозам. Зміст державного забезпечення цієї галузі науковець розглядає як «систему державних гарантій в інформаційній сфері, безпосередньо чи опосередковано визначених фундаментальними нормативно-правовими актами, що регламентують інформаційну сферу суспільних відносин» [88, с. 72].

В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський застосовують діяльнісний підхід до ідентифікації діяльності держави на напрямках інформаційного забезпечення та вказують, що «забезпечення інформаційної безпеки досягають у процесі свідомої цілеспрямованої діяльності органів державного управління, із запобігання множинному поширенню їх нормального функціонування в результаті дії загроз і небезпек» [89, с. 161].

Водночас поняття забезпечення інформаційної безпеки зазначені науковці формулюють як «систему теоретико-методологічних, нормативно-правових, інформаційно-аналітичних, управлінських, розвідувальних, контррозвідувальних, оперативно-розшукових, кадрових, науково-технічних, ресурсних та інших заходів, спрямованих на забезпечення свідомого цілеспрямованого впливу суб'єкта управління на загрози та небезпеки, за якого

державні, міжнародні та недержавні інституції створюють необхідні умови для реалізації та прогресивного розвитку інформаційних інтересів, ефективне функціонування системи забезпечення інформаційної безпеки» [89, с. 267].

Ми погоджуємося з висловленим групою науковців судженням, адже правдивість інформації, своєчасне її отримання, протидія інформаційним загрозам та ефективна їх нейтралізація насправді виступають основою для прийняття якісних і ефективних управлінських рішень на всіх рівнях державного управління.

Т. Ю. Ткачук розглядає забезпечення інформаційної безпеки як складне комплексне поняття, яке охоплює низку процесів і явищ, пов'язаних з протидією загрозам безпеці національних інтересів в інформаційній сфері [90, с. 114]. Такі висновки науковець зробив за результатами дослідження питання нормативного забезпечення інформаційної безпеки в умовах євроінтеграційних процесів в Україні.

Зміст цього поняття науковець висвітлює крізь призму сукупної роботи з убезпечення цілісності об'єкта безпеки, спричиненою інформацією та інфраструктурою, а також засобів і суб'єктів діяльності.

Мету діяльності із забезпечення інформаційної безпеки держави пропонується розуміти як досягнення стану захищеності суспільних відносин від вияву зовнішніх і внутрішніх загроз, пов'язаних з інформацією та інформаційною інфраструктурою у процесі захисту національних цінностей, досягнення національних цілей [90, с. 104].

Даним визначенням науковець перераховує елементи, які, на думку інших науковців, належать до механізму забезпечення інформаційної безпеки, чи до системи її забезпечення. Такими складовими науковець визнає об'єкт, суб'єкт, загрози, засоби, мету тощо. Проте, такий підхід до визначення структури

системи забезпечення інформаційної безпеки видається дещо обмеженим, оскільки не стосується її системи чи механізму.

У наукових дослідженнях різних напрямків національної безпеки, серед яких і інформаційний, широко використовують системно-структурний підхід, що дає змогу розглядати забезпечення інформаційної безпеки на різних рівнях [91, с. 51-54].

Завдання щодо дотримання достатнього рівня інформаційної безпеки в Україні перебувають у нерозривному діалектичному зв'язку з іншими питаннями вітчизняного державотворення (політичні, економічні, соціальні, реформування державних інституцій, виховання національного громадянського суспільства, поглиблення демократичних засад тощо), що відбито у положеннях Стратегії національної безпеки України [92] та Закону України «Про основні засади забезпечення кібербезпеки України» [93].

На підґрунті наведеного вище на порядок денний виходять завдання щодо здійснення подальших законодавчих і управлінських заходів на напрямках посилення функціональних можливостей комплексних інструментів, що структурно обрамлюються поняттям «інформаційна безпека».

Висловлені узагальнення сприяють набуттю загальнонаукового характеру проблемі забезпечення інформаційної безпеки України. Його розробка передбачає координацію зусиль вчених - фахівців різних галузей знань та практиків з метою отримання науково-обґрунтованих і дієвих результатів як основи конструювання адміністративно-правових засад діяльності державних органів влади та місцевого самоврядування, громадських утворень та об'єднань самоорганізації населення на напрямках забезпечення інформаційної безпеки

Теоретико-правовим підґрунтям поняття «інформаційна безпека» є загальнотеоретичне вчення про безпеку як фундаментальну проблему юридичної

науки, що носить виражений міждисциплінарний характер і дає вихід на концепти спеціального правозастосування [94, с. 12].

Разом з тим, окремі питання досліджуються у зв'язку з галузевою спеціалізацією та проблематикою й вивчені дещо в меншій мірі. Винятком є, мабуть, концепція національної безпеки, що характеризується високим ступенем інструменталізації свого теоретико-методологічного апарату, що підтверджується дослідженнями В. Л. Ортинського та інших [95, с. 7].

У цьому зв'язку доцільно зробити висновок про те. Що інститут інформаційної безпеки як складової національної безпеки на цей час у вітчизняній правовій науці досліджений недостатньо.

Методологічно превалююче розуміння парадигми безпеки інформації, яка узагальнює і упорядковує теоретико-практичне підґрунтя стосовно досліджуваного об'єкта, викликає неоднозначні наукові оцінки, оскільки питання походження і розвитку інформаційної безпеки, її структурних елементів, здійснення систематизації складових механізмів функціонування та типології, урівноважування зв'язків між ними в комплексному сприйнятті цієї галузі права як складного юридичного явища, сучасна правова наука не надає.

З огляду на сказане вище, об'єктивно необхідно напрацювати науково обґрунтовані шляхи для розв'язання проблеми, пов'язаної з розумінням парадигми інформаційної безпеки у контексті загальної теорії безпеки з виведенням її на перші позиції, тобто наділенням статусу методологічної пріоритетності.

На думку Р. А. Чемчекаленка, О. П. Дзьобаня та О. Ю. Панфілова, «предметом системного дослідження інформаційної безпеки виступає виявлення типів зв'язків і, передусім, системотворчих зв'язків цілісності, виокремлення об'єктивної структури даного системного утворення та її характеру [96, с. 178].

Це надзвичайно важливо під час виконання Законів України «Про особливості державної політики із забезпечення державного суверенітету України на тимчасово окупованих територіях у Донецькій та Луганській областях» [97], «Про основні засади забезпечення кібербезпеки України» [93] та Доктрини інформаційної безпеки України [98] для досліджень, в яких загальнонаукові інструменти пізнання об'єктивної дійсності забезпечують виконання евристичних функцій. За такого підходу створюється система нових наукових теорій і гіпотез про той чи інший аспект сфери безпеки; формування її комунікаційних зв'язків з іншими видами безпеки; перехід категоріально-понятійного апарату однієї сфери безпеки в іншу, що сприяє розширенню можливостей для інтерпретації результатів наукового пошуку.

Отже, з великою вірогідністю можна констатувати, що саме держава відповідальна за впровадження ефективних засобів з протидії порушенням законодавства у сфері інформаційної безпеки, тобто лише органи, наділені відповідним обсягом компетенції, керуючись чинними нормативними документами, управлені застосовувати передбачені законом інструменти забезпечення встановленого конституційного правопорядку.

У контексті сказаного чітко вимальовується посилення до міжгалузевої категорії «правове забезпечення», яке екстраполюється на інститут інформаційної безпеки і співвідноситься з цим загальним поняттям на принципах галузевого підпорядкування.

Колектив науковців у складі О. Д. Довганя, Т. Ю. Ткачука визначає правове забезпечення інформаційної безпеки як цілісну систему правового регулювання суспільних відносин, яка має власний предмет правового регулювання [99, с. 79].

Прагнучи до збалансованого аналізу структурних елементів поняття «правове забезпечення інформаційної безпеки», необхідно фахово застосувати

такий методологічний інструмент, як науковий синтез. Завдяки його можливостям вдасться поєднати теоретичні і прикладні аспекти на напрямках вивчення проблеми правового регулювання інформаційної безпеки так, щоб на підґрунті визначення її значення, структурно-функціонального призначення та місця в загальному переліку проблем утвердження національної безпеки, напрацювати і узагальнити кореспондуючі елементи категоріально-понятійного апарату, внести обґрунтовані пропозиції на напрямках реформування й удосконалення чинного у цій сфері законодавства, а також оновити практику його застосування.

При науково-прикладному аналізі проблематики у сфері організації забезпечення інформаційної безпеки особливого значення набуває її структурно-елементна класифікація, яка досить умовна, і формується згідно з покладеними цілями і завданнями. У контексті сказаного доцільним є з використанням методу наукового аналізу здійснити розчленування цілісного поняття «інформаційна безпека» на джерела загроз, яких вирізняємо два види: заходи безпеки технічного характеру, що є похідним від інформаційно-комунікативних процесів, і заходи захисту, спричинені соціальними чинниками.

Т. Ю. Ткачук у цьому зв'язку зазначає, що стратегічне інформаційне протистояння становить небезпечний компонент гібридної війни, розгорнутої росією проти України, межа між двома складовими вельми розмита [100, с. 185]. Водночас, на думку науковця, головна загроза закладена в деструктивному впливі ворога на інформаційну структуру, суспільство, свідомість і підсвідомість людей для нав'язування власної системи цінностей у життєво важливих сферах життя суспільства і держави шляхом використання інформаційних джерел, що формують систему поширення інформації.

На нашу думку, представлена градація джерел загроз інформаційній безпеці держави має право на життя, оскільки є корисною з багатьох причин, а

саме дозволяє класифікувати оприлюднені концептуальні підходи до розв'язання проблем нормативно-правового забезпечення сект, а також розкриває шляхи до більш ґрунтовного застосування у наукових дослідженнях міжгалузевого методологічного інструментарію.

На цей час спектр загроз інформаційній безпеці значно розширився, торкнувся у тому числі соціальної сфери, а також скерований для завдання деструктивного впливу на всі сфери суспільного життя (політичну, економічну, соціальну, військову, екологічну тощо). У даному разі виходимо з того, що інформаційна безпека є невід'ємною складовою цілісного поняття «національна безпека». За таких умов доцільним видається екстраполяція характерних ознак, що притаманні національній безпеці, на її структурну складову (інформаційну безпеку), що сприятиме більш повному включенню загально доступних методів наукового дослідження для вирішення завдань наукової розвідки.

Важливо зазначити, що наукова література юридичного спрямування презентує неоднакові трактування такого системоутворюючого поняття, як «забезпечення інформаційної безпеки». У нашому розумінні забезпечення інформаційної безпеки – це безперервний, здійснюваний управленими органами процес, який, будучи складним соціально-правовим механізмом, формує та сприяє реалізації державної політики з метою підтримання належного рівня захисту інформації всіма можливими способами, які в узагальненому вигляді включають технологічну складову і встановлення передбаченої законом відповідальності для суб'єктів використання інформації за порушення встановленого порядку користування, отримання і передачі різних відомостей.

Р. А. Калюжний та О. О. Баєв зазначають, що стан нормативно-правового забезпечення інформаційної безпеки України як єдиної системи правового регулювання суспільних відносин у галузі протидії загрозам національним інтересам України в інформаційній сфері розвинуто недостатньо, що суттєво

знижує потенціал України щодо протидії загрозам її інформаційній безпеці, зміцненню національної оборони України [101, с. 5].

Науковець розглядає взаємозв'язок між рівнем нормативно-правового забезпечення інформаційної безпеки України та ступенем урегульованості суспільних відносин загально обов'язковими нормами, що мають кореспондуватися з міжнародними нормативно-правовими актами у сфері забезпечення інформаційної безпеки, які відповідно до положень статті 9 Конституції України є частиною національного законодавства.

Як вбачається, на час написання цієї роботи актуальними залишились пропозиції щодо необхідності офіційного визначення окремих елементів інституту національної безпеки, оскільки поняття «інформаційна безпека» отримало нормативну дефініцію в аналізованих вище законах України.

15 жовтня 2021 року Указом Президента України затверджено Стратегію інформаційної безпеки на період до 2025 року. Метою Стратегії є посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами спеціальної та політичної стабільності, оборони держави... [102].

Дослідження питань щодо прогнозування розвитку законодавства як результатів діяльності держави на напрямках посилення інформаційної безпеки набуло значної уваги з причини поширення практики застосування програмних і цільових інструментів, методів стратегічного прогнозування і планування у сфері публічного управління. Разом з тим, науковий доробок з проблем інформаційної безпеки, як правило, відбиває чисто технічні аспекти у підходах до розроблення заходів із забезпечення інформаційної безпеки. Так, наприклад, вирізняють провадження заходів з охорони інформаційно-телекомунікаційних систем, каналів обміну і передачі інформації, регулювання можливості доступу до джерел інформації, засекречування стану розробки засобів захисту

інформації, баз даних від витоку і несанкціонованого доступу. Така ситуація проглядається при виданні актів стратегічного спрямування, якими визначаються головні напрямки політико-економічного і соціального розвитку держави, відбуваються дослідження у сфері ефективності чинних нормативно-правових актів, якими регулюються правовідносини із захисту інформаційного середовища України.

Стратегічні напрацювання у формі доктрин, що реалізуються у сфері інформаційної безпеки, набувають форми засобів рішення і впливу на інформаційне середовище. Водночас вони спрямовані більшою мірою на вирішення політичних, а не правових задач, що є відбиттям реального стану законотворення в Україні. У цьому разі говоримо про невиправдане обґрунтування таких рішень політичною доцільністю.

Доктрина інформаційної безпеки України визначає такий перелік національних інтересів в інформаційній сфері: забезпечення прав і свобод людини на збирання, використання та поширення інформації; забезпечення конституційних прав людини на захист приватного життя; захищеність від руйнівних інформаційно-психологічних впливів; життєво важливі інтереси суспільства і держави [103].

Зміни, що відбуваються на напрямках посилення захисту особи як суб'єкта інформаційних відносин, підтверджують цільове призначення здійснюваних у межах доктринальних рішень заходів, зокрема те, що обрання здійснюваних убезпечувальних дій не є випадковим чи довільним процесом. Адже сфера інформаційної безпеки особи є відбиттям регулюючих впливів права, що розкриває його сутнісну характеристику.

Логічним підсумком до сказаного є те, що принципи гуманності визначають цільову спрямованість здійснюваних у сфері приватно-правового

захисту інформаційного простору особи, що відповідає вимогам високих європейських стандартів.

Системно-правовий аналіз положень Доктрини інформаційної безпеки України показав, що достатнім аргументом для того, щоб забезпечити повномірну реалізацію конституційних прав особи у сфері інформації, є отримання реальних результатів від реформування і вдосконалення всіх елементів державно-владного впливу на галузь інформаційної безпеки з одночасним дієвим контролем за виконанням приписів цього документа на всіх етапах функціонування задіяних правових механізмів.

Приблизно аналогічні висновки знаходимо в аналітичній записці Національного інституту стратегічних досліджень при Президентові України «Проблеми впровадження сучасних стандартів інформаційної безпеки в умовах національної системи кібербезпеки України» (2018 року) [104].

Т. В. Тарасенко наголошує на тому, що «визначення основних принципів державної інформаційної політики, розподіл повноважень і відповідальності державних органів у забезпеченні інформаційної безпеки значно посилюють позиції України в інформаційному протистоянні та створюють, за умови прийняття в руслі Доктрини інформаційної безпеки відповідного законодавства, необхідну основу для ефективного подолання інформаційних загроз у нинішній гібридній війні [105].

Особливості розвитку інформаційної сфери свідчать про те, що існують об'єктивні передумови для зниження ефективності стратегічного планування та реалізації Доктрини інформаційної безпеки України. До числа таких передумов, насамперед, відноситься суперечливість розвитку національного права внаслідок нерівномірної адаптації правової бази до вимог Європейського Союзу і НАТО [106, с. 188].

2.3 Правова характеристика нормативної бази у сфері інформаційної безпеки

Процес провадження наукового дослідження вимагає чіткого розуміння споріднених і відмінних ознак обраного об'єкта чи системи об'єктів, що обрамлюється поняттям «правова характеристика». Принагідно треба зазначити, що дане поняття набуло широкого застосування в теорії права як науки. Водночас, науковці, надаючи правову характеристику тим чи іншим об'єктам і явищам, не висловлюються щодо дефініції цього ключового поняття, чим розширюється дискусійний простір навколо обраної проблематики. У такому разі відбувається порушення логічного ланцюга наукового дослідження, адже, не маючи чітких і зрозумілих вихідних даних, неможливо вибудувати правову конструкцію, яка б мала аргументовану основу і відповідала критеріям істинності.

Проте, не зважаючи на всю складність щодо узагальнення наукових підходів до розуміння поняття «правова характеристика», доцільно навести визначення цього поняття, запропоноване М. В. Григорчуком у монографії «Правовий захист суб'єктів господарювання (теорія і практика)».

Науковець визначає «правову характеристику» як комплекс повноважень, які делеговані державою статусному учасникові нормативно врегульованих процесів і містять істотні ознаки, котрі виділяють його з-поміж інших, прирівняних до нього регуляторів суспільних відносин [107, с. 87].

Грунтуючись на загальному розумінні змісту і ролі суб'єктно-об'єктного складу комплексного науково-практичного явища «інформаційна безпека», виникає потреба надати правову характеристику нормативно-правовій бази з висвітленням меж легітимного втручання управнених суб'єктів до цього типу правовідносин.

Здійснений авторський аналітико-правовий моніторинг чинного законодавства цієї складової як елементу національної безпеки показав, що нормативно-правове регулювання відносин у сфері інформаційної безпеки набуло багаторівневої структури, де чітко проглядаються не тільки національні інструменти забезпечення «здорового» інформаційного поля, а й упроваджуються міжнародні нормативно-правові акти відповідно до положень статті 9 Конституції України [6] як частина національного законодавства. Всі елементи цієї системи перебувають у тісному діалектичному зв'язку, забезпечуючи певні рівні імперативності, та поширюючи свій вплив відповідно до компетенції, визначеної нормативно-правовими актами різної юридичної сили.

На наш погляд, з позицій правової оцінки сутності нормативного регулювання суспільних відносин у сфері інформаційної безпеки доцільно виокремити такі елементи у структурі юридичного забезпечення цієї сфери життєдіяльності суспільства: застосування (імплементация) міжнародних нормативно-правових актів, національний рівень регулювання (закони, підзаконні акти) і нормативні документи локального характеру. Тобто ми пропонуємо сферу інформаційної безпеки розглядати як трирівневу, елементи якої діють не тільки між собою, а й піддаються регулювальному впливу іншими правовими інструментами.

На загальний стан інформаційної складової у структурі складеного поняття «національна безпека» впливають низка чинників при домінуючій ролі економічної системи як підґрунтя для забезпечення життєдіяльності Української держави. При цьому потужну роль відіграють зовнішні економіко-політичні впливи, оскільки Україна є повноправним суб'єктом міжнародного співтовариства.

За сучасних умов світової кризи продовжується падіння економік розвинених країн, зменшується потенціал промислового виробництва, уповільнюються процеси руху товарів, а отже, питання забезпечення стабільності економічних систем, фінансової та промислової сфери є пріоритетним завданням усіх країн світу, в тому числі й України.

Доцільно зауважити, що реалії суспільно-політичних відносин потребують постійного оновлення національного законодавства у сфері національної безпеки, приведення його у відповідність до найвищих світових стандартів, міжнародно-правових актів, що зумовлює вжиття системних кроків з боку законотворців, управнених органів держави та наукової спільноти в частині перегляду положень нормативних актів, які регулюють питання формування та реалізації державної політики на напрямках забезпечення інформаційної безпеки в державі.

Україна, як постійний член Організації Об'єднаних Націй, перебуваючи у статусі союзної республіки СРСР, та у подальшому після проголошення незалежності, приєдналася до основних міжнародних документів ООН з прав людини, якими визначено засадничі принципи діяльності суб'єктів державної політики у різних сферах, зокрема, щодо забезпечення свобод і прав людини і громадянина, оборони і національної безпеки, обігу і поширення інформації, а також на напрямках розвитку інститутів громадянського суспільства тощо.

На думку В. О. Торічного, найважливішим елементом, що забезпечує цілеспрямовану координацію зусиль всіх державних і громадських сил держави щодо забезпечення національної безпеки, виступає її система державного управління [108, с. 78].

Є. А. Макаренко, досліджуючи роль міжнародного співробітництва у сфері інформаційної безпеки, зазначає, що «регіональне співробітництво у сфері інформаційної безпеки зумовлює необхідність пошуку спільних рішень у межах

міжнародних організацій щодо протидії інформаційним та кіберзагрозам, інформаційному тероризму та інформаційній злочинності [109, с. 51].

Досліджуючи роль ООН в організації заходів з питань забезпечення інформаційної безпеки у планетарному масштабі, О. М. Фролова заявляє, що «увага міжнародної спільноти в останню чверть століття прикута здебільшого до розробки міжнародно-правових основ протидії транснаціональним інформаційним загрозам» [110].

На цьому етапі посилаємося до розробленої ООН Хартії про права людини, до складу якої включено Загальну декларацію прав людини (затверджена і проголошена Генеральною Асамблеєю ООН 10 грудня 1948 р.) [111], Міжнародного пакту про економічні, соціальні і культурні права [112] та Міжнародний пакт про громадянські та політичні права [113].

Загальна декларація прав людини [111] як фундаментальний міжнародно-правовий акт, включає систему правових гарантій, що визначають зміст та сутність інформаційної безпеки і свободи особи.

Положення статті 19 Загальної декларації прав людини [111] отримали продовження в нормах статей 33 і 34 Конституції України (наводилися вище).

Статтею 10 Конвенції про захист прав і основних свобод людини (Європейська конвенція з прав людини) 1950 року, послідовно поглиблюючи положення статті 19 Загальної декларації, встановлено певні запобіжники, які застосовуються: «в інтересах національної безпеки, територіальної цілісності або громадської безпеки, для запобігання заворушенням чи злочинам, для охорони здоров'я чи моралі, для захисту репутації чи прав інших осіб, для запобігання розголошенню конфіденційної інформації або для підтримання авторитету і безсторонності суду» [114].

На думку суддів Європейського суду з прав людини, мова йде «про з'ясування серйозності втручання у закріплені в Конвенції права порівняно з

шкодою суспільним інтересам, яка може виникнути як наслідок неповного захисту зазначених інтересів» [115].

Водночас, потрібно звернути увагу на імперативну вимогу щодо формування і функціонування інформаційного середовища, зазначеного частиною 2 статті 19 Міжнародного пакту про громадянські та політичні права 1966 року, де йдеться про те, що кожна людина має право одержувати і поширювати будь яку інформацію та ідеї, незалежно від державних кордонів, усно, письмово чи за допомогою друку або художніх форм вираження чи іншим способом на свій вибір.

Частиною 3 цієї статті [112] запроваджено нормативно-визначені обмеження щодо неприпустимості зловживання у демократичному суспільстві окремими правами, як, наприклад, заборона поширення інформації на шкоду державній безпеці, здоров'ю чи моральності населення, громадського порядку, а також неприпустимості проявів неповаги до прав інших осіб чи завдання іншої шкоди їх репутації.

Історико-правовий аналіз показав, що в результаті протиправного використання інформаційних ресурсів інформаційні технології набувають якостей зброї, що має наслідком поширення кіберзлочинності, інформаційні війни, а також міжнародний тероризм.

Оцінюючи ризики деструктивного впливу джерелами інформації на психологічний стан суспільства, М. В. Маркова зазначає, що «на сьогодні ІПВ (інформаційно-психологічна війна) по праву вважається найефективнішим засобом досягнення й забезпечення розвиненими країнами власних цілей та інтересів, ведеться постійно як у мирний, так і воєнний час, має прямий та безпосередній вплив на всі життєво важливі сфери діяльності країни-супротивника» [116, с. 73].

П. С. Черкашин, досліджуючи міжнародно-правові аспекти інформаційної безпеки у межах концепції «вільного потоку», вказує: «прихильники концепції обстоюють думку, що вона є невід'ємною частиною права людини на свободу пошуку, отримання та поширення інформації прихильники концепції обстоюють думку, що вона є невід'ємною частиною права людини на свободу пошуку, отримання та поширення інформації... [117, с. 138].

Водночас, Статут ООН від 26.06.1945 р. включає перелік принципів щодо формування внутрішньої політики держави, які є обов'язковими у всіх сферах соціального управління, включаючи інформаційну [118]. За змістом статей 1 і 2 аналізованого документу держави-учасники беруть зобов'язання розробляти і реалізовувати заходи, спрямовані на подолання джерел загроз миру і безпеці, здійснювати профілактику і не допускати акти агресії, протидіяти зазіханням на конституційний устрій, визнані державні кордони, а також невтручання у внутрішні справи держави.

На доповнення до вищенаведеного необхідно звернутися до положень окремих конвенцій Ради Європи і постанов ООН, якими врегульовуються правовідносини в інформаційній сфері з урахуванням превентивних заходів, метою яких є недопущення порушень встановленого порядку у сфері роботи з інформацією.

У цьому зв'язку звертаємо увагу на рішення Конвенції Ради Європи про кіберзлочинність (ратифіковано Законом України від 07.09.2005 р. № 2824-IV) [119].

Коментований нормативно-правовий акт обґрунтовує низку обов'язкових положень, які необхідно враховувати суверенним державам як стандарти розробки і реалізації заходів управлінської політики, спрямованої на забезпечення належного рівня інформаційної безпеки. У нашому розумінні коментованими положеннями прокладається правова рівновага між захищеними

законом інтересами і повагою до основоположних прав і свобод людини, забезпечується активізація і виведення на якісно більш високий рівень кримінальних проваджень, пов'язаних з протиправним втручанням в інформаційну сферу, а також криміналізація діянь, які, завдаючи шкоду особі чи державі, не внесені до переліку кримінально караних.

Наступним документом, яким є Конвенція ООН про використання електронних повідомлень у міжнародних договорах (затверджена резолюцією Генеральної Асамблеї ООН (далі - ГА ООН) № 60/21 від 23.11.2005 р., визначено, що «держава сприяє визнанню юридичної сили інформації, яка міститься в електронних повідомленнях, що використовуються у процесі налагодження міжнародної торгівлі [120].

Таким чином, держава сприяє стимулюванню комерційної діяльності, а також активізації міжнародної торгівлі.

Не менш важливого значення для формування міжнародно-правових стандартів державного управління у сфері забезпечення інформаційної безпеки набули Резолюції Генеральної Асамблеї ООН. Примітним є те, що зазначений тип документів ухвалюється за результатами предметних обговорень їх змісту у середовищі спеціалістів, у процесі переговорів між лідерами світових держав, а також у ході роботи міжнародних симпозіумів, конференцій тощо.

На думку О. В. Бойченко, такий підхід «дає змогу прийняти «виважений» міжнародно-правовий акт з урахуванням специфіки національних законодавств» [121, с. 79].

За два останніх десятиліття Генеральна Асамблея ООН схвалила низку нормативних документів, які торкаються питань забезпечення інформаційної безпеки країни у межах міжнародно визнаних територій. Для більш повного висвітлення досліджуваної проблематики проаналізуємо окремі з них, а саме Резолюції:

– ГА ООН № 60/45 «Досягнення у галузі інформатизації та телекомунікацій в контексті міжнародної безпеки (в редакції від 02.12.2008 р.) [122]. Відповідно до положень даного документу держави-учасниці ООН мають забезпечити вільний доступ до джерел інформації, одночасно розробляючи заходи для нейтралізації загроз інформаційній безпеці;

– ГА ООН № 64/211 від 21.12.2009 р. «Створення глобальної культури кібербезпеки та оцінка національних зусиль із захисту найважливіших інформаційних інфраструктур [123]. Документ надає кожній державі-учасниці право самостійно визначати інструменти і засоби захисту власних інфраструктур у сфері інформації, одночасно забезпечивши рівний доступ до інформаційних ресурсів (технології). При цьому обмін даними має бути достатньою мірою захищений;

– ГА ООН № 65/141 від 20.12.2010 р. «Використання інформаційних комунікацій технологій з метою розвитку» [124], якою від країн-учасниць вимагається дотримання гендерної рівності при доступі і використанні інформаційних технологій, забезпечити недостатньо забезпечених верств населення користуватися ними, а також налагодити державно-правове партнерство при фінансуванні розвитку інфраструктури у сфері інформації.

Зміст наведених положень резолюцій підтверджує, що ООН враховує глобальні проблеми сучасності у процесі формування універсальних пропозицій із питань протидії загрозам інформаційної безпеки на національному рівні.

Для досягнення більш високого рівня розуміння специфіки становлення і розвитку в Україні цілісного правового явища «інформаційна безпека» ми здійснили авторський аналіз нормативно-правового регулювання цієї сфери з позицій хронології законотворчої діяльності та впровадження підзаконних нормативно-правових актів. На підставі отриманих висновків пропонуємо розглядати чотири етапи у розвитку і функціонування правових механізмів у

сфері інформаційного забезпечення процесів вітчизняного державного будівництва:

перший етап – доконституційний (1991 – 1996 роки);

другий етап – ранньоконституційний (1996 – 2006 роки);

третій етап – (2007 – 2013);

четвертий етап – 2014 – до сьогодні. Останні два етапи (третій і четвертий) пропонуємо визначати як зрілоконституційні.

Приступаючи до теоретико-правового аналізу законодавчого забезпечення сфери інформаційної безпеки, зазначаємо, що першим етапом розвитку цієї складової національної безпеки України доцільно визначити 1991 – 1996 рр. З перших днів державної незалежності перед Україною постало завдання нормативно-правовими інструментами врегулювати відносини у сфері створення, зберігання, обміну інформацією між її учасниками, оскільки такої правової спадщини від колишнього СРСР не було отримано.

Зважаючи на тогочасні реалії вкрай необхідним було напрацювати національні механізми регулювання інформаційної сфери. Першим документом незалежної України на напрямку нормативно-правового супроводження сфери інформаційних відносин став Закон України «Про інформацію», схвалений 02.10.1992 р. [3]. Ним визначено національні пріоритети для розвитку державної політики в інформаційній сфері, а саме: забезпечити громадянам доступ до інформації; формування вітчизняної системи інформаційних мереж; посилення матеріально-технічного, фінансового, організаційного, правового і наукового супроводження процесу становлення інформаційної сфери, створити умови для розвитку міжнародного співробітництва у галузі інформації при суворому забезпеченні захисту інформаційного суверенітету України.

Закон України «Про інформацію» [3], схвалений до прийняття Конституції України, започаткував упровадження інших актів різної юридичної сили, що

сприяло подальшому удосконаленню механізмів правового регулювання сфери захисту інформаційної безпеки. Закладені положення у нині нечинному Законі України набули видозміненого вигляду в нормативно-правових актах, у тому числі Законах України:

– «Про друковані засоби масової інформації в Україні» (від 16.11.1992 № 2782-XII [125] – створено правову базу для діяльності друкованих засобів масової інформації, запроваджено державну підтримку і закладено гарантії свободи преси та інструменти міжнародної співпраці в галузі поширення інформації друкованими виданнями;

– «Про науково-технічну інформацію» (від 25.06.1993 № 3322-XII) [126] – визначено основні напрямки державної політики у сфері науково-технічної інформації, розроблено порядок її формування і виконання з метою забезпечення;

– «Про телебачення і радіомовлення» (від 21.12.1993 № 3759-XII) [127] – врегулював відносини співпраці між телебаченням і радіомовленням, сформував правові, соціальні, організаційні, економічні відносини, а також участь громадян у даних видах діяльності при суворому дотриманні свободи слова та правомірного поширення інформації;

– «Про авторське право і суміжні права» (від 23.12.1993 № 3792-XII) [128] – створено правове поле для легітимної охорони особистих майнових і немайнових прав у сфері інтелектуальної власності, розроблено і захищено авторське право і суміжні права при використанні результатів інтелектуально-творчої діяльності;

– «Про державну таємницю» (від 21.01.1994 р. № 3855-12) [129] – розроблено і забезпечено порядок роботи з інформацією, що віднесена до державної таємниці, з метою захисту інтересів держави та національної безпеки встановлено режим засекречування і розсекречування інформації;

– «Про захист інформації в автоматизованих системах» (від 05.07.1994 № 80/94-ВР в редакції 2005 р.) [130] – врегульовано відносини у галузі дотримання встановленого порядку користування інформацією в інформаційно-телекомунікаційних системах;

– «Про інформаційні агентства» (від 28.02.1995 № 74/95-ВР) [131] – закладено основу для діяльності в Україні інформаційних агентств, а також розроблено порядок їх міжнародного співробітництва.

Другий етап розвитку нормативно-правового забезпечення інформаційної безпеки України в економічній сфері необхідно визначити з 1996 – 2006 рр. Цей етап співпав зі схвалення Конституції України, положеннями якої кожному гарантовано право вільно збирати, використовувати, зберігати і поширювати інформацію у будь-який спосіб (усно чи письмово, засобами джерел масової інформації тощо. Крім того, Основний Закон гарантує таємницю телефонних розмов та листування, пересилання інших видів кореспонденції.

З прийняттям Конституції України Верховна Рада України і органи державної влади продовжили роботу щодо удосконалення чинної нормативно-правової бази, що віднайшло відображення у прийнятті нових документів, а саме Законів України:

– «Про рекламу» (від 03.07.1996 № 270/96-ВР) [132] – визначено принципи діяльності, пов'язаної з надання рекламних послуг, врегульовано відносини при виробництві, розповсюдженні та використанні реклами;

– «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації» (від 23.09.1997 № 539/97-ВР) [133] – встановлено основи для об'єктивного і всебічного висвітлення представниками засобів масової інформації результатів роботи органів державної влади та місцевого самоврядування, а також

запроваджено інструменти захисту їх убезпечення від протиправного тиску управнених структур з різними владними повноваженнями;

– «Про державну підтримку засобів масової інформації та соціальний захист журналістів» (від 23.09.1997 № 540/97-ВР) [134] (запроваджено організаційно-правові та економічні основи державної підтримки діяльності засобів масової інформації, а також правові гарантії соціального захисту журналістів, що сприяло підвищенню ефективності правового регулювання у сфері інформації;

– «Про Концепцію національної програми інформатизації» (від 04.02.1998 № 75/98-ВР) [135] – подається характеристика актуального стану інформаційної сфери, окреслено стратегічні напрямки, мету та правову основу інформатизаційних процесів, а також здійснюється прогноз очікуваних результатів від застосовуваних заходів;

– «Про національну програму інформатизації» (від 04.02.1998 № 74/98-ВР) [136] – закладено основи формування, коригування та виконання передбачених даним документом заходів;

– «Про захист суспільної моралі» (від 20.11.2003 № 1296-IV) [137] – встановлено нормативні обмеження щодо поширення серед громадян шкідливого інформаційного контенту, який негативно впливає на моральні устої суспільства;

– «Про електронні документи та електронний документообіг» (від 22.05.2003 № 851-IV) [138] – врегульовано порядок роботи та обігу електронних документів;

– «Про електронний цифровий підпис» (від 22.05.2003 № 852 IV) [139] – обґрунтовано правове забезпечення і юридичний статус електронного цифрового підпису, а також сферу його застосування.

Квінтесенцією законотворчої діяльності можна вважати прийняття і введення в дію Закону України «Про звернення громадян» [140], яким врегульовано механізми практичної реалізації громадянами України наданого їм Основним Законом гарантованого права оскаржувати неправомірні, на їх думку, дії представників органів державної влади і місцевого самоврядування, а також брати участь у роботі об'єднань громадян, подавати індивідуальні і колективні скарги тощо.

На виконання положень вищенаведених актів законодавства видано підзаконні нормативно-правові акти різної юридичної сили, а саме: постанови Верховної Ради України (далі – ВРУ), укази Президента України та постанови Кабінету Міністрів України (далі – КМУ).

У переліку постанов ВРУ доцільно зазначити:

- «Про затвердження Концепції технічного захисту інформації в Україні (від 08.10.1997 № 1126) [141] – визначено основні засади державного регулювання процесів забезпечення технологічними інструментами захисту інформаційної сфери держави;

- «Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації систем і засобів автоматизованої обробки та передачі даних» (від 04.02.1998 №121) [142] – узаконено види робіт на напрямках використання інформаційних систем, гарантійне і післягарантійне обслуговування систем автоматизованої обробки даних тощо;

- «Про заходи щодо посилення контролю за обґрунтованістю проєктів інформатизації діяльності центральних органів виконавчої влади» (від 16.02.1998 № 160) [143] – упорядковано процеси фінансування з державного бюджету проєктів щодо забезпечення інформаційного обслуговування діяльності центральних органів виконавчої влади, запроваджено обов'язковий порядок попереднього погодження доцільності запровадження таких ініціатив;

– «Про затвердження Положення про формування та виконання Національної програми інформатизації» (від 31.08.1998 № 1352) [144] – передбачено запровадження комплексу заходів з метою поглиблення чинних нормативно-правових актів у сфері інформаційної безпеки, виконання завдань щодо розроблення пропозицій з удосконалення систем і засобів використання і захисту інформаційного середовища, а також робіт, пов'язаних з експлуатацією та обслуговуванням технологічних складових інформатизації;

– «Про затвердження Порядку локалізації програмних продуктів (програмних засобів) для виконання Національної програми інформатизації (від 16.11.1998 № 1815) [145] – означеного суб'єкти і об'єкти локалізації, специфіку покриття витрат на локалізацію програмних продуктів;

– «Про затвердження Порядку формування та виконання регіональної програми і проекту інформатизації» (від 12.04.2000 № 644) [146] – визначено принципи формування регіональних програм у складі Національної програми інформатизації, а саме джерела їх фінансування, права і зобов'язання державних замовників, суб'єктів програм та концепції щодо їх впровадження;

– «Про Урядову комісію з питань інформаційно-аналітичного забезпечення діяльності органів виконавчої влади» (від 07.05.2000 № 777) [147] – визначено повноваження, службову компетенцію, завдання та правову основу діяльності Урядової комісії з питань забезпечення інформаційними ресурсами органів виконавчої влади;

– «Про затвердження Порядку формування та виконання галузевої програми і проекти інформатизації» (від 18.12.2001 № 1702) [148] – визначено джерела фінансування, а також суб'єкти та державні замовники програм, концепції і програми подальшого розвитку інформаційного забезпечення;

– «Про Концепцію національної інформаційної політики» (від 03.04.2003 № 687-IV) [149] – схвалено проект однойменного Закону України;

Третій етап розвитку нормативно-правового забезпечення інформаційної безпеки України в економічній сфері визначити з 2007 – 2013 рр., який характеризується внутрішньополітичними та соціально-економічними реформами. У цей період приймаються низка законодавчих актів, зокрема:

- «Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки» (від 09.01.2007 № 537-V) [150] – визначено стратегічні цілі розвитку інформаційного суспільства, впровадження новітніх інформаційних технологій в усі сфери життя суспільства, прискорення розробок у галузі інформаційних технологій;

- «Про захист персональних даних» (від 01.06.2010 № 2297-VI) [151] – запроваджено правові механізми регулювання відносин, пов'язаних з використанням персональних даних при суворому дотриманні конституційних засад прав людини і громадянина;

- «Про доступ до публічної інформації» (від 13.01.2011 № 2939-VI) [4] – визначено порядок доступу до інформації, що перебуває у володінні суб'єктів владних повноважень і становить суспільний інтерес, з урахуванням конституційних гарантій на отримання правдивої і неупередженої інформації;

- «Про адміністративні послуги» (від 06.09.2012 №5203-VI) [152] – сформульовано правові основи реалізації прав учасниками інформаційної сфери при отриманні і наданні адміністративних послуг.

Н. А. Литвин, досліджуючи адміністративно-правове забезпечення інформаційної діяльності органів ДФС України, виокремлює четвертий етап розвитку нормативно-правового забезпечення інформаційної безпеки України в економічній сфері, вказавши період з 2014 р. по теперішній час [153, с. 77–85].

21 червня 2018 р. було ухвалено Закон України «Про національну безпеку України» [7], яким визначено сутність та надано тлумачення ключових термінів-складових частин цілісного юридичного явища «національна безпека»,

окреслено основні напрямки утвердження і захисту конституційного правопорядку у сферах воєнної, державної безпеки, громадського порядку і громадської безпеки, оборонне планування тощо, розроблено відповідні стратегії.

Отже, як бачимо, у профільному Законі України значну увагу акцентовано на секторах безпеки і оборони, контррозвідувальній діяльності, інформаційній та кібер- сферах. Особливе значення надано питанням організації діяльності Збройних Сил України.

Водночас, коментований Закон України не надає системного розуміння економічної безпеки держави як основоположного елементу, завдяки якому будуються інші складові національної безпеки. За відсутності достатнього матеріального і фінансового забезпечення Збройних Сил, оборонного комплексу та захисту інформаційного забезпечення їх функціонування неможливо розраховувати на належний захист державного суверенітету від зовнішніх і внутрішніх загроз.

З урахування вищенаведеного доцільно запропонувати пропозиції щодо вдосконалення коментованого Закону на таких напрямках: більш повно викласти окремі визначення системоутворюючих понять, а саме поняття «національна безпека», у зв'язку з тим, що у ньому нерозривно поєднані всі сфери життєдіяльності суспільства (політична, військова, економічна, кібернетична, інформаційна, екологічна тощо).

Наступна пропозиція торкається більш чіткого формулювання поняття «національні інтереси» (п. 10 ст. 1 та ст. 3 Закону) [20], яке у чинній редакції визначено як скеровані на убезпечення важливих життєвих інтересів людини, держави і суспільства, захист державного суверенітету України, придатні для життя умови життєдіяльності та добробут громадян.

На нашу думку, ч. 3 ст. 3 додатково слід включити більш широке коло інтересів з урахуванням широкого аспекту життєво важливих сфер життя суспільства, оскільки складові, включені до переліку національних інтересів, не повною мірою охоплюють значне коло правовідносин.

Визначаючи Стратегії національної, воєнної, кібербезпеки, оборонно-промислового комплексу та інших напрямків захисту державного суверенітету на тривалу перспективу, коментований Закон України не приділяє достатньої уваги супровідним документам, якими забезпечується формалізована складова цих процесів, а саме поетапне планування (короткострокове, середньострокове тощо) з урахуванням реальної ситуації в державі.

Ці положення Закону майже повністю співпадають зі змістом Закону Грузії «Про правила планування та координації політики національної безпеки», відповідно до якого планування політики національної безпеки Грузії здійснюється за допомогою концептуальних та організаційних документів національного та відомчого рівнів [154].

Отже, здійснивши правову характеристику нормативного забезпечення процесів провадження державно-правової діяльності у сфері інформаційної безпеки, з урахуванням специфіки функціонування міжнародних інструментів на напрямках утвердження демократичних цінностей у планетарному масштабі, доцільно перейти до наступних складових цього дослідження, у ході яких проаналізуємо джерела загрозам інформаційній безпеці, міжнародний досвід, у тому числі у країнах Європейського Союзу, та інструменти стримування і профілактики деструктивних проявів у зазначеній сфері.

Висновки до розділу 2

Таким чином, аналіз наукової літератури щодо дослідження проблем розуміння соціальної цінності змісту і функціонування правового явища «інформаційна безпека» показав, що нормативно-правове забезпечення цієї сфери в Україні характеризується високим рівнем науковості, відзначається системність при обранні підходів до галузевого дослідження проблематики на цьому напрямку. Все вказане свідчить про наявність складного механізму, який функціонує на базі діалектично поєднаних складових, що перебувають у постійному русі, обслуговуючи інформаційний простір. З таких позицій можна зробити обґрунтований висновок про багатоаспектність проблематики, яка простежується у процесах практичного застосування заходів у сфері інформаційної безпеки на напрямках утвердження моральних засад насправді демократичного суспільства.

Доведено, що правове регулювання суспільних відносин у сфері забезпечення інформаційної безпеки є матеріальним підґрунтям, яким визначається правомірність використання інформаційних ресурсів суб'єктами даного типу правовідносин, межі дозволеного втручання в інформаційне поле, а також провадження превентивно-профілактичних заходів на напрямках протидії шкідливому і ворожому втручання в інформаційну сферу України. Така діяльність з боку суб'єктів законодавчої ініціативи має проводитись у тісній співпраці з науковцями і практиками для досягнення найбільш ефективного результату на зазначених напрямках.

Не потребує доведення той факт, що на сьогодні інформаційна сфера в Україні є однією з найбільш уразливих складових у системі національної безпеки. У цьому зв'язку на порядок денний постають питання щодо посилення загороджувальних дій з боку управлінських органів на всіх напрямках

функціонування інформаційної сфери, адже порушення її цілісності як підґрунтя формування і утвердження національних інтересів спричинить надзвичайно потужний руйнівний ефект, який зробить вразливими інші складові національної безпеки.

Агресія з боку росії щодо України викликала потребу в терміново переглянути стратегічні засади, у тому числі гуманітарні, на яких ґрунтувалася система не лише вітчизняної, а й європейської безпеки донині. З огляду на це, Україні необхідно запропонувати адекватні ситуації термінові заходи щодо забезпечення енергетичної, економічної та інформаційної безпеки.

У зв'язку з цим актуалізується проблема нормативного забезпечення процесів, при яких інформаційна сфера стає фундаментом для провадження комунікації на всіх рівнях життя суспільства, а сама інформація як явище матеріального світу відіграє трансмісійну роль, яка покладається у пряму залежність від коректної дії комплексу механізмів, що урухомлюють всю систему відносин передавання і обміну даними в Україні.

У нашому розумінні значення ціннісного (аксіологічного) підходу для виконання завдань нашого дослідження полягає у тому, що завдяки притаманним йому міжгалузевим правовим і морально-філософським якостям забезпечується виховання моральності членів суспільства, завдаються ціннісні орієнтири у свідомості людей, формуються високоморальні внутрішні переконання, що спонукає їх до неухильного виконання приписів законів та підзаконних нормативно-правових актів.

Державна політика у сфері забезпечення інформаційної безпеки має ґрунтуватись ґрунтуватися на результатах наукових і методологічних розробок, сформованих у певну систему і розроблені у форматі концепцій чи стратегій. Для такого стану справ потрібні сформовані і чітко окреслені цілі і завдання таких робіт, встановлені конкретні строки та відповідальні особи. При цьому

передбачається необхідним залучити громадськість до обговорення цієї проблематики, а також забезпечити широке міжнародне представництво.

Завданнями державної політики на напрямках дотримання достатнього рівня інформаційної безпеки розглядаємо необхідність створення нормативного поля для формування відкритого інформаційного суспільства, яке би набуло практичної можливості користуватися у повній мірі як досягненнями технологічної складової цього елементу національної безпеки, так і мало гарантії того, що вона перебуває у тотально захищеному інформаційному просторі, який охороняється найбільш ефективними інструментами протидії капітулянтству чи дезінформації.

Достатньою умовою виконання заходів, передбачених у межах нормативного регулювання відносин в інформаційній сфері, є забезпечення якісного нормативно-правового регулювання цієї сфери у формі ухвалення законодавчих і підзаконних актів, встановлення дієвого контролю за дотриманням встановленого порядку користування інформацією, запровадженням відповідальності за порушення встановлених правил тощо.

Здійснивши теоретико-аналітичне дослідження документів різного рівня юридичної сили (закони, підзаконні акти тощо) на напрямках утвердження гарантованого Конституцією України порядку поведінки з інформацією, здобуто чітке розуміння якісних складових процесів провадження заходів з дотримання інформаційного «здоров'я» Українського суспільства крізь призму застосування механізмів аналізу і синтезу. Такі методологічні інструменти застосовано у межах вивчення правової характеристики нормативної бази на декількох рівнях і в тому хронологічному порядку, який представлено в авторському поділі на часові періоди.

Поглиблене аналітико-правове дослідження міжнародних нормативно-правових актів, прокладання діалектико-філософських зв'язків між ними і

чинним українським законодавством у сфері регулювання відносин на напрямках забезпечення інформаційної безпеки сприятиме фаховому аналізу інших аспектів відображення ролі цієї складової у загальному контексті дотримання належного рівня національної безпеки, нейтралізації джерел загроз інформаційній безпеці тощо. Все це буде представлено у подальших підрозділах.

РОЗДІЛ 3

АНАЛІЗ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ТА МІЖНАРОДНИЙ ДОСВІД З ПРОТИДІЇ ПОРУШЕННЯМ ВСТАНОВЛЕНОГО ПОРЯДКУ ПОВОДЖЕННЯ З ІНФОРМАЦІЄЮ

3.1 Джерела загроз інформаційній безпеці та їх класифікація

Міжнародний світовий порядок та внутрішня ситуація в Україні поряд з закономірними тенденціями взаємодії і розвитку підпадають під перманентну дію деструктивних інструментів різного рівня загроз. Така ситуація проглядається в усіх сферах життєдіяльності суспільства. Особливо чутливою для протиправних зазіхань і проявів є інформаційна складова в організації суспільної діяльності. У контексті сказаного доцільно навести всесвітньо відомий вислів Натана Ротшильда про те, що той, хто володіє інформацією, - володіє світом. Цим лаконічним виразом відбивається всі сутність і значення інформаційної сфери як суспільного продукту, за володіння яким триває постійна відкрита чи прихована боротьба між зацікавленими сторонами.

Оцінюючи можливі напрямки протиправного втручання у легітимне інформаційне поле, Ю. Є. Максименко [73, с. 3] вказує, що розвиток вищезгаданих інформаційних засобів й технологій спричиняє негативний ефект, оскільки відбувається значне зростання порушень порядку використання відомостей, а саме протизаконного збирання інформації, несанкціонованого доступу до інформаційних ресурсів, знищення чи пошкодження баз даних шляхом запуску вірусних програм, викрадення інформації з архівів, банків, бібліотек тощо. Значних збитків завдається незаконним витоком інформації чи її протиправним копіюванням.

Особливого значення для нашої держави набувають завдання щодо дотримання необхідного рівня захисту інформації у напередодні та під час повномасштабного вторгнення росії до України 24 лютого 2022 року. За таких умов потрібно вести розмову про запровадження перманентно діючого механізму відвернення чинних загроз інформаційній сфері, а також ведення постійного моніторингу інформаційного простору з метою створення превентивно-профілактичного середовища для відфільтровування шкідливого контенту та нейтралізації протиправних дій щодо втручання в конкретну інформаційну систему.

Здійснене авторське дослідження нормативно-правової бази та наукового доробку, якими подано фахово-практичну оцінку джерел загроз інформаційній безпеці, дає підстави розуміти, що небезпека для інформаційної сфери може з'являтися на різних рівнях використання, що потребує формально визначених дефініційних і компетенційних меж для забезпечення ефективного регулюючого і профілактико-превентивного впливів з боку управнених державою органів. Вихідними положеннями для визначення і класифікації джерел загроз інформаційній безпеці України обираємо конституційні інструменти дозволених меж володіння і поширення різного наповнення відомостей, про що йдеться в раніше цитованій у підрозділі 1.1 статті 17 Основного Закону [6], а також визначених частиною 2 статті 32 Конституції України [6], положеннями якої містять заборону без згоди особи поширювати, зберігати чи використовувати конфіденційну інформацію про неї. Виключення становлять випадки, коли це необхідно для забезпечення національної безпеки, прав людини чи економічного добробуту.

Про значний рівень шкідливості від деформованого інформаційного поля і масиву даних йдеться у науковому доробку Г. Сащука [48]. Науковець висловлює застереження, що деструктивний вплив інформаційних атак може

змінювати мораль і світогляд не тільки окремої людини, а посягати на переорієнтування в своїх інтересах всього суспільства чи значної його частини. Таким атаками нав'язуються чужі інтереси, здійснюється прихована агресивна дія на основні моральні цінності особи і суспільства, що через наявність агресивного контенту завдає шкоди інформаційному середовищу та національній безпеці. У зв'язку з наведеним постає нагальна необхідність запроваджувати ефективні механізми захисту проти посягань на державний суверенітет і територіальну цілісність шляхом протиправного втручання в інформаційну сферу України.

Водночас, реалізуючи своє суб'єктивне право на право вираження свободи думки, вільне волевиявлення переконань і поглядів, частиною 3 статті 34 Конституції впроваджено обмеження щодо вільного тлумачення права на володіння інформацією і її використання (таке право може бути обмежене законом задля недопущення протиправного втручання у сферу інтересів, що загрожують національній безпеці, зазіхають на територіальну цілісність держави, а також несуть загрози громадському порядку і безпеці, спонукають до вчинення правопорушень і злочинів проти інших осіб та їх конституційних прав, загрожують їх репутації, є загрозами для встановленого порядку обігу інформації тощо).

Отже, саме з протиправних дій щодо володіння і використання інформації виникають першопочаткові небезпеки у цій сфері, які набувають визначення як джерела загроз інформаційній безпеці.

Для фахового дослідження піднятої проблематики вдамося до застосування методологічних інструментів, які є, на нашу думку, найбільш відповідними для розуміння юридичної природи і семантики поняття «джерела загроз», а саме гносеологічного методу у поєднанні з методами наукової індукції і дедукції.

Інтернетресурс без посилання до авторства надає дефініцію поняття «джерела загроз» - це умови і чинники, які таять в собі і за певних умов самі по собі або в різній сукупності виявляють ворожі наміри, шкідливі властивості, деструктивну природу [155].

На нашу думку, поточним поясненням сутності і юридичної описовості джерел загроз інформаційній безпеці також можна визначати первинні причини і їх прояви загрозливого характеру в інформаційній сфері, спрямовані на ураження життєво важливих інтересів особистості, суспільства, а також держави. На цьому рівні доцільно говорити про тісну співпрацю науковців і представників практичного сектору інформаційного поля, оскільки автономне функціонування зазначених елементів у структурі механізмів захисту інформаційної безпеки призведе до вкрай негативних наслідків у забезпеченні національної безпеки як найвищої мети для фізичного існування суверенної держави.

В. П. Горбулін та М. М. Биченок, досліджуючи проблем и інформаційного середовища України, у монографічному дослідженні [156] акцентують увагу на необхідності тісного поєднання науки і практики. Науковці зазначають, що несформованість у суспільній думці і науковому середовищі цілісного бачення інформаційної безпеки з позиції права і юридичної науки виступає однією з основних причин невідповідності інформаційного законодавства України вимогам сьогодення.

Для розв'язання завдання нашого дослідження ми абстрагуємось від буквального розуміння наведеного у попередніх абзацах визначення і зупинимося на детальному вивченні джерел загроз соціального і техногенного походження, які є найбільш дотичними до інформаційної сфери.

Розглядаючи джерела загроз інформаційній безпеці з позицій соціальної природи, потрібно усвідомлювати їх рівень масштабування (зовнішнє втручання чи внутрішнє походження) як інструментарій впливу на суспільну думку, її

формування і утвердження, чи намір завдати шкоди інформаційній системі як матеріальному, захищеному об'єкту, який регулюється відповідними нормами права і положеннями підзаконних нормативно-правових актів.

На нашу думку, до зовнішніх ознак проявів джерел загроз інформаційній безпеці можна віднести:

- діяльність закордонних центрів дезінформації і перенесення цієї інформації на максимальну кількість споживачів;
- намагання окремих країн здобути перевагу в інформаційному просторі з метою викривлення, спотворення чи пошкодження баз даних та інших відомостей з метою отримання домінуючих позицій на міжнародних інформаційних майданчиках;
- заходи, спрямовані на заволодіння новітніми технологічними інструментами як засіб потенційного перехоплення ініціативи на конкретних напрямках (оборонний, комерційний тощо);
- терористичні загрози та підривна діяльність закордонних організацій;
- технологічна експансія з боку закордонних комерційних та інших структур на фоні послаблення впливу України на глобальну інформаційну мережу з причин російської військової агресії;
- поширення відомостей стратегічного характеру, що завдають шкоди національній безпеці України, отриманими різноманітними засобами, у тому числі супутниками-шпигунами тощо;
- кібервійна та інформаційна війна як джерела загроз, що завдають шкоди усім сферам життєдіяльності суспільства шляхом застосування інструментів знищення, спотворення чи викрадення інформації, насамперед національній безпеці.

Внутрішні характеристики джерел загроз інформаційній безпеці є дещо відмінними від тих, що посягають на встановлене інформаційне поле України з-

поза територіальних меж держави, оскільки своїми витокami пов'язані з недосконалістю, недієвістю, подекуди застарілістю легітимізованих інструментів, що забезпечують організацію з упорядкування і захисту інформації всередині країни. До таких джерел доцільно віднести:

- проблеми економічного розвитку, у зв'язку з чим має місце недостатнє фінансове забезпечення заходів із забезпечення інформаційної безпеки;
- неконкурентоздатний рівень інформатизації основних галузей, що є наслідком загального стану економіки;
- прогалини у сфері нормативно-правового регулювання відносин інформаційного середовища, що є чинником підвищеного зловмисного інтересу до оволодіння інформацією з метою збагачення чи завдання іншої шкоди;
- послаблена увага за вивченням особистих даних кандидатів перед призначенням на посади, пов'язані з розпорядженням інформацією, насамперед з обмеженим доступом, а також ефективний контроль за працівниками, які обіймають зазначені посади;
- поширення кримінальних зв'язків серед осіб, управнених на доступ і розпорядження інформацією, їх підкуп, шантаж та інші дії з метою схилити їх до злочинної співпраці та порушення професійного обов'язку;
- недостатня координуюча і організуюча роль центрального органу влади, відповідального за реалізацію політики у сфері забезпечення інформаційної безпеки;
- недостатній розвиток інформаційного середовища, що є підґрунтям для зловживань у сфері інформаційної безпеки.

Представлена авторська класифікація зовнішніх і внутрішніх загроз у сфері забезпечення інформаційної безпеки не є вичерпною і ми її розглядаємо як привід для подальшої наукової дискусії.

При класифікації джерел загроз інформаційній безпеці необхідно вирізняти дві категорії чинників: суб'єкти (дії чи бездіяльність особи) і об'єктивні прояви (хакери, злочинці, конкуренти, корупціонери, наділені повноваження щодо доступу до інформації представники органів державної влади та місцевого самоврядування. Уніфікованою метою практичного результату виникнення і застосування протиправних і заборонених дій у галузі інформаційної безпеки є завдання матеріальних збитків і моральної шкоди об'єкту посягання, яким є суспільні відносини у сфері інформації.

Більш глибоке розуміння ролі суб'єкта інформаційних відносин як джерела загрози інформаційній безпеці знаходимо у науковому доробку В. А. Нехай. Науковець зазначає, що потенційними збудниками протиправного використання інформаційного контенту з боку особи можуть бути: несанкціонований доступ до інформації, що зберігається в системі; заперечення дій, пов'язаних із маніпулюванням інформацією; введення в програмні проекти і продукти «логічних пломб», які спрацьовують за виконання певних умов або після закінчення певного періоду часу і частково або повністю виводять з ладу комп'ютерну систему; розроблення в поширення комп'ютерних вірусів та інші [157].

Колектив науковців, серед яких Ю. Є. Максименко, В. М. Желіховський, В. А. Ліпкан [89], вирізняють «загрози порушення конфіденційності». До таких небезпек, на їх думку, слід віднести: «витік» інформації з встановленим порядком використання, несанкціонований доступ до інформаційних ресурсів, порушення цілісності, модифікація, пошкодження, заміна даних, а також вчинення дій, що утруднюють доступ до інформації чи використання інформаційних ресурсів.

Висловлені судження знайшли підтримку у науковому доробку (термінологічний довідник словник з інформаційної безпеки) таких науковців, як В. М. Богуш, В. Г. Кривуца та А. М. Кудін [158].

Окремі аспекти як прояви джерел небезпек для інформаційного поля України знаходимо у доробку В. Петрика, який визначає загрози національній безпеці в інформаційній сфері як сукупність умов та чинників, які становлять небезпеку життєво важливим інтересам держави, суспільства і особи через можливість негативного інформаційного впливу на свідомість та поведінку громадян, а також на інформаційні ресурси та інформаційно-технічну інфраструктуру [159].

З наведеного судження робимо висновок, що першопричинами тривожних ознак неправомірного втручання у встановлений порядок користування інформацією можуть стати шкідливий інформаційний вплив, закладений в продукований контент, імплементовані у вітчизняний інформаційний простір ворожі медіаресурси, якими закладаються у свідомість людини зрадницькі і капітулянтські кліше, нав'язуються негативні для нашого середовища стереотипи мислення тощо.

Подібних думок дотримується Р. Р. Марутян [160], який вважає, що здійснення іноземними державами негативного інформаційно-психологічного впливу на суспільну свідомість громадян України та світову громадськість через проведення інформаційних акцій та кампаній, спеціальних інформаційних операцій є найсуттєвішою загрозою національній безпеці України в інформаційній сфері. Такий результат досягається шляхом систематичного поширення неповної, упередженої чи тенденційної інформації про стан справ в Україні, її політичному чи суспільному житті.

А. І. Марущак, досліджуючи джерела загроз інформаційній безпеці за ознаками природи походження [161], висловлюється про їх зовнішню і

внутрішню природу. До зовнішніх загроз науковець відносить злочинні угруповання і формування, а також несумлінних конкурентів. Серед внутрішніх джерел вбачаються адміністративний і технічний персонал підприємства, установи, організації, що мають можливість спричинити шкоду юридичній особі шляхом порушення встановленого порядку використання інформації.

Дане судження поглиблюється висновками О. А. Євтушевської, яка основні загрози для інформації як об'єкта правового захисту вбачає в розголошенні, витоку і несанкціонованому доступі до її джерел [162, с. 159].

Колектив науковців у складі К. А. Кононенка, Б. Парахонського та Г. Яворської дійшли порозуміння у тому, що між джерелами виникнення і способами виявлення внутрішніх і зовнішніх загроз існує тісний обопільний зв'язок і саме такий порядок взаємозалежності є загрозливим для стану національної безпеки [163, с. 30].

Л. В. Борисова і В. В. Тулупов [164, с. 40] здійснили теоретико-практичний аналіз проєкту Концепції міжнародної інформаційної безпеки. За висновками науковців, які співзвучні з поглядами інших вчених, необхідно вирізнити транскордонну сферу як одне з джерел загроз інформаційній безпеці. Такі загрози матимуть місце при переміщенні інтелектуальних ресурсів через кордон, а саме вивезенні відомостей, що мають унікальний науково-технологічний характер, і якими володіють спеціалісти, аналітична та інша інформація щодо прогнозування тенденцій розвитку в інших державах для отримання несанкціонованого доступу до відомостей конфіденційного змісту і баз даних.

Теоретико-правовий та методологічний аналіз комплексу чинників, які безпосередньо чи побіжно торкаються сфери інформаційної безпеки показав, що як складова національної безпеки ця сфера відповідно до сучасного розвитку її теорії в узагальненому вигляді ґрунтується на таких базових елементах: національні інтереси – загроза – захист [165, с. 8]. Тобто, як зазначає науковець,

джерела загроз є підставою для застосування механізмів захисту відповідно до виявленої першопричини і рівня потенційної шкоди.

На думку Т. О. Гуржій, на практиці аналіз викликів – це завжди суб'єктивний процес сприйняття суб'єктом певних факторів через призму власних інтересів і професійності. Фахівці називають важливий компонент гібридної війни – вторгнення в інформаційно-комунікаційний простір певної країни з метою придушення опору та формування світового політичного стандарту, узгодженого з інтересами агресора. Для цього використовуються найрізноманітніші інструменти маніпулювання громадською думкою: втручанням у функціонування інформаційно-телекомунікаційних систем і мереж; розвиток кіберзлочинності; вплив на засоби масової комунікації та маніпуляція суспільною думкою [166, с. 18].

Б. А. Кормич вбачає джерела загроз інформаційній безпеці у недостатній захищеності спеціальних технічних засобів і недосконалості застосовуваних технологій. У цьому зв'язку науковець висловлюється про те, що основні дії щодо збирання, передачі та розповсюдження інформації здійснюються за допомогою спеціальних технічних засобів і технологій. Відповідно з розвитком науки і техніки ці інформаційні засоби та технології перетворилися на один з найважливіших компонентів інформаційних процесів, одночасно із самою інформацією і суб'єктами інформаційних відносин [167, с. 322].

Дослідження джерел загроз інформаційній безпеці не буде повним і довершеним без обґрунтування нормативно-правовими актами, якими встановлюються загороджувальні заходи превентивного характеру. При цьому беремо до уваги, що ґрунтовне вивчення законодавчої бази нами здійснено в попередніх підрозділах, що виключає повторне звернення до положень галузевих законів. Тому зосередимося на висвітленні сутності підзаконних актів,

якими передбачено організаційно-практичні заходи з недопущення протиправного втручання в інформаційне середовище України.

З метою надання актуальності цій науковій розвідці вибірково проаналізуємо крайні передвоєнні документи, а саме окремі Укази президента України з означеного питання:

- уведена в дію Указом Президента України від 14 вересня 2020 року № 392/2020 Стратегія національної безпеки України визначає одним із напрямків протидії загрозам у сфері інформаційної безпеки «посилення спроможностей національної системи кібербезпеки для ефективної протидії кіберзагрозам у сучасному безпековому середовищі[168];

- уведена в дію Указом Президента України від 28 грудня 2021 року № 685/2021 Стратегія інформаційної безпеки визначає актуальні виклики та загрози національній безпеці у сфері обігу та поширення інформації, окреслює стратегічні цілі та завдання, спрямовані на нейтралізацію таких загроз, і посилення захисту інформаційної сфери України [169]. Особливістю аналізованого нормативно-правового акту є те, що ним уперше здійснено офіційне розмежування джерел загроз інформаційній безпеці на глобальні і національні;

- уведена в дію Указом Президента України від 26 серпня 2021 року № 447/2021 Стратегія кібербезпеки України позиціонує кіберпростір як джерело небезпеки глобального масштабу і вказує на те, що пріоритетними цілями для кібертерористів були і залишаються об'єкти атомної енергетики, електро- та водопостачання, сфери електронних комунікацій, фінансової та банківської сфери, авіаційного та залізничного транспорту, сховищ стратегічних видів сировини, хімічні й біологічні об'єкти тощо [170].

Аналітико-правове дослідження документа показало, що у державі розуміють деструктивне значення неконтрольованого чи послабленого підходу

до сфери захисту інформаційного простору. При цьому виокремлюються нові джерела загроз, які призводять до гібридної агресії (кібервійна), кібертероризму, кіберзлочинності, кібершпигунства.

На думку Л. С. Любохинець та О. В. Поплавської, «забезпечення доступності, цілісності й конфіденційності кіберпростору стало однією з глобальних проблем XXI ст., метою ефективного функціонування держави, економіки та суспільства загалом» [171, с. 95].

Здійснений колективом науковців (С. В. Онищенко та С. С. Білько) теоретико-правовий аналіз нормативно-правового регулювання сфери інформаційної безпеки [172, с. 52, 53] підтвердив відсутність ґрунтовної систематизації загроз. На їх думку, підґрунтям для формування шляхів протидії, недопущення та максимального зменшення деструктивного і шкідливого впливу від їх реалізації може стати модернізована багаторівнева класифікація джерел загроз у сфері інформаційної безпеки.

Обравши положення аналізованих Стратегій як підґрунтя для своїх висновків, науковці здійснили систематизацію джерел загроз інформаційній безпеці у розрізі протиправних зазіхань на національну безпеку України, зокрема й на кіберпростір як на найбільш уразливу складову інформаційної безпеки. До загроз у сфері інформаційної безпеки науковці відносять:

- глобальні, а саме: збільшення кількості міжнародних інформаційних кампаній, загрози з боку російської федерації у галузі інформаційної політики, соціальні мережі як суб'єкти впливу в інформаційному середовищі, недостатній рівень медіаграмотності (медіакультури) в умовах стрімкого розвитку інформаційних технологій;

- національні, а саме: обмежені можливості реагувати на дезінформаційні кампанії, не сформованість системи стратегічних комунікацій, недосконалість регулювання правовими інструментами відносин у сфері інформаційної

діяльності та захисту журналістів при здійсненні ними професійних обов'язків, недостатній рівень інформаційної культури населення для протидії маніпулятивним та інформаційним впливам, ускладнений доступ до інформації на місцевому рівні [172, с. 52, 53].

Якщо з більшістю наведених висновків науковців можна погодитись, то окремі з них, як, наприклад, ускладнений доступ до інформації на місцевому рівні, видається надто дискусійним, адже кожному доступні інтернет технології і з їх допомогою можна отримати будь яку інформацію (додаток «ДІЯ», пошукові системи тощо).

Наступне. Логіко-правова оцінка наведеної систематизації джерел загроз інформаційній безпеці засвідчує про певне порушення вимог щодо упорядкованості і коректної послідовності викладення думок. Так, аналізуючи окремі види джерел небезпек для інформаційного середовища України, спостерігаємо недостатньо аргументоване перенесення елементів з категорії «глобальні загрози» до категорії «національні загрози». Йдеться про деструктивний вплив інформаційних російських ресурсів, а також різнопланове маніпулювання поняттями, вирізняючи роль медіапростору, низький рівень медіакультури населення тощо. Такий підхід до систематизації джерел загроз інформаційній безпеці не може бути повністю прийнятним для розуміння першопричин зловмисних посягань на встановлений порядок нормативно-правового регулювання сфери інформації в Україні, а також організації і провадження профілактико-превентивних заходів на всіх напрямках її нейтралізації чи мінімізації їх впливу.

З урахуванням актуальності зазначеної проблеми ми долучаємося до створення класифікації джерел загроз інформаційній безпеці України, яку розглядаємо в декількох аспектах, а саме: загрози, які мають глобальний характер, національні (внутрішньодержавні) загрози і локальні загрози.

У цьому разі доцільно дослухатися висновків М. А. Еделєвої, яка стверджує, що «...розвиток інформаційних технологій, що необхідні для накопичення й ефективного використання інформаційних ресурсів, стає стратегічним чинником забезпечення національної безпеки [173].

До джерел глобальних загроз відносимо міжнародні інформаційні ресурси з ворожим і недружнім контентом (насамперед з боку російської федерації), недостатній рівень захоплення міжнародного інформаційного простору вітчизняними медіаресурсами, недостатній ступінь легітимними інструментами правового і технологічного захисту інформаційного простору України, насамперед інформації з обмеженим доступом.

Національні (внутрішні) джерела загроз вбачаємо у недосконалості нормативно-правового регулювання сфери інформаційної безпеки, недостатній рівень медіаобізнаності населення України, занижений поріг резистентності шкідливим ресурсам, представленим у соціальних мережах та інших каналах впливу на окремі прошарки суспільства і в цілому на населення держави, уразливість інформаційної сфери з причин вчинення протиправних дій особами, управненими на володіння, розпоряджання і зберігання інформації, недостатня роль засобів масової інформації на напрямках виховання у населення достатнього рівня інформаційної гігієни.

Локальні (місцеві) джерела загроз інформаційній безпеці полягають, на наше переконання, в діях, спрямованих на розпалювання національної нетерпимості і ворожнечі на підґрунті мови, місцевих традицій, перекручування і переоцінка офіційної інформації з метою поширення панічних і капітулянтських настроїв, незадоволення політикою держави в цілому або окремих її складових тощо.

Все, зазначене вище, спонукає до поєднання зусиль усіх суб'єктів, що входять до структури національної безпеки України, з метою досягнення

максимально високого рівня убезпечення масивів даних від протиправного зазіхання на їх цілісність і порядок роботи з ними. У цьому зв'язку доцільно дослухатися до Н. С. Оніщенко, яка зазначає: «умови існування можуть виступати стимулом розвитку здатностей та підвищення спроможності суб'єкта, що, у свою чергу, надає йому можливість впливати на умови свого існування з метою їх покращання. До таких умов можна віднести і потенційні загрози, рівень яких не дестабілізує діяльність суб'єкта, а навпаки спонукає до розвитку. Тоді завданням «мінімум» для держави стає створення загальних мінімальних умов, що забезпечать саморозвиток і самореалізацію індивідів» [174].

На нашу думку, державним будівничим нагально потрібно працювати на «максимум», щоб створити настільки безпечні умови у сфері інформації та інформаційних технологій, при яких у зловмисників не виникало би спокуси випробувати дієвість профілактично-превентивних механізмів державного примусу.

Представляючи авторську класифікацію джерел загроз інформаційній безпеці, усвідомлюємо, що вона не є бездоганною і викличе дискусію у науковому середовищі. Саме такого результату ми домагаємося задля вироблення єдиної системи у підходах до комплексного розуміння значення особливо небезпечного напрямку впливів на психологічне здоров'я народу України і збереження надійно захищеним інформаційного простору держави – джерел загроз інформаційній безпеці.

3.2 Досвід інформаційної безпеки в країнах Європи

Юридичний аналіз практики європейських країн у побудові власних моделей правового забезпечення інформаційної безпеки, протидії кіберзагрозам, а також дослідження низки ряду міжнародних правових документів дає змогу

зробити висновок про відсутність єдиної союзної моделі правового забезпечення інформаційної безпеки.

Авторське дослідження показало, що Європейський Союз проводить активну політику у сфері забезпечення інформаційної безпеки, законодавство якого об'єднує розвинуті країни, котрі відчутно впливають на організацію та становлення міжнародних відносин, встановлюючи правове регулювання і стандарти поведінки держав-учасниць у політичній, економічній, соціальній, інформаційній та інших сферах.

Завдання щодо забезпечення інформаційної безпеки були розроблені в 1991 році і знайшли відображення у «Європейських критеріях безпеки інформаційних технологій» (Information Technology Security Evaluation Criteria (ITSEC) [175]. Для країн-підписантів (Німеччина, Великобританія, Нідерланди, Франція) визначено конкретні заходи, зокрема: убезпечення носіїв інформації від протиправного доступу з метою забезпечення належного рівня конфіденційності; гарантії щодо безмодифікаційного використання чи знищення інформаційних ресурсів через створення ефективних механізмів захисту; досягнення автономності інформаційних систем у разі відмови у їх підтримці та обслуговуванні.

Наступним кроком стало прийняття у 1996 році стандартів європейської інформаційної безпеки, які знайшли своє відбиття у «Єдиних критеріях безпеки інформаційних технологій» [176].

Ю. В. Нестеряк, характеризуючи наведений документ, зазначає: «У цьому документі застосовано модель тріади CIA (CIA Triad), яка передбачає такі основні характеристики інформаційної безпеки:

- а) конфіденційність;
- б) цілісність;
- 3) доступність» [177, с. 43].

Для країн Європейського Союзу 2001 рік відзначився прийняттям Європейською Комісією документа під назвою «Мережева та інформаційна безпека: європейський політичний підхід» [178], яким визначено базові засади Співтовариства у підходах до проблем, пов'язаних з забезпеченням захисту інформації.

Словосполучення як ознака створення нового терміну «мережева та інформаційна безпека» пояснюється «як здатність мережі або інформаційної системи чинити опір випадковим подіям або зловмисним діям, котрі становлять загрозу доступності, автентичності, цілісності та конфіденційності даних, що зберігаються або передаються, а також послуг, які надаються через ці мережі й системи [178].

Згаданий документ визначає пріоритетні напрями європейської політики на напрямках організації заходів у сфері інформаційної безпеки, серед яких: розвиток міжнародного співробітництва з питань інформаційної безпеки; створення європейської системи попередження та інформування про нові загрози; забезпечення технологічної підтримки; підвищення медіаосвіченості користувачів про потенційні загрози при використанні комунікаційних мереж; зміцнення інформаційної безпеки на державному рівні шляхом упровадження ефективних і сумісних засобів забезпечення інформаційної безпеки та заохочення використання країнами-членами електронних підписів під час надання державних онлайн послуг; правове забезпечення, пріоритетами якого є захист персональних даних, регламентація телекомунікаційних послуг та протидія кіберзлочинності; підтримка ринково орієнтованої стандартизації та сертифікації тощо.

На підставі наведеного вище необхідно зазначити, що всіма країнами ЄС приділяється особлива увага проблемам правового забезпечення інформаційної безпеки. Водночас, значної актуальності як завдання, що потребують негайного

вирішення, набувають проблеми боротьби з кібезагрозами як складовими діяльності з забезпечення інформаційної безпеки.

З 1999 року впроваджуються програма «Безпечніший Інтернет» (Safer Internet) [179], у межах якої здійснюється профілактика, поряд з протидією шкідливому наповненню, протиправна і небезпечна поведінка при користуванні інформаційними ресурсами.

Теоретико-правовий аналіз нормативної бази Європейського Союзу на напрямках формування європейської глобальної системи правового забезпечення інформаційної безпеки показав послідовний і поступальний характер такої діяльності. Ще в 2007 році Європейська Комісія ухвалила документ «На шляху до загальної політики у сфері боротьби з кіберзлочинністю» [180], в якому задекларовано підходи до оцінки кіберзлочинів як кримінально карані діяння, що вчинені з протиправним використанням інформаційних систем та комунікаційних мереж і поєднані з усталеними складами злочинів, як, наприклад, публікація незаконного контенту, шахрайство з використанням інформаційно-телекомунікаційних мереж, хакерство, Ддос атаки (DDoS attack).

Головні виклики та проблеми, які потребують першочергового реагування зі сторони країн ЄС, були у 2009 році оприлюднені у Повідомленні Європейської комісії «Захист Європи від широкомасштабних кібератак та руйнувань: посилення рівня підготовленості, безпеки та стійкості» [181]. Указаним документом визначено також низку заходів на напрямках підвищення рівня захисту європейської критичної інфраструктури і здатності ефективно протидіяти зовнішнім інформаційним загрозам.

Важливим аспектом правового забезпечення інформаційної безпеки у рамках ЄС є питання інформаційної відкритості органів державної влади країн-учасниць. У цьому зв'язку аналізованим документом позитивно оцінюється діяльність, спрямована на повномірне інформування населення:

«...загальноновизнано, що демократична система може функціонувати найбільш ефективно лише у разі, коло громадськість повністю поінформована» [182, с. 110].

Гарантування припустимої участі всіх у суспільному житті необхідно забезпечити, проте мають бути покладені певні обмеження у доступі до інформації, яка мається у розпорядженні органів державної влади. Такі положення закладені в рекомендації Ради Європи № R(81)19 «Про доступ до інформації, яка перебуває у розпорядженні державних органів» [183].

Інтернет, як глобальна і доступна мережа, а також потужний розвиток інформаційно-комунікаційних ресурсів, резолюцією Генеральної Асамблеї ООН «Право на приватність у цифрову епоху» від 18.12.2013 р., поряд з беззаперечними перевагами, несуть у собі загрози протиправного заволодіння персональними даними.

Даним документом підсилено підходи до захисту приватності незалежно від того, як відбувається комунікація: офлайн чи онлайн [184].

На думку С. Л. Гнатюк, засади захисту персональних даних у правовій практиці країн ЄС можна звести до такого: пріоритетність права особи розпоряджатися своїми персональними даними; використання персональних даних без дозволу володільця тягне відповідальність згідно з законодавством; для будь-кого, хто здійснює користування персональними даними фізичних осіб з їхнього дозволу, встановлено відповідальність у разі умисного розголошення цих даних третім особам (крім випадків, коли на це надано дозвіл) [185, с. 5–6].

Окрім вищенаведених документів ЄС про захист персональних даних, необхідно проаналізувати положення директиви 95/46/ЄС «Про захист фізичних осіб у контексті обробки персональних даних і вільного обігу таких даних» [186]. Директивою утверджується необхідність забезпечити вільний обіг інформації між країнами ЄС з одночасною гарантією ефективного захисту прав

громадян щодо недоторканності їх особистих даних та недопущення протиправного заволодіння ними третіми особами.

Кожну державу-учасницю ЄС Директива зобов'язує ухвалити свої національні закони про захист персональних даних, які б співвідносилися з рекомендаціями OECD 1980 року. Особливу увагу серед аналізованих зосереджуємо на «Принципах гарантованої безпеки №11» [187]. Згідно з наведеним положенням вимагається, щоб «персональні дані були захищені розумними засобами безпеки від таких загроз, як утрата чи неавторизований доступ, руйнування, використання, модифікація або розголошення». Зазначені правила захисту персональних даних (GDPR), ухвалені 14.04.2016 року, набули чинності у 2018 році.

Важливою обставиною є те, що порядок захисту приватних відомостей не обмежується національними рамками конкретної країни, а розповсюджується на суб'єктів інших держав, які співпрацюють з країною-підписантом Декларації.

Аналізуючи зазначений документ, Д. П. Василенко та В. І. Маслак указують, що ним «доопрацьовані і розширені цивільні права користувачів, відповідальність за схоронність даних, а також запроваджено деякі обмеження переміщення даних між країнами. Слід констатувати, що країни ЄС сформували «в певному сенсі злагоджену систему захисту інформації» [188, с. 129].

Т. Ю. Ткачук, розглядаючи проблеми правового забезпечення інформаційної безпеки України при здійсненні євроінтеграційних процесів, дійшов висновку, що «кожна країна має свої закони, положення, інструкції щодо врегулювання питань інформаційної безпеки [189, с. 269].

Вибіркове науково-практичне дослідження законодавства окремих держав Європейського Союзу, а також Великобританії, засвідчило наявність національних особливостей на напрямках дотримання положень із захисту інформації. Проте необхідно зазначити, що такі особливості повномірно

кореспондуються з загальним порядком, встановленим директивними документами ООН і ЄС.

Вивчення національного законодавства Великобританії у сфері інформаційної безпеки показало, що впродовж останніх років керівництво держави доклало чимало зусиль для систематизації нормативно-правової бази у зазначеній сфері. Прикладом такої роботи є планове здійснення реформ у системі права Великобританії в напрямку його рекодифікації (консолідація нормативно-правових актів у різноманітних правових сферах).

Великобританія, визначаючи межі правового регулювання інформаційної безпеки, ухвалила національну програму «The Government's Policy for the Information Age» [190, с. 98]. Даним документом передбачено поглиблений розвиток електронної комерції з метою забезпечення зростання економічного сектора, розширення телекомунікаційного ринку, поширення інформаційно-комунікаційних технологій в усі сфери життя суспільства.

Визначальною рисою інформаційної політики Англії політики виступає завдання щодо створення регіональних мереж і супермагістралей з метою удосконалення і підвищення ефективності між місцевим і міжнародним рівням и науково-технічної співпраці [191, с. 97–98].

У Великобританії діє Закон про захист даних, яким здійснюється контроль за тим, як використовуються персональні дані людини підприємствами, організаціями або державними органами. Кожному, управненому на використання персональних даних людей, покладено за обов'язок неухильно дотримуватись правил, які охоплюються «принципами захисту даних».

Користувачі мають переконатися, що інформація: справедливо, законно і прозоро використовується для визначених, явних цілей; зберігається не довше, ніж це потрібно; обробляється таким чином, що забезпечує відповідну безпеку,

включаючи захист від незаконної або несанкціонованої обробки, доступу, втрати, знищення або пошкодження [192].

Схвалена Великобританією Стратегія кібербезпеки визначила значний перелік цілей, дій та показників, які відображаються у трьох важливих розділах: 1. Захист: Уряд зміцнить власні засоби захисту інформації та працюватиме з промисловістю, щоб забезпечити захист британських мереж, даних і систем від кіберзагроз. 2. Утримання: Велика Британія зміцнить спроможність правоохоронних органів збільшити вартість кіберзлочинності. Розвиток: Уряд допоможе розвивати критичні можливості Великобританії, включаючи кібернавички, а також зростаючу індустрію кібербезпеки країни, щоб не відставати від кіберзагроз [193].

У контексті вищенаведеного доцільно здійснити посилання до положень Угоди між Україною та Сполученим Королівством Великої Британії і Північної Ірландії про політичне співробітництво, вільну торгівлю і стратегічне партнерство, в якій статтею 374 зазначено напрямки такого співробітництва, а саме:

- а) обмін інформацією, найкращими практиками, досвідом та передачею морського ноу-хау, зокрема інноваційних технологій у морській галузі;
- б) обмін інформацією й найкращими практиками щодо можливостей фінансування проєктів, зокрема щодо державно-приватного партнерства [194].

Квінтесенцією сказаного на адресу позитивного впливу Стратегії на стан дотримання достатнього рівня безпеки в інформаційній сфері є положення про те, що Великобританія буде працювати на міжнародному рівні, продовжуватиме відігравати важливу роль у зміцненні потенціалу глобальної кібербезпеки і використовувати свій вплив у багатосторонніх організаціях, таких як Європейський Союз і НАТО [195].

Як поточний підсумок зазначимо, що Великобританія під час провадження політики у сфері інформації має на меті покращання умов конкурентної боротьби у цій сфері, підвищення якісних характеристик інформаційних послуг, а також упровадження новітніх інформаційних технологій у сферу державного управління.

Запроваджені Іспанією заходи у сфері інформаційної політики можна умовно розділити на три основні напрямки: законодавство про інформацію; дії, спрямовані на заохочення та просування використаної інформації; заходи щодо поліпшення управління інформаційними ресурсами в державних адміністраціях.

Іспанія, як будь-яка країна Західної Європи, створила складну систему законів, що регулюють відносини в інформаційній сфері. Як правило, ці закони забезпечують право громадян на інформацію, що має підґрунтям Конституцію Іспанії 1978 року.

Здійснений аналіз системи інформаційного законодавства Іспанії показав, що воно значно відрізняється від аналогічного нормативного середовища США й більшості європейських країн, оскільки не передбачає узагальненого плану для становлення інформаційного суспільства. Водночас, відсутність загального формалізованого планування не завадило урядовим установам вживати адекватні ситуації заходи на напрямках захисту інформаційного простору держави.

Серед найважливіших заходів необхідно вказати План національних наукових досліджень та технологічного розвитку, відповідно до якого у забезпечення інформаційної безпеки країни, починаючи з 1986 року, інвестовано значні асигнування.

Наступним документом є Національна стратегія кібербезпеки, який слугує для іспанського уряду основою щодо розроблення Стратегії національної безпеки[196], метою якої є запобігання кіберзагрозам, захист, виявлення, реагування та відновлення інформаційного простору.

Країни Балтії, зокрема Естонія, запровадила цифрову програму 2020, якою передбачено використання інформаційно-комунікаційні технології (ІКТ) у різних сферах життя. Кінцевою метою таких заходів є збільшення економічної конкурентоспроможності, добробуту людей та ефективності державного управління. Стратегія визначає різні заходи та дії для досягнення цієї мети, зокрема завершення роботи широкопasmової мережі; у майбутньому електронні послуги стануть все більш транскордонними; 20% активного населення Європейського Союзу має користуватися цифровими технологіями; Естонія почне надавати свої безпечні послуги громадянам інших країн; сприяння репутації Естонії як центру інновацій та розвитку інформаційного суспільства [197].

З метою уникнення вразливості власного кіберпростору Естонія ухвалила національні стратегії кібербезпеки. Це було пов'язано зі значним розширенням спектру і переліку сервісних послуг та запровадженням новітніх технологічних інструментів у сфері інформації.

Внутрішні процедури, правове регулювання та інституції для забезпечення ефективного розподілу співпраці між установами було відображено в першому документі. Друга стратегія скерована на захист критичної інфраструктури від протиправних посягань, протидію кіберзлочинності та інших заходів для покращання інформаційної сфери. Паралельно з цими процесами було ухвалене національне законодавство для ефективного розвитку сектору кібербезпеки та міжнародного співробітництва у сфері захисту інформації.

Становлення сфери захисту інформаційної безпеки Німеччини має давню історію. Перші законодавчі заходи Федеральної влади Німеччини щодо захисту інформації та інформаційних ресурсів сягають 70-х років минулого століття і пов'язані із убезпеченням особи від протиправних посягань на її особисту

безпеку, неприпустимість невмотивованого втручання в приватне життя людини шляхом маніпулювання персональними даними.

Правові основи забезпечення інформаційної безпеки Німеччини формувались з середини 1980-х років і відбувались паралельно з європейськими процесами. З того часу сфера інформаційної безпеки, з урахуванням численних директив Євросоюзу та національного законодавства, стала однією з найскладніших галузей права.

Основним принципом провадження інформаційної безпеки в Німеччині є заборона будь-якого використання інформації. Таким чином, незаконним вважається зберігання, передача чи зміна інформації. Виключення з встановленого порядку є те, що використання інформації дозволено в конкретно передбачених випадках.

Водночас, інформаційна політика ФРН включає концепцію вільного транскордонного обміну інформацією, вільного відбиття підходів, підвищення рівня інформаційних систем і комунікаційних мереж, сприяння вільній конкуренції у сфері інформації, забезпечення оновлених інструментів правового регулювання інформаційної сфери на основі позитивних змін у німецькому суспільстві, у політичній, економічній та інших сферах.

Нові політичні пріоритети, медіа-концентрація, упровадження сучасних технологій в організацію федерального й місцевого управління набули продовження у Програмі федерального уряду Info-2000 (Germany's Way the Information Society) («Німецький шлях до інформаційного суспільства»), ухваленій у 1996 році [190, с. 99].

З урахуванням вектору розвитку інформаційного бізнесу вироблено нову стратегію національної інформаційної політики ФРН, головними напрямками якої визначено формування інформаційного суспільства, створення інформаційної економіки, розвиток нових інформаційних супер магістралей, запровадження і

поширення інформатизації у сфері державного управління, лібералізація телекомунікацій, підтримка вітчизняного виробника електронної галузі, одночасний розвиток державного і приватного інформаційного бізнес середовища.

Концепція інформаційної безпеки ФРН визначає низку заходів, які, не дивлячись на їх відкритість і деяку ліберальність, повномірно виконують покладені завдання щодо транскордонного обміну інформацією, забезпечення свободи совісті та слова, розвитку інформаційно-комунікаційних технологій і телекомунікаційних мереж. Значна увага приділяється створенню конкурентного середовища у сфері інформації при суворому правовому регулюванню відносин цієї сфери [198, с. 40].

У 1977 році ухвалено Закон ФРН «Про захист персональних даних», який, з причини возз'єднання ФРН та НДР у 1990 році в єдину німецьку державу, набув нової редакції, а також через поступове впровадження в німецьких структурах (федеральні, земельні, муніципальні органи, ЗМІ, приватні фірми тощо) автоматизованої обробки такої категорії інформації поруч з картотечною формою [199, с.323].

Прийнятий у 1997 році Закон ФРН «Про основи надання інформаційних та комунікаційних послуг» [200] встановлює стандарти захисту інформації виключно в інформаційно-телекомунікаційних мережах загального доступу.

На рівні законодавства в 2009 році, належно оцінюючи значення захисту інформаційних мереж, об'єктів економіки та інших потенційно вразливих об'єктів ФРН, визначено пріоритетність фізичного та технологічного захисту «критичної інфраструктури» (вперше такий термін застосовано в США у 1998 році).

Превентивно-профілактична реакція на події у зв'язку з кіберзагрозами, координація сил та засобів на напрямках управління процесами і захисту

критичної інформаційної інфраструктури, у тому числі при участі приватного сектору, відповідно до Закону ФРН «Про посилення безпеки інформаційних систем» [201] покладено на Федеральне відомство безпеки інформаційних систем (BSI) ФРН.

Для виконання покладених завдань BSI розроблено, а Федеральним Урядом у 2011 році ухвалено Стратегію забезпечення кібернетичної безпеки ФРН [202], яка є головним доктринальним документом ФРН у сфері забезпечення захисту інформаційної інфраструктури держави від кібератак і хакерських нападів.

Концептуально визначено ряд протиправних проявів у сфері кібербезпеки, окреслено загрози інформаційній інфраструктурі з боку кіберзлочинців, можливі об'єкти та суб'єкти, на які потенційно зазіхають порушники, передбачено організаційно-практичні заходи з протидії порушенням встановленого порядку користування інформацією та інформаційними ресурсами, посягання, а також організаційні засади протидії протиправним проявам. Визначено роль і значення співпраці з приватними особами та міжнародними структурами.

Посилаючись на зміст аналізованого правового акту, наводимо основні напрямки, визначені Стратегією забезпечення кібернетичної безпеки ФРН, а саме: захист критично важливих інформаційних інфраструктур; захист ІТ-систем і Німеччині; посилення інформаційної безпеки в державному управлінні; створення національного центру кіберреакції; створення національної ради з кібербезпеки; проведення ефективного контролю за злочинністю у кіберпросторі; проведення ефективних скоординованих дій для забезпечення кібербезпеки в Європі і в усьому світі; використання надійних інформаційних технологій; розвиток персоналу у федеральних органах влади; інструменти для реагування на кібератаки [203].

Стратегією як один з найважливіших напрямків визначено впровадження цільових пільг і державної підтримки німецьким розробникам сертифікованих засобів захисту інформації, що призначені для масового використання, у тому числі на напрямках дотримання правил поведження з інформацією при обміні каналами електронної пошти [204, с. 28].

Політика Франції у сфері інформаційної безпеки структурно включена до складу «державної стратегії розвитку країни, збереження національної самобутності й ідентичності, є компонентом зовнішньої політики, участі Франції в інформаційних програмах і проектах міжурядових європейських організацій, створення інформаційної економіки та поширення комп'ютерних мереж і систем, інформаційних послуг» [190, с. 100].

Для Франції метою інформаційної політики визначено заходи з реформування законодавства у сфері інформації, підтримка та заохочення наукових досліджень, створення і підвищення ефективності роботи систем безпеки у галузі інформатизації і використання баз даних, протидія та запобігання джерелам загроз інформаційному середовищу держави.

У Програмі розбудови інформаційного суспільства у 1998 році французьким урядом визначено завдання щодо формування інформаційних та комп'ютерних технологій, розроблення системно-цілісних підходів до нормативного, науково-дослідницького, прикладного і зовнішньоекономічного аспектів розвитку глобальної системи інформатизації. Такі заходи мали відбуватися шляхом проведення міжнародних консультацій з проблем уніфікації інформаційно-комунікаційних мереж з урахуванням встановленого порядку щодо захисту приватного життя, обміну даними тощо. Положеннями зазначеної Програми передбачалось також здійснення комплексу заходів щодо покращання рівня обміну інформацією на міжнародному рівні.

Окремо слід відзначити заходи, що вживалися в рамках французької національної стратегії з кібербезпеки. Даним документом покладались такі стратегічні цілі: забезпечити здатність Франції приймати рішення шляхом захисту інформації, пов'язаної з суверенітетом; посилити заходи з протидії порушенням у сфері кібербезпеки; забезпечити безпеку у кіберпросторі [205].

Уряд Республіки Італія при розробленні стратегії у сфері інформаційної політики обрав за пріоритети видозміну органів державного управління на підґрунті впроваджених і таких, що підлягали вдосконаленню інформаційно-комунікативних технологій, забезпечення вільного доступу всіх категорій громадян до використання офіційно доступних відомостей, виконання прогами електронної освіти та продовження комп'ютеризації для державних структур та їх працівників, прозорість документообігу в державі з використанням можливостей Інтернету, а також надання високоякісних послуг інформаційного характеру.

Проте, як зазначають А. Є. Шевченко, О. А. Павлюх та В. А. Санжаров, Італія за всіма параметрами є сучасним суспільством з розвиненою економікою. Проте, на думку італійських фахівців, порівняно з іншими країнами, такими як Франція, Німеччина, Японія чи Канада, вона повільніше впроваджує нові технології та інтегрує їх в економіку [206, с. 80]. Водночас, контроль за виконанням і реалізацією зазначених цілей покладено на Національний центр з питань інформатики при Державній адміністрації (Centro Nazionale per l'Informatica nella PA, CNIPA)

Національний план дій щодо наукових розробок, загального розвитку та зайнятості (2005 р.) є одним з найважливіших документів національної інформаційної політики Італії. В його основу закладено принципи розвитку й постійного зростання послуг інформаційно-комунікаційних технологій, зміцнення інтелектуального потенціалу країни тощо.

Завданнями Національної стратегії кібербезпеки Італії, прийнятої у 2013 році, окрім іншого, визначено: на основі посилення міжнародного співробітництва сприяти і заохочувати культуру кібербезпеки, посилювати заходи з протидії онлайн-злочинності, шкідливій і незаконній діяльності з використанням інформації та інформаційних ресурсів [207].

Основними завданнями інформаційної безпеки у розумінні урядових стратегій визначено контроль за сферою онлайн-послуг, підвищення якості роботи внутрішніх мереж, оцінювання інтелектуальних ресурсів, запровадження програми «Електронний уряд для ефективного федералізму: одне бачення – спільна реалізація», розвиток культури електронного спілкування між державними установами та громадянами, а також на рівні місцевих органів влади [208].

Ухвалений Урядом Італії Національний план із захисту кіберпростору та безпеки інформаційно-комунікаційних технологій визначив пріоритетні напрямки діяльності щодо гарантування безпеки кіберпростору та заходи ефективної протидії джерелам загроз для кіберпростору держави [209, с. 60–70].

Політика Республіки Польща в інформаційній сфері концептуально скерована на розвиток відкритого і вільного суспільства, упровадження засад легального і всеосяжного транскордонного обігу інформації, підтримку незалежних медіаресурсів при дотриманні основоположних прав людини і громадянина. Практичним втіленням правової концепції у сфері інформаційної безпеки є ухвалені наприкінці ХХ сторіччя Закони «Про пошту і телекомунікації», «Про телебачення і радіомовлення», «Про державні відносини з римською католицькою церквою в Республіці Польща». Зазначеними нормативно-правовими актами сформовано вектори інформаційної політики, якими запроваджено технологічні стандарти щодо якості інформаційного зв'язку, форми залучення закордонних інвестицій, а також дозвільні процедури

провадження діяльності у галузі інформаційного забезпечення польських громадян.

З причин значного впливу клерикальної інформації на політичне життя і моральні засади суспільства окремо визначено правові основи впливу церкви на інформаційну сферу та діяльність у медіапросторі Республіки Польща [210, с. 114].

Основне функціональне навантаження у сфері забезпечення інформаційної безпеки Польщі покладено на Агентство внутрішньої безпеки (ABW). За сприяння і участі вказаного органу у 2013 році розроблено Стратегію кібербезпеки Польщі, а також створено Центр криптології при Міністерстві національної оборони з повноваженнями планування та проведення кібероперацій, здійснення інших профілактико-превентивних заходів щодо захисту сфери інформаційної безпеки держави [211].

З метою належного реагування на комп'ютерні інциденти Агентством внутрішньої безпеки сформовано урядову команду (CERT) [212]. Її основними завданнями визначено забезпечити і розвивати можливості органів державного управління на напрямках протидії кіберзагрозам.

Окремо розглядаються загрози від зазіхань на інфраструктуру, до складу якої включено ІТ-системи та комп'ютерні мережі, перешкоджання роботі або знищення яких може в значній мірі становити небезпеку для життя людей, їх здоров'я, становити загрозу національним багатствам та навколишньому середовищу, чи спричинити значні фінансові збитки і непередбачувані форсмажорні обставини у діяльності органів державної влади [213].

Для більш чіткого оперування поняттями теорії безпеки, як, наприклад, «загрози», «виклики», «ризики» тощо за сприяння ABW у 2015 році розроблено Доктрину кібербезпеки Польщі [214].

2015 рік для Польщі ознаменувався початком роботи над Доктриною інформаційної безпеки, якою визначено загрози інформаційній безпеці. До джерел загроз встановленому порядку поводження з інформацією документом віднесено: ескалація напруження у міжнародних стосунках; дискредитація польської міжнародної політики і формування негативного іміджу країни на світовій арені, у тому числі й серед союзників по НАТО та ЄС; формування образу Польщі як країни ксенофобів та антисемітів; провокування польсько-литовського конфлікту на тлі польської меншини в Литві; підбурювання польсько-українського конфлікту на складному історичному тлі з можливим застосуванням терористичних замахів, які буцім-то могли би здійснити українці проти поляків чи навпаки. Доктрина інформаційної безпеки Польщі розглядається як виконавчий документ до Стратегії національної безпеки [215].

На цей час залишається актуальною небезпека, джерелом якої є розпалювання ворожнечі між українським і польським народами з використанням медіаресурсів та Інтернету. Як успішний приклад такої взаємодії потрібно назвати створену в 2018 році неурядову організацію – Центр аналізу і пропаганди. Основним завданням створеного Центру є протидія російській пропаганді.

Насправді, зазначена неурядова організація є першою такого роду інституцією у Польщі, діяльність якої спрямовується на розроблення аналітико-пошукових заходів до визначення та припинення російської пропаганди та дезінформації у інформаційному просторі Польщі.

У межах визначених повноважень Центр провадить науково-дослідну та аналітичну діяльність, а також співпрацює з іншими суб'єктами, щоб закласти фундамент розуміння у польському суспільстві загроз, позаяк інформаційна і психологічна війна проникає у різні сфери життєдіяльності суспільства і держави [216].

Необхідно зазначити, що ретроспективний аналіз процесів формування політики інформаційної безпеки країн Європейського Союзу засвідчив про існування однієї спільної риси – необхідності виконання комплексу вимог для вступу до НАТО. Одним із ключових завдань для країн-кандидатів було приведення сфери інформаційної безпеки до вимог високих міжнародних стандартів, що слугувало однією з підстав для позитивного рішення про їх членство у Північно-Атлантичному блоці. Для Республіки Польща таким «екзаменом» було ухвалення Закону «Про захист конфіденційної інформації» [217].

Що стосується Угорщини, та ця країна першою з постсоціалістичних країн, яка прийняла профільний закон у сфері інформаційної безпеки (Про захист інформації про особу та доступ до інформації, що становить суспільний інтерес», запровадивши інститут Парламентського комісара із захисту інформації та свободи інформації» [218]. Дана подія відбулася в 1922 році.

У відповідності до зазначеного закону при необхідності використати персональні дані особи вона має бути повністю ознайомлена про мету таких дій.

Нормами правового акту дозволено збір даних про особу лише в межах тієї необхідності, яка обрамлюється зрозумілою для людини необхідністю. При цьому такі дані могли зберігатися упродовж терміну, який потрібен для вирішення конкретного питання. Будь-хто, чия персональна інформація була піддана обробці, мав право на її виправлення та знищення у разі настання необхідності.

Підвищений статус захищеності надавався персональній інформації, віднесений до розряду чутливих (sensitive) даних, а саме тих, що містять відомості про расове походження, національність, етнічний статус, політичної і партійної приналежності, релігійних чи інших переконань, а також тих, що

стосуються стану здоров'я конкретної особи, сексуальної орієнтації чи судимості.

Крім згаданого закону, Угорщина ухвалила низку дотичних нормативно-правових актів (законів), які стосуються питань, пов'язаних з забезпеченням інформаційної безпеки у різних галузях суспільного життя. Говоримо про Закони «Про обробку і захист медичної інформації та пов'язаних з нею персональних даних» (1997), «Про право на інформаційне самовизначення та свободу інформації» (2011). Охороною прав людини на захист персональних даних від протиправного використання здійснювало Національне бюро із захисту даних та свободи інформації [219].

Більш повний і детальний аналіз вищезгаданих законодавчих актів знаходимо у науковому доробку Т. Ю. Ткачука [220, с. 108].

Для нашого дослідження наукову цінність представляє також ухвалений у 1995 році Закон Угорщини про державні та офіційні секрети, який, як зазначає Ю. Г. Телеховський, був доповнений і виправлений, тобто угорські законотворці адаптували раніше існуючий закон...Він був прийнятий парламентом та підписаний президентом країни і цілком задовольнив вимоги Альянсу [221, с. 155].

Водночас, ухвалений у 2010 році Закон «Про засоби масової інформації» був неоднозначно сприйнятий світовими спільнотами. Оскільки, на думку мас-медіа, запроваджував тотальний контроль за засобами масової інформації, у тому числі й Інтернет. Угорщину звинуватили у наступі на свободу слова з метою встановлення тоталітарного режиму. Такі висловлювання знайшли підтримку в Європейському парламенті, який ухвалив резолюцію із засудженням позиції угорського уряду до свободи слова, прав людини і демократичних цінностей. Принагідно треба зазначити, що така резолюція вперше була висловлена на адресу країни-учасниці Європейського Союзу.

У відповідь на оприлюднені звинувачення парламент Угорщини вніс окремі, здебільшого «косметичні» зміни до цього закону, проте вони практично не змінили сутності ключових питань [222, с. 11-12].

Крім наведеного вище, питання правового регулювання сфери інформаційної безпеки в Угорщині оговорені в ухваленому в 2013 році Законі «Про електронну інформаційну безпеку державних та муніципальних органів» [223], а також п. 31 Стратегії національної безпеки Угорщини, прийнятій у 2012 році [224]. В основному, підняті в даних документах питання стосувалися протидії злочинам у сфері кібербезпеки.

Положеннями коментованої Стратегії передбачено, що держава має бути здатною керувати загрозами і ризиками, спрямованими на порушення стану національної безпеки, оборони, боротьби зі злочинами і правопорушеннями у сфері використання і обміну інформацією, а таж здійснювати превентивні заходи на напрямках можливих форсмажорних ситуацій у кіберпросторі. При цьому має бути забезпечено достатній рівень кібербезпеки, а також гарантуватися виконання інших завдань щодо недопущення протиправних дій у зазначеній сфері.

Закладені в Стратегії положення щодо забезпечення систематичного визначення пріоритетів у сфері потенційних загроз і ризиків у кіберпросторі, підвищення рівня інформування громадян щодо можливих протиправних проявів, набули подальшого розвитку в ухваленій в 2013 році Національній стратегії кібербезпеки Угорщини [225].

На підставі здійсненого теоретико-правового аналізу загальних аспектів сучасного стану забезпечення інформаційної безпеки в Україні можна з певною мірою впевненості зробити висновок про те, що: означений вид діяльності має на меті сформувати єдиний інформаційний простір з дружніми країнами; забезпечити розвиток інформаційно-комунікаційних технологій на підґрунті

найкращих світових досягнень з урахуванням особливостей інформаційної сфери України та міжнародних стандартів регулювання цієї сфери.

3.3 Шляхи вдосконалення інформаційної безпеки в Україні

Завдяки науковому аналізу буде здійснено теоретико-правову оцінку ефективності використання позитивного досвіду європейських країн у сфері забезпечення інформаційної безпеки, що має важливе значення для розбудови цієї галузі в Україні. Звернення до передових юридичних напрацювань і практичних здобутків країн Європейського Союзу і Великобританії може слугувати тим підґрунтям, на якому продовжиться стратегічна лінія щодо формування дієвих механізмів протидії протиправному втручання в інформаційну сферу України, насамперед тих, якими забезпечиться постійне функціонування превентивних інструментів нейтралізації інформаційних загроз. Як було вказано вище, такий стан упорядкування інструментно-правового клімату сфери інформаційної безпеки в державі найбільш повно відповідатиме завданням захисту кіберпростору України як складової національної безпеки в умовах протистояння російській військовій агресії та налагодження належного інформаційного поля після перемоги України у цій війні.

В результаті застосування методологічного інструментарію, у цьому разі наукового синтезу, ми отримаємо висновки, які продемонструють авторське розуміння джерел і шляхів оздоровлення сфери інформації в Україні, а також проаналізуємо нормативно-правові акти і наукові підходи до розуміння цієї проблематики.

Відповідність критеріям сучасного рівня державної політики із забезпечення інформаційної безпеки є досить складним завданням, що вимагає аналізу широкого кола проблем, напрямків та їх інтерпретації в організаційно-

правовому полі, як підґрунтя розбудови і необхідного удосконалення системи національної безпеки. В її основу має бути покладена методологія як інструмент дослідження оцінки діяльності органів сфери державного управління щодо забезпечення гарантій інформаційної безпеки не тільки приватній особі чи соціальним групам, а суспільству як суб'єкту правовідносин цієї сфери.

На думку С. В. Ковтуна, критеріями оцінки стану інформаційної безпеки може виступати «інформаційний статус» суб'єктів, що її реалізують (можливості індивідів у використанні інформаційного простору, забезпеченість всіма необхідними засобами, рівень інформаційної освіти та ін.); розвиненість, доступність та надійність інформаційно-комунікаційних мереж; розвиненість, надійність, систематизованість і зручність інформаційних ресурсів тощо [226, с. 88].

Для характеристики критеріїв інформаційної безпеки рекомендовано застосовувати модель тріади CIA (англ. – CIA Triad), якою передбачено використання трьох основних якостей інформаційної безпеки, а саме: цілісність, доступність і конфіденційність.

Ю. В. Нестеряк вважає, що в цілому, до основних критеріїв міжнародної інформаційної безпеки, окрім захисту інформаційних ресурсів з метою забезпечення їх конфіденційності, захисту даних ввід несанкціонованої модифікації або знищення, варто віднести ще «забезпечення працездатності систем за допомогою технології протидії загрозам» [177, с. 43–45].

В умовах глобалізації та вільного обігу інформації великого значення набуває комплексний характер оцінки актуальних загроз національній безпеці в інформаційній сфері. Такий підхід потребує, насамперед, вирізнення ефективних інструментів, які б відповідали рівню загроз, що виникають у зв'язку з використанням інформації та функціонуванням системи захисту інформаційних ресурсів.

Саме з такою метою потрібно формувати ефективну управлінську діяльність, яку доцільно розглядати в двох аспектах: управління технічними системами та вплив на соціальні процеси для організації діяльності на шляху до виконання поставлених завдань [227, с. 113].

Принагідно зазначаємо, що зазначена тематика глибоко і всебічно досліджувалась з позицій юридичних аспектів, про що свідчать ранні і більш сучасні результати наукового доробку, на окремі з яких ми зішлемося як на підстави свої майбутніх авторських узагальнень.

В. Шатун та О. Гладун, досліджуючи проблематику функціонування інформаційної безпеки у структурі національної безпеки, зазначають, що події останніх років у нашій державі показали неспроможність протистояти інформаційним війнам, позаяк проблеми інформаційної політики досі не вирішені на належному рівні [228, с. 179].

Як вбачається, наразі Україна запроваджує окремі положення законодавства Європейського Союзу на напрямках розбудови та провадженням контролю з урахуванням багатоступеневої політики в інформаційній сфері (глобальний; рівень Євросоюзу, національний рівень). Тому для поглиблення наукової цінності дослідження доцільно проаналізувати механізми формування та реалізації інформаційної політики в країнах з високим рівнем розвитку з метою вирізнення позитивних практик та їх застосування в українську практику.

У цьому зв'язку В. С. Політанський зазначає, що, визначившись із зовнішньополітичним курсом, Україна має орієнтуватись першочергово на стратегію розвитку країн-учасниць Європейського Союзу в інформаційній сфері [229, с. 18].

Шляхами вдосконалення організаційних засад державної політики у галузі інформаційної безпеки України прогнозовано передбачується приведення її у відповідність до високих стандартів (насамперед, США) щодо реформування

цілісної економіко-правової галузі, а саме інформаційно-комунікаційної сфери. Такий підхід повномірно співвідноситься з конституційними положеннями, що передбачено статтею 9 Основного Закону (щодо формування національного законодавства і включення до нього міжнародних правових актів, ратифікованих Верховною Радою України).

Така державницька стратегія, з одного боку, забезпечить утвердження стійкої організаційно-інформаційної мережі, з іншого – сприятиме організації заходів із захисту інформаційних мереж і комунікаційних засобів від джерел потенційних загроз. У такому разі в умовах тотальних заходів з протидії загрозам у сфері інформаційної безпеки вадливу роль відіграватиме новітня модель міжвідомчої взаємодії на цих напрямках.

Поточне узагальнення проаналізованої нормативно-правової бази і наукового доробку показало, що Україна, перебуваючи у вкрай складній ситуації, має бути здатна надати адекватну відповідь на всі існуючі чи потенційні загрози власній сфері інформаційної безпеки. Саме це виступає причиною розроблення цілісної стратегії захисту інформаційного поля держави на кшталт тих стратегій, які вже понад чверть століття ефективно забезпечують цю сферу в країнах Європейського Союзу.

У подальшому таку стратегію необхідно вдосконалювати з врахуванням досягнень науки права і технологічних досягнень, а також опираючись на технологічні, фінансово-економічні та інші індикатори розвитку держави. Натепер, коли державні ресурси надто обмежені через повномасштабне вторгнення росії, виникає потреба у залученні зовнішніх джерел фінансування тих галузей і сфер суспільного життя, які потребують першочергової підтримки. Одне з чільних місць у цих процесах відведено матеріально-технічному забезпеченню сектору інформаційної безпеки як індикатора стану морального здоров'я суспільства.

Результати дослідження наукового доробку В. К. Конаха показали узагальнені підходи до розуміння значення розвитку сфери інформаційної безпеки. Ми погоджуємося з тим, що на тривалу перспективу перед Україною поставатиме завдання «розвивати, враховуючи правові, технологічні, матеріально-фінансові та інші аспекти» [230, с. 25].

Зі свого боку додамо, що перелік напрямків удосконалення і посилення сектора інформаційної безпеки у структурі національної безпеки необхідно розширити завданнями щодо протидії джерелам зовнішніх інформаційних загроз незалежно від їх характеру чи держави походження, виховання населення у дусі високої моральності та особистої відповідальності за стан справ у країні, впровадження у всі елементи інформаційної безпеки позитивного закордонного досвіду.

Ми повністю погоджуємося з думками В. Конаха і вважаємо, що запровадження таких інструментів міжвідомчого контролю і взаємодії на всіх рівнях державотворення сприятиме повномасштабному формуванню інформаційного поля, належно захищеного від протиправних посягань.

Водночас доцільним є висловити авторське бачення шляхів розв'язання проблем, які, на думку В. К. Конаха, мають місце у сфері забезпечення інформаційної безпеки. На наш погляд, вирішення даного питання має відбуватися у такий спосіб:

- здійснювати постійний моніторинг нормативно-правового забезпечення інформаційної безпеки з урахуванням змін в суспільстві і міжнародному середовищі, максимально швидко і якісно реагувати на всі наявні і потенційні виклики ;

- розробити і здійснити комплекс заходів, які б максимально широко і швидко донесли до світової громадськості зміст і значення тієї героїчної діяльності України, яка відбувається в Україні в період відбиття агресії росії;

– на прикладі сучасних героїв і героїв минувшини, визначних історичних подій в історії українського державного будівництва розробити цілісну ідеологію із забезпечення виховання громадян у дусі поваги і шани до тих, хто в жорстоких боях відстоював і щоденно виборює наше право на вільне життя в демократичній країні;

– удосконалення технічного і професійного супроводження процесів провадження державної політики у сфері захисту інтересів особи і держави в інформаційній сфері;

– розроблення і реалізація скоординованих з іншими зацікавленими державними і недержавними структурами заходів щодо нейтралізації загроз у сфері інформаційної безпеки та забезпечення ефективної протидії таким зазіханням.

О. В. Курбан, виходячи з юридичного аналізу ситуації у сфері інформаційної безпеки, вбачає низку напрямів, якими ці проблеми можна вирішити. Таке рішення науковець пропонує розглядати в прикладному, кадровому і науковому сенсах [231, с. 61].

Ми ж маємо намір дещо скоригувати і одночасно доповнити висловлені науковцем судження, з тлумаченням яких ми повністю погоджуємося.

На наш погляд, серед завдань, за якими доцільно характеризувати означені питання, можна визначити:

- прикладне – вироблення та імплементація стандартів і прийомів протидії інформаційним атакам і війнам, що сприятиме швидкій та ефективній нейтралізації наявних чи потенційних загроз для сфери інформаційної безпеки держави;

- кадрове – організація та проведення заходів з професійної орієнтації і перекваліфікації працівників з метою їх залучення до праці у галузі захисту інформаційного простору держави;

- науково-практичне – розвиток і створення науково-дослідних центрів, які в тісній співпраці з практичними працівниками мали змогу верифікувати результати своїх досліджень і найбільш прогресивні, корисні та ефективні зразки і прийоми мали можливість дуже швидко, без зайвої бюрократичної тяганини запроваджувати у практику.

Цілі реалізації державної політики забезпечення інформаційної безпеки можуть бути досягнуті лише шляхом послідовного та випереджаючого розвитку вітчизняного законодавства, за умов обов'язкового дотримання конституційних засад державотворення з урахуванням досвіду європейських країн.

Оскільки нормативно-правова база не охоплює повномірно всі складові, що становлять інструментарій протидії загрозам у сфері інформаційної безпеки, є певною мірою застаріла, то саме з цих причин цей напрямок як складова національної безпеки потребує глибинного удосконалення всієї законодавчої сфери відповідно до сучасних воєнно-економічних і політико-правових викликів.

На нашу думку, ефективні механізми та належний рівень правового захисту можуть бути досягнені при запровадженні єдиного порядку управління усіма складовими сфери інформаційної безпеки. У цьому зв'язку доцільного надати пропозицію щодо розроблення і ухвалення універсального закону (кодифікованого акту на кшталт Кодексу України з процедур банкрутства тощо), який би звів до спільного нормативно-правового знаменника на цей час розпорошені і такі, що дисонують між собою правові норми, закладені у різних законодавчих і підзаконних нормативно-правових актах. Для даного документу може бути прийнятною назва «Кодекс України у сфері інформації».

Таку думку висловлюють окремі науковці, серед яких В. П. Горбулін та М. М. Биченок, які вважають, що «відсутність системного підходу до формування права й нормотворчості є актуальним завданням, зумовленим належною систематизацією чинного законодавства [156, с. 98].

При формуванні цілісної сфери нормативно-правового регулювання інформаційної безпеки необхідно створити методологічне підґрунтя для інформаційного нормотворення відповідного рівня, усунувши труднощі суб'єктивного і об'єктивного характеру.

Ми схильні думати, що існуючі виклики у сфері інформаційних загроз вимагають створення сучасної нормативно-правової і політико-економічної бази на основі діалектичного поєднання головних цілей та ідей правового забезпечення сфери інформаційної безпеки у тісному взаємозв'язку з потребами національної безпеки. У цьому разі, а також з урахуванням того, що ця проблема є головною у питаннях посилення дієвості інструментів інформаційної безпеки країни, доцільно вести розмову про вироблення уніфікованих стандартів, вимог, способів та заходів на напрямках функціонування оновленої цілісної системи інформаційної безпеки на національному рівні, відмежовуючись від регіональних особливостей та політичної доцільності.

Підтвердженням вищезазначеному є судження О. В. Левченка, який вказує, що система правових стандартів має стати об'єктивним «чинником для системної та ефективної реалізації державної інформаційної політики, а також надійної протидії деструктивному іноземному інформаційному впливу та інформаційним загрозам в цілому» [232].

Серед інструментів, спрямованих на утвердження правопорядку у сфері використання інформації, доцільно розглянути можливість посилення кримінальної відповідальності за умисне публічне поширення завідомо неправдивої інформації, яке вчиняється для сіяння тривоги, паніки та страху серед громадян, підбурювання до правопорушень і злочинів, спрямованих на завдання шкоди встановленому порядку функціонування інформаційного середовища, а також невиконання законних розпоряджень представників держави та місцевих органів влади. Особливої актуальності набуває така

законотворча діяльність в умовах воєнного стану, коли російська ворожа пропаганда використовує всі можливі і доступні джерела для того, щоб підірвати патріотичний дух українського народу при супротиві їх загарбницьким діям, а також здійснює кібератаки та фейкові вкидання для формування неправдивого інформаційного середовища поза межами України.

Подальша активна робота щодо розроблення національного законодавства у сфері безпеки інформації, приведення її до міжнародних вимог, а саме адаптація до найвищих стандартів у забезпеченні права людини, держави на інформацію, правомірність її використання, однозначно сприятиме підвищенню рівня ефективності заходів з протидії загрозам у сфері користування інформацією, а також підвищенню авторитетності України в очах міжнародних партнерів.

Такий підхід сприятиме формування справжньої інформаційної незалежності України, утвердженню підвалин інформаційного суверенітету, що передбачає покращання всієї галузі інформаційної сфери на основі запровадження ефективних механізмів правового регулювання, застосування оновлених і новітніх інструментів технологічного та захисного характеру, поширення на внутрішньому ринку та міжнародних медіаресурсах достовірної інформації про Україну. Також позитивний вплив справлятимуть активне залучення представників ЗМІ до висвітлення деструктивних явищ і подій, які загрожують не тільки інформаційній безпеці, а й посягають на основи національної безпеки.

Водночас необхідно зазначити, що така діяльність має здійснюватися у при неухильному дотриманні конституційних гарантій і чинного законодавства, якими врегульовані питання інформаційної безпеки і порядок користування відкритими і закритими базами даних. Особливим запобіжником для стабілізації позитивних змін у сфері поширення інформації є завдання щодо недопущення

зловживань з боку представників державної влади і місцевого самоврядування, тобто приведення такої роботи у відповідність до положень статті 19 Конституції України [6].

Г. А. Піскорська, досліджуючи значення новітніх інформаційних технологій у захисті інформаційної безпеки України, зазначає, що «основними організаційними напрямками розвитку технології щодо виявлення загроз інформаційній безпеці держави на перспективу і в порядку важливості є:

- по-перше – це створення і впровадження спеціальних інформаційних технологій, які орієнтовані на діючу інфраструктуру країни, досягнення вітчизняної науки і техніки, менталітет і технічну культуру персоналу, який відповідає за її організацію;

- по-друге – створення спеціальних інформаційних і технологічних сил та засобів, які призначені для успішного ведення інформаційного протистояння з агресивними інформаційними ворожими системами інших держав;

- по-третє – здійснення міжнародної політики в галузі інформаційної безпеки, яка належно спрямована на створення взаємо безпечних загальних інформаційних технологій та єдиних інформаційних засобів (типу мегамережі «Інтернет»), які гарантують можливість інформаційної співпраці на основі дотримання міжнародного права усіма суб'єктами інформаційної співпраці [233, с. 125].

Як вбачається, запропоновані науковцем заходи не втратили актуальності на час написання цього дисертаційного дослідження, що засвідчує певний рівень наукового передбачення, і є беззаперечним свідченням сталості інформаційних викликів навіть без урахування особливостей воєнного стану в Україні. Такі завдання Україна змушена було б вирішувати для того, щоб стати повноцінним учасником світового інформаційного середовища.

Все це потребує цілеспрямованої скоординованої діяльності органів державного управління та місцевого самоврядування, які мають характеризуватися: плановірністю, конкретністю, активністю; надійністю, універсальністю, комплексністю та бути своєчасними. Зарубіжний досвід забезпечення інформаційної безпеки, свідчить, що майже всі світові держави ведуть постійну роботу і приділяють посилену увагу захисту своїх інтересів у сфері інформації шляхом створення компетентних органів для протидії порушенням на цю галузь, а також провадження превентивно-профілактичної роботи на напрямках виявлення і протидії джерелам внутрішніх і зовнішніх загроз.

Разом з тим, не дивлячись на певні складнощі в організації потужної протидії деструктивним впливам та нападам на інформаційну сферу України, недостатнє кадрове забезпечення органів та інших структур на напрямках знешкодження шкідливого інформаційного контенту, ця робота щоденно вдосконалюється, а імплементований у систему позитивний досвід дружніх країн приносить відчутні результати у розумінні розвінчування фейкових вкидів та інших шкідливих повідомлень в інформаційне середовище держави.

Постала також необхідність розробити нові інструменти, передусім аналітично-оцінювального характеру, що здатні на початкових етапах виявляти і знешкоджувати актуальні загрози інформаційній безпеці і відповідно можливим матеріальним та інтелектуальним збиткам для суспільства й держави.

На думку Є. В. Кобко, таку функцію має виконувати державна система моніторингу стану «національної безпеки як комплекс заходів щодо спостережень, збирання, опрацювання, передавання, збереження та аналізу інформації про стан національної безпеки...[234, с. 125].

Важливим завданням видається необхідність системно підвищувати рівень інформаційної культури для всіх учасників інформаційної сфери та забезпечення

їх ефективної співпраці, що слугуватиме основою для досягнення належного рівня інформаційної безпеки. Тому потрібно, щоб у концепції подальшого розвитку держави на напрямках руху до європейської спільноти, викладеної в стратегічних документах, насамперед в Конституції України, зосереджено увагу на тому, як може бути використаний її досвід щодо формування відповідного кадрового складу для розв'язання пріоритетних завдань щодо нейтралізації загроз психологічного і економічного характеру в контексті забезпечення інформаційної безпеки.

Колектив науковців у складі М. Ф. Криштановича, Я. Я. Пушака, М. І. Флейчука та В. І. Франчука вважають, що у ході обрання критеріїв для визначення ефективності політичних і державних заходів на напрямках стабілізації ситуації у сфері інформаційної безпеки необхідно зосередитись на показниках [235, с. 154–161], які ми прокоментуємо та подамо в авторській редакції.

На наш погляд, основне навантаження при розв'язанні зазначеного питання має розподілятися наступним чином:

- оцінка та аналіз концептуальних засад інформаційної безпеки, її принципів, стандартів та правил, які б кореспондувалися і відповідали положенням чинного законодавства, а також утверджували принципи цілісного механізму захисту інформаційного середовища держави;
- системний моніторинг джерел загроз інформаційній безпеці, за результатами якого вирізняти нові об'єкти і оновлювати чи покладати нові цілі;
- стан резистентності суспільства з огляду на масштабність ІПСО, запровадження конкурсного набору на посади в структурах, які відповідають за організацію протидії ворожим і деструктивним проявам у сфері інформаційного забезпечення тощо.

Таким чином, можна стверджувати, що гарантування належного стану інформаційної безпеки в Україні набуло значення серйозної проблеми, яка сягає найбільш уразливих елементів у структурі суспільства, а саме особу, спільноти людей, державні установи, органи місцевого самоврядування та інші господарські утворення. На цьому етапі історичного розвитку необхідно застосовувати комплексні заходи загальнонаціонального характеру, застосовуючи інструменти законотворення, державного будівництва і легітимного примушування до виконання вимог встановленого порядку користування та доступу до інформації та інформаційних ресурсів.

Ми також переконані, що формування конкурентоздатної і достатньо резистентної до джерел внутрішніх і зовнішніх загроз системи інформаційної безпеки України, а також розроблення дієвих стратегій і тактик протидії різним інформаційним загрозам повинні стати пріоритетними завданнями для органів державної влади, недержавних інституцій та організації і проведення наукових розвідок.

З огляду на вищесказане можна визначити основні вектори, за якими має розвиватися державна політика у сфері забезпечення інформаційної безпеки. До таких напрямків, на наше переконання, доцільно віднести:

- 1) утвердження і розширення конституційних гарантій захисту права людини на інформацію;
- 2) удосконалення системи протидії інформаційним загрозам у сфері інформаційної безпеки у комплексі заходів з дотримання національної безпеки;
- 3) створення надійних інструментів захисту економічних інтересів України за підтримки технологічних і медіа ресурсів інформаційної сфери.

У цьому зв'язку необхідно чітко розуміти роль і значення комплексного підходу до вирішення цього триєдиного завдання, оскільки роздільне чи сегментарне виконання окремих складових не принесе очікуваного результату

для забезпечення дотримання належного інформаційного порядку в усіх сферах життєдіяльності українського суспільства.

Для реалізації державної політики на напрямках захисту національних інтересів держави в інформаційній сфері слід заохочувати впровадження міжнародних стандартів, сприяти надходженню інвестицій в розбудову інформаційної сфери держави, що означає відкритість у відносинах на шляху формування вільного ринкового середовища, включення і підтримки функціонування інструментів правового захисту права інтелектуальної власності і комерційної таємниці від викрадення, пошкодження чи неправочинного використання. Узагальненою метою таких заходів є забезпечення верховенства при застосуванні сумісних і безпечних стандартів.

Дослідження державної політики стосовно інформаційної безпеки України показало, що оскільки ця галузь є однією з основних серед компонентів національної безпеки, то ця сфера потребує постійної роботи з удосконалення нормативно-правової бази, яка б ефективно і належним чином урівноважувала взаємовідносини між усіма суб'єктами національної безпеки, визначала їхні, передбачені Конституцією України межі відповідальності, а також задекларовані права та встановлені нормативними актами обов'язки.

Зокрема, доцільно розробити Закон України «Про економічну та інформаційну безпеку України», а також Концепцію законодавства у сфері економічної та інформаційної безпеки, а також відповідну Програму з підготовки нормативно-правових актів, пов'язаних із забезпеченням ефективного функціонування і захисту права на користування інформацією учасниками економічної сфери та дотичним до цієї діяльності суб'єктів владних повноважень та представників українського суспільства. Такі дії сприятимуть упорядкуванню правовідносин в інформаційній сфері на принципах демократичності, що, своєю чергою, уможливить уникнення хаотичності та

безсистемності на зазначених напрямках з метою збереження належного рівня верховенства права.

Наступним, на наш погляд, дієвим кроком може стати проведення наукової експертизи нормативно-правових актів попередніх років з метою надання юридичної оцінки їх відповідності сучасним викликам в умовах воєнної агресії росії проти України. У разі виявлення будь-якої невідповідності, недієвості, а також протиріч при упорядкуванні однотипних відносин нормативно-правовими актами, необхідно розробляти пропозиції щодо скасування цих документів чи внесення до них відповідних змін.

Також, на нашу думку, важливо здійснювати поглиблене експертне дослідження тих нормативно-правових актів, які розробляються або вже перебувають на розгляді відповідних компетентних органів. Особливу увагу слід приділити правовій експертизі проектів законів для закладання у них прогностичних і перспективних заходів з урахуванням наукового моделювання ситуації у сфері інформаційної безпеки.

Зважаючи на актуальність проблеми забезпечення інформаційної безпеки України, вкрай важливим є звернення до позитивного досвіду дружніх країн європейського та інших континентів з метою узагальнення таких відомостей для вироблення національних інструментів впливу на загрози цієї складової національної безпеки України.

Необхідно також зазначити, що процес реформування соціально-економічної та інших сфер життєдіяльності суспільства є надто утрудненим оцінювання досвіду інших держав, аналізу позитивних результатів, які засвідчила кожна з виокремлених моделей розвитку інформаційних правовідносин та захисту і дотримання встановленого порядку у цій сфері, застосування фахових підходів для реалізації ефективної національної політики, у тому числі у сфері забезпечення інформаційної безпеки.

В умовах сьогодення, коли росією зруйнована вся система міжнародної безпеки, знівельовано основоположні права людини, має відбутися переоцінка соціально-економічних пріоритетів суспільного розвитку з урахуванням справжніх наслідків і прогнозованих матеріальних збитків і моральної шкоди не тільки вітчизняній національній безпеці, а й усім державним і недержавним інституціям, залученим до процесу вивільнення України з-під російського колоніального гноблення. У такий спосіб вдасться, з одного боку, нейтралізувати джерела зовнішніх і внутрішніх загроз інформаційній безпеці держави, з другого – імплементувати позитивний міжнародний досвід на напрямках оздоровлення ситуації на пріоритетних напрямках українського державотворення.

Таким чином, забезпечення інформаційної безпеки України в у контексті провадження заходів з утвердження національної безпеки виступає вирішальним фактором у становленні правосуб'єктності України як кандидата на вступ до Європейського Союзу.

О. В. Іващенко та В. М. Гельман [236, с. 125], досліджуючи проблеми фінансово-економічної безпеки, вбачають інформаційну безпеку компонентою економічної сфери і зазначають основні, на їх думку, напрями підвищення рівня захищеності інформаційної безпеки України.

З урахуванням думок згаданих науковців ми пропонуємо авторське бачення таких першочергових дій, а саме:

- постійний контроль і аналіз для прогнозування і своєчасного виявлення джерел загроз фінансово-економічній сфері з боку неналежної організації фізичного захисту інформаційного середовища як підґрунтя для дезінформації та викривлення дійсних обставин;

- на підставі дослідження порогових значень індикаторів економічної безпеки та їх порогових значень запровадити систему моніторингу

взаємовпливів між цими двома елементами національної безпеки з метою своєчасного реагування у випадку виявлення негативних тенденцій;

- удосконалення системи заходів для забезпечення інформаційної мережі на межі її дотичності до економічної галузі, розроблення механізмів стримування протиправних зазіхань на встановлений конституційний порядок в економічному та інформаційному секторах;

- посилення правового контролю за виконанням вимог і правил безпеки щодо використання інформації при використанні підприємницькими структурами, пов'язаними з виконанням важливих державних замовлень, насамперед в оборонній сфері;

- забезпечення необхідного рівня захисту інформаційними ресурсами стратегічних та мобілізаційних джерел держави.

З наведеного можна зробити висновок, що забезпечення інформаційної безпеки держави в економічній сфері має перманентний характер, потребує комплексного вирішення на основі поєднання професійних зусиль як науковців, так і практиків з різних галузей техніки та управління.

Своєю чергою, зміст діяльності щодо забезпечення інформаційної безпеки в економічній сфері має на меті забезпечити підтримку і просування провідних міжнародних та вітчизняних досягнень у цій сфері, застосування профільних правових механізмів тощо. Зазначені проблеми мають віднайти своє розв'язання на підставі використання чинних механізмів інформаційної сфери з урахуванням особливостей тих ресурсів, які перебувають у їх віданні, з дотриманням ієрархії та компетенції при розкритті доступу до баз даних.

Розглядаючи інформаційну безпеку держави як складне і багатоаспектне політичне та економіко-правове явище, доцільно вести розмову про систему показників, своєрідних індикаторів, які включають в себе здатність владно-державних утворень функціонувати в режимі розширеного відтворення,

стійкість до спроб протиправного втручання, раціональну структуру контролюючих механізмів, підтримку на необхідному рівні наукового та технологічного потенціалу, збереження єдиного інформаційного простору і цілісності ресурсного забезпечення, створення нормативно-правового середовища, що виключають криміналізацію інформаційної сфери, забезпечення необхідного регулювання процесів зберігання, передавання та обміну даними тощо.

За таких обставин інформаційна безпека в структурі національної безпеки полягає у можливості контролю держави за дотриманням конституційного правопорядку, досягнення безпечного рівня передавання відомостей різного ступеню правового захисту, який міг би забезпечити ефективну протидію зовнішнім і внутрішнім протиправним зазіханням на цілісність системи захисту інформаційного середовища держави.

Колектив науковців у складі А. Й. Француза, С. В. Кудіна, О. В. Федорчука зазначають, що сучасний стан нашої держави характеризується як етап формування інформаційного суспільства. Впровадження новітніх інформаційних технологій значно прискорює процес отримання, обробки, аналізу інформації. Широкий і оперативний доступ до інформації підвищує ефективність її використання, що стає невід'ємним елементом управління всіма інститутами і процесами [237, с. 6].

Інформаційна безпека, перебуваючи у діалектичному зв'язку з іншими структурними елементами національної безпеки, насправді відбиває реальний стан, загальну картину функціонування цілісної системи державної безпеки в усіх сферах життєдіяльності суспільства. Саме тому рівень превентивно-профілактичної діяльності на найбільш вразливих напрямках забезпечення функціонування державного апарату інформацією, насамперед з обмеженим доступом, має відповідати критеріям стійкості, стабільності, резистентності, що

досягається шляхом перманентного провадження компетентними органами упереджувальних дій на основі застосування нормативно-правової бази з регулювання правовідносин цієї сфери.

Відтак, на наш погляд, ефективне забезпечення національної безпеки України у галузі захисту інформації передбачає необхідність розробки науково обгрунтованої державної політики та стратегії у цій сфері, а також провадження постійного моніторингу потенційних і актуальних загроз інформаційній безпеці держави, пошуку ефективних інструментів для створення безпечних умов функціонування в усіх її сегментах та проявах.

З урахуванням зазначеного вище можна говорити про те, що зростання рівня інформатизації та діджиталізація сучасного суспільства створює умови для стійкого функціонування інформаційної інфраструктури, що своєю чергою сприяє реалізації національних інтересів України в інформаційній сфері.

На це й час для України відкривається перспектива, завдяки набуттю статусу країни-кандидатки на вступ до ЄС, а також з урахуванням обставин, що виникли у протистоянні повномасштабному вторгненню росії, розробити та впровадити нові, високі стандарти захисту інформаційного простору. Це – унікальна ситуація, коли держава перебуває на гребні військової звитяги і демонструє нестримне бажання долучитись до клубу країн – найбільш дієвими системами захисту своєї державності, суверенітету і свободи.

Оцінюючи загрози інформаційній безпеці, Н. Б. Новицька, В. М. Петрик та В. М. Кудико зазначають: «В інформаційній війні російської федерації проти України активно використовується дезінформування. Проведення росією дезінформування на території України виявилось малоефективним, що у певний спосіб вплинуло на поразки на військовому фронті» [238, с. 129].

Теоретико-правовий аналіз нормативного регулювання відносин у сфері захисту інформації в країнах ЄС показав, що при значній індивідуалізації і

нетипових підходах до розуміння змісту і обсягу сфери безпеки інформації, відзначається багато спільного, насамперед щодо досягнення консенсусу при організації міждержавної взаємодії щодо обміну відомостями в і базах даних, доступу до інформації, непорушність національних суверенітетів у галузі інформації, сприяння досягненню приблизно однакового техніко-технологічного рівня інструментів захисту інформаційного поля своїх держав.

У контексті результатів дослідження, представлених у попередньому підрозділі, вважаємо за доцільне запропонувати використання позитивного досвіду країн ЄС у сфері захисту інформаційної безпеки врахувати під час внесення змін до чинного законодавства у цій галузі, а також при розробленні і ухваленні нових законодавчих актів.

На думку О. І. Косілової та Х. К. Солодовнікової, які висловлюються стосовно завдань із управління інформаційно-безпековим середовищем та формування медіазрілого суспільства: «...є підстави стверджувати, що на сьогодні в Україні основні принципи захисту прав людини в постіндустріальну, епоху четвертої революції задекларовано, а їх імплементація стикається з багатьма перешкодами) [239, с. 63].

До списку проблемних питань у ході формування вітчизняного зрілого інформаційного суспільства слід віднести наступні:

- недостатня координуюча роль з боку держави на напрямках організації взаємодії між публічним та приватними секторами економіки;
- послаблений контроль за використанням матеріальних і фінансових ресурсів, виділених на модернізацію сфери захисту інформаційної безпеки, що має наслідком нецільового, а в окремих випадках і злочинного використання коштів;
- недостатній професійний рівень працівників сфери інформаційної безпеки;

- уповільнені темпи з розбудови інформаційної інфраструктури;
- нерівномірний розподіл матеріальних ресурсів між регіонами, що породжує проблеми для доступу населення як до джерел інформації, так і отримання належного інформаційного забезпечення;
- недостатня присутність вітчизняних медіаресурсів в глобальному інформаційному просторі;
- послаблений контроль за дотриманням авторських і суміжних прав при використанні продуктів програмного забезпечення;
- недостатнє фінансування науково-дослідних робіт у сфері розроблення нових інформаційних технологій.

Наведений перелік не є вичерпним, підлягає доповненню і може бути у певній мірі скоригований.

З урахуванням вищезазначеного, пропонуються заходи для виправлення ситуації, тобто на рівні держави вчинити дії, які б не тільки нейтралізували виявлені недоліки в організації і функціонуванні сфери інформаційної безпеки, а й суттєво її покращили. Такі дії доцільно здійснити на таких напрямках:

- переформатувати державну стратегію у сфері інформаційної безпеки з урахуванням сталих і нових джерел загроз;
- промоніторити весь масив вітчизняних інформаційних ресурсів на предмет їх відповідності чинному законодавству;
- створити умови для системного розвитку афілійованих до сфери інформаційної безпеки галузі економіки з метою якнайшвидшого впровадження новітніх технологій збереження інформації;
- забезпечити подальший розвиток цифрових технологій у сфері використання інформації та перехід на електронний варіант підготовки і обігу документів;

- розвивати конституційні гарантії у сфері забезпечення права громадян на інформацію, ефективно протидіяти протиправним зазіханням на встановлений порядок використання інформаційних баз даних;

- привести у відповідність до норм забезпечення національної безпеки інформаційну сферу, посилити контроль за доступом до інформації з обмеженим доступом;

- звести чинне законодавство України до єдиного кодифікованого акту з метою забезпечення уніфікованих підходів до правил регулювання відносин у сфері інформаційного права.

Задля створення єдиного світового інформаційного простору, з урахуванням періоду активного розвитку, інформатизації та глобалізації, важливу роль відіграє забезпеченість високотехнологічним та промисловим потенціалом. У такому разі до глобальних інформаційних мереж зможуть приєднатися лише ті країни, які відповідатимуть найвищим стандартам, закладеним для подолання об'єктивних перепон, пов'язаних з неналежним рівнем розвитку інформаційно-комунікаційних систем.

З урахуванням сказаного виникла можливість запропонувати конкретні варіанти дій, спрямованих на досягнення високих міжнародних вимог щодо входження до глобальних інформаційних мереж. Такими діями можуть бути:

- 1) посилення впливу у сфері нормативно-правових відносин органів державної влади як розпорядників механізмів захисту в поширенні інформації;

- 2) розроблення програми для формування переліку нормативно-правових актів державно-владних органів та актів місцевого самоврядування з метою приведення їх до єдиної системи обліку з наданням відповідного доступу користувачам (у межах дозволеного);

- 3) прискорення впровадження новітніх інформаційно-комунікаційних технологій, розроблення відповідних програм для забезпечення громадянам

можливості отримувати якісні і відомості, убезпечені від неправомірної модифікації;

4) забезпечення організації та проведення різних інформаційних кампаній серед широкого загалу;

5) посилення співпраці з різними національними та міжнародними громадськими організаціями.

Отже, сучасний етап у розвитку України на напрямках захисту інформаційної безпеки вимагає підвищення рівня державної участі у цих процесах, організацію і забезпечення контролю за всіма суб'єктами інформаційної сфери з позицій оцінки правомірності користування і використання ними інформації.

У цьому зв'язку О. І. Косілова та І. П. Федірко зазначають: «Можемо говорити про те, що інтелектуалізація управлінських процесів зі сфери економіки поширилася на сферу державного управління, формуючи таким чином новий тип інформаційної політичної культури та партисипаторної демократії» [240, с. 59].

Аналізуючи сучасний стан інформаційного законодавства, необхідно зазначити, що значна кількість нормативно-правових актів, якими врегульовано питання інформаційної безпеки, не сприяє створенню єдиної основи для виконання завдань цієї сфери у структурі національної безпеки. На нашу думку, ефективним інструментом систематизації нормативно-правової бази інформаційної безпеки була б її кодифікація, тобто ухвалення Інформаційного кодексу України, в основу якого доцільно закласти Концепцію національної інформаційної політики та оновлений Закон України «Про інформацію».

Окрім проведеного аналізу, важливим убачається й запровадження досвіду інших країн європейського медіапростору, які проходять аналогічний шлях оновлення сфери захисту інформації. Тож дослідження, оцінка та імплементація

позитивних напрацювань на напрямках забезпечення інформаційної безпеки набувають першочергового значення для нашої держави як суб'єкта глобальної інформаційної сфери. Сучасний стан правопорядку у сфері захисту інформації потребує не тільки «косметичного втручання», а подекуди мають бути внесені кардинальні зміни з урахуванням повномасштабної агресії росії проти України.

Більше того, для України матиме позитивне значення у випадку вступу до клубу європейських країн як учасника сфери захисту інформаційної безпеки, що значно підсилить позиції України на напрямках протидії порушенням в інформаційній сфері, кіберзлочинам і кібертероризму. Такі дії доцільно проводити вже на ранніх етапах підготовки до вступу України в Європейський Союз та НАТО.

Висновки до розділу 3

Підсумовуючи викладене, необхідно зазначити, що коментований розділ є фіналізованою частиною попередніх частин наукового дослідження, оскільки піднята проблематика деталізує і поглиблює розуміння поняття «інформаційна безпека» у поєднанні з чинниками, які породжують протиправні зазіхання на встановлений порядок користування інформацією.

Синтезований підсумок складових інформаційної безпеки у контексті дотримання вимог національної безпеки показав можливі першопричини, з яких можуть завдаватися зловмисні посягання на встановлений порядок користування відомостями і базами даних з різним рівнем технологічного і правового захисту. Виходячи з власних висновків, з урахуванням оприлюдненого наукового доробку з цієї проблематики, а також на підґрунті офіційних тлумачень виокремлених аспектів проявів функціонування інформаційної сфери, подано авторську класифікацію джерел загроз інформаційній безпеці. При цьому взято

до уваги правову природу і територіальне походження таких дій, які можуть свідчити про наміри протиправного втручання у чинну систему захисту масивів баз даних та інших відомостей, порядок зберігання яких визначається законом.

Деталізовано джерела загроз інформаційній безпеці з урахуванням людського фактору, визначено напрямки провадження профілактико-превентивних заходів з метою нейтралізації протиправних посягань на інформаційну сферу як підгрунтя комунікації у всіх сферах життєдіяльності держави. Подано також глибинний аналіз джерел загроз з боку російської федерації як країни-агресора, який, окрім фізичного знищення нашої держави, має на меті провадження інформаційно-психологічних спеціальних операцій для поширення паніки і капітулянтських настроїв серед громадян України.

У межах предмета дослідження проаналізовано законодавство Європейського Союзу і Великобританії. Вивчення показало окремі аспекти у підходах до правового регулювання відносин у сфері інформаційної безпеки, які продемонстрували ефективність нормативного впливу на стан збереження відомостей і протидії зовнішнім і внутрішнім загрозам, спрямованим на протиправне заволодіння технологічними, військовими та іншими секретами. Відзначається високий рівень координації заходів у сфері інформаційної безпеки європейських країн та Великобританії, що сприяє стабільному функціонуванню всіх ланок передачі даних з урахуванням особливостей економічного розвитку країн співдружності. Виокремлено низку позитивних інструментів, які при умові їх імплементації у нормативну базу України наближуватимуть наші правові системи до створення спільного, надійно захищеного інформаційного середовища. Вирішення такого завдання забезпечить більш швидке просування нашої держави на шляху до повноцінного членства у Євросоюзі та НАТО.

Оцінюючи реальний стан забезпечення ефективного функціонування сфери інформаційної безпеки в Україні, дійшли висновку про необхідність

провадження профілактичної діяльності у цій сфері на трьох основних напрямках, а саме:

- імплементації європейських зразків у чинне законодавство, максимальне наближення технологічної складової до вимог захисту і збереження баз даних згідно з вимогами передових країн;

- реформування вітчизняного інформаційного права на умовах упровадження ефективних інструментів захисту сфери передавання і використання відомостей різного рівня доступу, запровадження перманентного моніторингу медіапростору (зовнішнього і внутрішнього) для своєчасної і повної нейтралізації не тільки реальних загроз щодо протиправного втручання в інформаційне поле, а й вирізнення першоджерел у формі зазіхань на встановлений порядок в інформаційній сфері. Особливу увагу необхідно приділити оздоровленню медіапростору України з метою недопущення проявів інформаційно-психологічних спеціальних операцій, спрямованих на порушення збалансованості при забезпеченні належного морального і психологічного клімату в суспільстві;

- з урахуванням ситуації на українсько-російському фронті і міжнародної підтримки України у боротьбі проти російських окупантів створити надійний інформаційно-правовий щит, який би унеможливив просочення зловмисних відомостей з боку країни-терориста до нашої держави, і будь яким чином впливав на настрої населення. Таке можливе лише при тісній співпраці науковців і законотворців, адже своєчасне теоретичне обґрунтування можливих загроз інформаційній безпеці або розвінчання прихованого шкідливого контенту в діючих медіаресурсах здатне забезпечити ефективну протидію дезінформації та іншим проявам порушення конституційного порядку в державі.

ВИСНОВКИ

На підґрунті опрацьованого наукового доробку і практичних матеріалів у дисертації виведено наукове завдання – узагальнити наукові підходи та чинну практику у сфері захисту інформаційних ресурсів України, на підставі результатів теоретико-правового аналізу запропонувати авторські шляхи вирішення проблем, пов’язаних із застосуванням нормативно-правових інструментів регулювання відносин із забезпечення інформаційної безпеки як складової національної безпеки.

Як підсумок до проведеної наукової розвідки щодо дослідження теоретико-правових основ регулювання інформаційної безпеки в Україні, необхідно акцентувати увагу на особливостях науково-практичного аналізу нормативної бази з упорядкування відносин цієї сфери, а також наукового доробку, що торкається піднятої у дисертації проблематики.

Здобуті результати, підтверджені відповідним науковим матеріалом та широкою емпіричною базою, сприяли вирішенню наукового завдання - узагальнити наукові підходи та чинну практику у сфері захисту інформаційних ресурсів України, на підставі результатів теоретико-правового аналізу запропонувати авторські шляхи вирішення проблем, пов’язаних із застосуванням нормативно-правових інструментів регулювання відносин з забезпечення інформаційної безпеки як складової національної безпеки. Отримані у дослідницькому процесі наукові і практичні висновки обґрунтовуються покладеними завданнями.

1. З метою виконання покладених завдань всебічно досліджено першоджерела становлення юридичного явища «інформаційна безпека». Такий підхід зроблено з метою показати особливе значення цієї сфери для всіх етапів суспільного розвитку шляхом джерельного та історико-правового аналізу

пам'яток з філософії, історії, юриспруденції, історико-військових та інших документів.

Обґрунтовано, що проблеми захисту інформаційної безпеки, розглядалися не відірвано від основних сфер суспільного життя, а комплексно супроводжувались як звичаями на ранніх стадіях розуміння державності, так і писаними правилами, що покладалися як обов'язок для членів громадянського суспільства.

Підтверджено, що дослідженими історичними джерелами висвітлюються факти маніпулювання інформацією з різною метою. Найчастіше такі дії пов'язані з мистецтвом війни як інструментом введення противника в оману щодо справжніх планів сторони-опонента.

Ми дійшли висновків про багатоаспектне значення способів і цілей передавання і збереження інформації на ранніх етапах розвитку цивілізації. З філософсько-історичних джерел випливає, що донесення відомостей до мешканців окремих держав чи інших суспільних утворень виступало своєрідним інструментом спілкування між владою і підданими шляхом встановлення певних регулюючих норм при передаванні інформації, а також формування внутрішнього суспільного мікроклімату.

Дослідження генези інформаційного права сприяло отриманню об'єктивної картини щодо оцінки ролі і значення цієї сфери відносин у суспільстві. Це є свідченням розуміння високого аксіологічного значення стану організації інформаційного забезпечення для формування подальших інструментів регулювання правових відносин на етапах отримання і розпоряджання суспільно значимими відомостями.

2. Обраний методологічний інструментарій у межах проведеного наукового дослідження забезпечив досягнення фахового розуміння внутрішніх, діалектично пов'язаних процесів, які супроводжують державно-правову

діяльність у сфері підтримання належного рівня правового захисту інформаційної сфери України. Такий підхід дозволив повномірно проаналізувати фундаментальне значення сфери інформаційного права на всіх етапах його впливу на стан забезпечення відомостями всіх зацікавлених суб'єктів у системі заходів з підтримання конституційно визначеного рівня національної безпеки.

Базовим орієнтиром для виведення авторських узагальнень стали положення методологічної науки про складну елементну структуру поняття «інформаційна безпека», роль і значення законодавства України для функціонування всіх галузей права і встановлення легітимних основ для їх взаємодії.

Виокремлений методологічний інструментарій забезпечив компетентне посилення до структурних елементів у складі механізмів правового захисту, що, своєю чергою, підсилило авторські висновки про необхідність запровадження більш високого і захищеного рівня використання інформації в умовах воєнної агресії росії проти України. Саме аналіз і синтез системоутворюючих категорій, які застосовуються при нормативно-правовому регулюванні відносин у сфері інформаційної безпеки, відкрили шлях до прогностичних узагальнень на напрямках моделювання ідеалізованих варіантів системи захисту нематеріальних активів, якими є всі види баз даних.

3. Історико-правовий аналіз наукового доробку в частині виведення найбільш коректної дефініції поняття «інформаційна безпека», а також аргументи, висловлені на обґрунтування конкретних позицій щодо цієї ситуації, показав високий рівень зацікавленості з боку представників юридичної науки особливостями процесів становлення, функціонування і розвитку не тільки інформаційної сфери як засобу комунікації, а й пропонувалися заходи, які мали убезпечити сферу передачі інформації від протиправного втручання та зловмисного використання. У такий спосіб відбулося розмежування сфер

розуміння сутності інформації як динамічного соціального явища і елементів її супроводження, що створювали середовище легітимного користування інформацією. У цьому зв'язку відзначається поліаспектність загальної проблеми забезпечення інформаційної безпеки, оскільки соціально-економічні і правові інструменти механізмів її функціонування вимагають постійної взаємодії структурних складових у процесах, які обрамлюються цілісним поняттям «національна безпека». Таким чином говоримо про діалектичний зв'язок між рівнем утримання належного порядку при користуванні інформацією та загальним станом громадської безпеки, що здійснює вирішальний вплив на функціонування держави як суб'єкта міжнародного права.

Нова хвиля наукового інтересу до проблем, пов'язаних з інформаційною безпекою, набула поширення з причини нападу росії на Україну, який відбувся 24 лютого 2022 року. Саме агресія росії виявила прогалини як у законодавчому регулюванні інформаційної сфери, так і технологічні проблеми у виявленні ранніх зазіхань на встановлений порядок користування інформацією. Як бачимо, вітчизняна контрdezінформаційна система і нормативне середовище були повністю готовими до протидії масштабним ІІСО, dezінформаційним нападам та кібератакам з боку країни-терориста. У цьому дослідженні побіжно розглядаються питання щодо можливості запровадження загальнодержавних заходів з метою нейтралізації деструктивних інформаційних впливів з боку ворога.

Обґрунтовано, що первинним завданням державного будівництва, поряд з вирішенням проблем, пов'язаних зі збереженням достатнього рівня національної безпеки, є встановлення у суспільстві сприятливого психологічного мікроклімату, при якому були би реалізовані конституційні гарантії щодо правомірного володіння і використання інформації. Беззаперечним є факт, що цінність будь якої події у світовому, державно чи локальному масштабі

відбивається в інформаційних джерелах завдяки застосовуваним методам зберігання і поширення такої інформації.

4. Говорячи про застосування аксіологічного підходу до розуміння ролі і значення державно-правової діяльності на напрямках забезпечення інформаційної безпеки, необхідно зазначити, що у цей процес ми закладаємо міжгалузеву природу цього методологічного інструменту. Завдяки його можливостям забезпечується досягнення належного рівня праворозуміння і виконання імперативних правових вимог членами суспільства, встановлюються вимоги щодо моральних і етичних цінностей, формування високоморальних внутрішніх переконань, що спонукає їх бути активними учасниками внутрішньодержавних процесів. На даному етапі фізичного існування України високоморальний аспект у свідомості громадян демонструє відвагу і звитязність українського воїна, медика, волонтера (перелік невичерпний).

5. Достатньою умовою виконання заходів, передбачених у межах нормативного регулювання відносин в інформаційній сфері, є забезпечення якісного нормативно-правового регулювання цієї сфери у формі ухвалення законодавчих і підзаконних актів, встановлення дієвого контролю за дотриманням встановленого порядку користування інформацією, запровадженням відповідальності за порушення встановлених правил тощо.

Здійснивши теоретико-аналітичне дослідження документів різного рівня юридичної сили (закони, підзаконні акти тощо) на напрямках утвердження гарантованого Конституцією України порядку поведінки з інформацією, здобуто чітке розуміння якісних складових процесів провадження заходів з дотримання інформаційного «здоров'я» Українського суспільства крізь призму застосування механізмів аналізу і синтезу. Такі методологічні інструменти застосовано у межах вивчення правової характеристики нормативної бази на

декількох рівнях і в тому хронологічному порядку, який представлено в авторському поділі на часові періоди.

Поглиблене аналітико-правове дослідження міжнародних нормативно-правових актів, прокладання діалектико-філософських зв'язків між ними і чинним українським законодавством у сфері регулювання відносин на напрямках забезпечення інформаційної безпеки сприятиме фаховому аналізу інших аспектів відображення ролі цієї складової у загальному контексті дотримання належного рівня національної безпеки, нейтралізації джерел загроз інформаційній безпеці тощо.

6. Ґрунтуючись на висновках, отриманих як результат наукового синтезу структури і взаємодії елементів механізму забезпечення інформаційної безпеки, зроблено узагальнення про можливі і перманентні джерела загроз цій складовій як сегменту комплексного юридичного явища «національна безпека». Вирізнено напрямки прогнозованих першопричин протиправних зазіхань на вітчизняну систему захисту інформації, а також зазначено інструменти своєчасної та ефективної протидії недружнім і ворожим втручанням у порядок функціонування інформаційної сфери на всіх рівнях її захисту.

З метою фахового подання авторських узагальнень деталізовано окремі наукові підходи щодо класифікації джерел загроз інформаційній безпеці з урахуванням природи та територіальності їх походження.

Одним з критеріїв джерел загроз інформаційній безпеці визначено людський фактор. Це ганебне явище набуло значного поширення в період російської агресії з боку росії проти України (шпигунство, колаборантство тощо). Узагальнене бачення потенційно шкідливої ролі людини, управненої на володіння інформацією, насамперед з обмеженим доступом, сприяло виведенню пропозицій у складі комплексу профілактико-превентивних заходів з метою

недопущення витоку конфіденційних та інших відомостей, віднесених до державної таємниці.

7. Вибіркове дослідження нормативно-правового регулювання сфери інформаційної безпеки Європейського Союзу і Великобританії засвідчило про ефективність і дієвість проведених цими державами заходів на напрямках протидії зловмисному поводженню з інформацією. Відзначаємо, що для більш якісного проведення захисних дій у сфері інформаційної безпеки для нашої держави слід перейняти найбільш позитивні інструменти, якими є координація всіх задіяних у процесах володіння інформацією структур, усунення протиріч між учасниками проходження і передавання інформації, стабільність правового середовища, яким врегульовано різнотипні відносини у сфері володіння інформацією.

Запропоновано низку заходів, які торкаються основ нормативного супроводження сфери захисту інформаційної сфери. Не вдаючись до критики чинних інструментів протидії зазіханням на встановлений порядок взаємодії між суб'єктами передавання-отримання відомостей, виокремлено нагальну необхідність посилення, а подекуди і реформування чинної нормативно-правової бази як комплексного юридичного явища, що відіграє роль підґрунтя для ефективного функціонування всіх складових національної безпеки. З цією метою пропонуються зосередити законотворчі і технологічні зусилля на трьох основних напрямках, а саме: прискорити імплементацію позитивного європейського досвіду у систему захисту інформаційної сфери України, здійснити кодифікацію інформаційного права в умовах постійного моніторингу інформаційного середовища на предмет недопущення зловмисного і несанкціонованого втручання у цю сферу ким би то не було. Особливу увагу при цьому приділити протидії інформаційно-психологічним операціям, спрямованим на

розбалансування українського суспільства, поширення капітулянтських і панічних настроїв в Україні.

8. Обґрунтовано, що пріоритетним напрямком удосконалення вітчизняного законодавства у сфері інформаційної безпеки є категоричне відмежування від будь яких медіаконтактів з країною-агресором, що передбачає створення своєрідного «залізного купола», який би працював постійно, знешкоджуючи деструктивний вплив російської пропаганди на психологічний і моральний стан громадян України.

На нашу думку, такий стан у сфері інформаційної безпеки може бути досягнутий лише завдяки плідній співпраці науковців, законотворців та професійних представників, які безпосередньо опікуються проблемами захисту інформації.

Наостанок зазначаємо: ми свідомі того, що наведені авторські висновки не є довершеними, можливо, не мають достатньо переконливої аргументації чи не відповідають усталеним підходам до розуміння юридичного явища «інформаційна безпека». Проведеним дослідженням ми намагалися внести посильний вклад у процеси реформування законодавства сфери інформаційної безпеки, розроблення насправді дієвих інструментів захисту інформації на всіх рівнях її використання. Саме таке авторське бачення слугуватиме підґрунтям для продовження дискусії та ініціювання нових досліджень у цій мегаважливій сфері як складовій комплексного явища «національна безпека».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Словник української мови. URL : <http://www.inmo.org.ua/sum.html?wrld>.
2. Сучасний тлумачний словник української мови : 65000 слів. [заг. ред. В. В. Дубчинський]. Харків, 2006. 1008 с.
3. Про інформацію. Закон України №2657-XII від 02.10.1992. URL : <https://zakon.rada.gov.ua/laws/show/2657-12#Text>.
4. Про доступ до публічної інформації. Закон України № 2939-VI від 13.01.2011. URL : <https://zakon.rada.gov.ua/laws/card/2939-17>.
5. Тлумачний словник української мови. URL : <http://www.inmo.org.ua/sum.html?wrld=%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0>
6. Конституція України від 28 червня 1996 р. URL : <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>
7. Про національну безпеку України. Закон України № 2469-VIII від 21.06.2018. URL : <https://zakon.rada.gov.ua/laws/card/2469-19>.
8. Про основи національної безпеки України. Закон України № 964-IV від 19.06.2003. URL : <https://zakon.rada.gov.ua/laws/card/964-15>.
9. Довгань О. Д., Ткачук Т. Ю. Наукова рефлексія інформаційної безпеки України: від позитивізму до метафізики права. *Інформація і право*. 2018. № 4 (27). С. 79 – 89.
10. Золотар О. О. Генеза суспільних відносин щодо інформаційної безпеки людини. *Інформація і право*. 2018. № 1 (24). С. 139 – 148.
11. Псалтир. Харків: Фоліо, 2013. 574 с.
12. Плутарх. Сравнительные жизнеописания. [пер. с древнегреч. В. Алексеева]. Харьков: Фолио, 2013. 348 с.
13. Курбан О. В. Сучасні інформаційні війни в мережевому он-лайн просторі. Київ, 2016. 286 с.
14. Дзьобань О. П. Національна безпека України: концептуальні засади та світоглядний сенс: монографія. Харків: Майдан, 2007. 284 с.

15. Павленко О. Історія виникнення інформаційної безпеки. URL : <https://www.sutori.com/en/story/istoriia-vinikniennia-informatsiinoyi-biezpieki-94qRpbMUisHMP2JQSCupsNrN>.
16. Організаційно-правові основи захисту інформації з обмеженим доступом : навч. посіб. [А. Б. Тоцький, О. І. Тимошенко, А. М. Гуз та ін.]. Київ : Європейський університет, 2006. 232 с.
17. Соціально-правові основи інформаційної безпеки. [В. М. Петрик, А. М. Кузьменко, В. В. Остроухов та ін.] : навч. посіб. [за ред. В. В. Остроухова]. Київ : Росава, 2007. 496 с.
18. Оуен Р. Організаційна поведінка в освіті: Керівництво учбовими закладами та шкільна реформа. [пер. з англ. О. В. Христенко]. Харків: Каравела, 2003. 488 с.
19. Канигін Ю. М., Кушерець В. І. Біблія та майбутнє науки: орієнтири сучасних знань. Київ: Т-во «Знання України», 2009. 163 с.
20. Історія інформаційно-психологічного протидіювання. Підручник. [Є. Д. Скулиш, Я. М. Жарков, Л. Ф. Компанцев, В. В. Остроухов, В. М. Петрик] : [заг. ред. Є. Д. Скулиш]. Київ : Наук.-видав. відділ НА СБУ, 2012. 212 с.
21. Біленчук П. Д., Гель А. П., Семаков Г. С. Криміналістична тактика і методика розслідування окремих видів злочинів. Навчальний посіб. Київ : МАУП, 2007. 512 с.
22. Лисенко С. О. Історія досліджень інформаційної безпеки як об'єкта правовідносин. *Міжнародний науковий журнал «Верховенство права»*. 2016. № 2. С. 34 – 44.
23. Універсальний словник-енциклопедія. [кер. проекту О. Коваль ; гол. ред. ради М. Попович]. Київ, 1999. 1551 с. URL : <http://slovopedia.org.ua/29/53409/20574>. Html.
24. Перун Т. С. Методологічні засади дослідження механізму забезпечення інформаційної безпеки в Україні. 2017. URL : <https://science.lpnu.ua/sites/default/files/journal-paper/2018/jun/13373/48.pdf>.

25. Булавін Л., Чолпан П. Філософські і методологічні аспекти сучасної фізики. Київ : Інститут журналістики, 2004. 208 с.
26. Костицький М. В. Про діалектику як методологію юридичної науки. *Філософські та методологічні проблеми права*. 2012. № 1. С. 3 – 17.
27. Кельман М. С. Юридична наука: проблеми методології. Тернопіль : ТзОВ «Терно-граф», 2011. 492 с.
28. Онищук І. І. Методологія й техніка дослідження правового моніторингу. URL : <https://science.lpnu.ua/sites/default/files/journal-paper/2017/may/2492/vnulpurn201581324.pdf>.
29. Сурмин Ю. П. Теорія систем і системний аналіз : навч. посіб. Київ : МАУП, 2003. 368 с.
30. Качинський А. Б. Безпека, загрози і ризик: наукові концепції та математичні методи. Київ : Національна академія служби безпеки України, 2004. 471 с.
31. Арістова І. В. Методологія науки «інформаційне право». *ІТ право: проблеми і перспективи розвитку в Україні: збірник матеріалів науково-практичної конференції (Львів, 18 листопада 2016 р.)*. Львів, 2016. С. 11–18.
32. Скиба Ю. Класифікація методів наукових досліджень. *Вища освіта України*. 2016. № 2. С. 51 – 59.
33. Ковальчук В. В., Моїсєєв Л. М. Основи наукових досліджень: Навчальний посібник. Київ, 2004. 208 с.
34. Павліченко Є. В., Голинська М. І. Становлення порівняльного правознавства та порівняльно-правової методології. *Правовий часопис Донбасу*. 2019. № 1 (66). С. 18 – 24.
35. Шевченко А. Є., Француз А. Й., Кудін С. В. Методологічні засади нормативно-правового забезпечення інформаційної безпеки. *Ірпінський юридичний часопис : науковий журнал*. Ірпінь : Державний податковий університет, 2023. Випуск 2 (11). С. 48 – 55.

36. Братута О. Г. Засоби проведення наукового дослідження як елемент методологічного забезпечення української економічної науки. *Науковий вісник Миколаївського національного університету імені В. О. Сухомлинського*. 2016. № 14. С. 8 – 16.

37. Конверський А. Є. Логіка (традиційна та сучасна): підруч. для студ. вищих навч. закл. Київ : Центр учбової літератури, 2008. 536 с.

38. Основні методи наукового пізнання. URL : http://megalib.com.ua/content/4712_50_Osnovni_metodi_naykovogo_piznannya.html.

39. Закаленко О. В., Большакова О. В. Методико-антропологічні засади дослідження та розуміння права на адміністративний позов. *Право та інновації*. 2019. № 3 (27). С. 111 – 117.

40. Юркевич Х. Порівняльно-правовий метод в конституційно-правових дослідженнях. *Підприємництво, господарство і право*. 2019. Вип. 2. С. 156–160.

41. Проблеми сучасної конституціоналістики: навчальний посібник. [вступ та наукова редакція д.ю.н., професора НУ «ОЮА» М. П. Орзіха]. Випуск 1. Київ: Юрінком Інтер, 2010. 268 с.

42. Шигун М. М. Моделювання як метод наукових досліджень та інші методи пізнання дійсності. Міжнародний збірник наукових праць, 2016. Випуск 3 (9). С. 203 – 214.

43. Котенко М. В. Спосіб тлумачення правових норм як юридична категорія. *Науковий вісник Ужгородського національного університету, Серія Право*. 2013. Випуск 21. Частина II. Том 1. С. 62 – 64.

44. Шевченко А. Є., Старостюк А. В. Теорія держави і права: навчальний посібник. Ірпінь: Університет ДФС України, 2016. 187 с.

45. Теорія держави та права : навчальний посібник. [Є. В. Білозьоров, В. П. Власенко, О. Б. Горова, А. М. Завальний, Н. В. Заяць та ін.] ; [за заг. ред. С. Д. Гусарєва, О. Д. Тихомирова]. Київ : НАВС, Освіта України, 2017. 320 с.

46. Онищук І. І. Техніка юридичного письма в нормативно-правових актах: монографія. Київ : Лабораторія академ. дослідж. прав. регулювання та юрид. техніки, 2014. 226 с.

47. Балинська О. М. Семіотика права як філософсько-правова парадигма : дис. на здобуття наук. ступ. доктора юрид. наук; спец. 12.00.12 : філософія права. Львів, 2013. 485 с.

48. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки. URL. <http://troubleshooter.com.ua/ru/inform-bezopasnost/52-informatsijna-bezpeka-v-sistemi-zabezpechennya-natsionalnoji-bezpeki>.

49. Цимбалюк В. С., Бабінська А. В. Правове регулювання інформаційної безпеки в Україні: проблеми теорії та практики. URL : <http://applaw.knu.ua/index.php/arkhiv-nomeriv/2-8-2014/item/284-pravove-rehulyuvannya-informatsiynoyi-bezpeky-v-ukrayiniproblemy-teoriyi-ta-praktyky-tsymbaliuk-v-s-baby>.

50. Ніщименко О. А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. *Наше право*. 2016. № 1. С. 17 – 23.

51. 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.

52. Єсімов С. С. Шляхи удосконалення нормативно-правового регулювання в сфері інформаційної безпеки. *Наукові записки Львівського університету бізнесу та права*. 2013. Вип. 11. С. 73–76.

53. Кормич Б. А. Інформаційна безпека : організаційно-правові основи : навчальний посібник. Київ : Кондор, 2004. 382 с.

54. Громико І., Саханчук Т. Державна домінантність визначення інформаційної безпеки України в умовах протидії загрозам. *Право України*. 2008. № 8. С. 130 – 134.

55. Цимбалюк В. С. Інформаційне право (основи теорії і практики) : монографія. Київ : Освіта України, 2010. 388 с.
56. Калюжний Р. А. Інформаційне право України: концептуальні основи формування. *Науковий вісник Дніпропетровського юридичного інституту МВС України*. 2001. №3 (6). С. 234 – 244.
57. Гуцу С. Ф. Правові основи інформаційної діяльності: навч. посібник. Харків : Нац. Аерокосм. Ун-т «Харк. авіац. ін-т», 2009. 48 с.
58. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ : Видавничий дім «Гельветика», 2017. 168 с.
59. Харченко Л. С., Ліпкан В. А., Логінов О. В. Інформаційна безпека України: глосарій. [заг. ред. Р. А. Калюжний]. Київ : Текст, 2004. 136 с.
60. Мороз Н. С. Сутність інформації в контексті загальних принципів інформаційної безпеки. *Вісник Національного університету «Львівська політехніка». Юридичні науки*. 2016. № 845. С. 137 – 142.
61. Ярема О. Г., Єсімов С. С. Предмет правового забезпечення інформаційної безпеки в інформаційному праві. *Науковий вісник Львівського державного університету внутрішніх справ*. 2016. № 2. С. 244 – 252.
62. Кісілевич-Чорнойван О. Інформаційна безпека та міжнародна інформаційна безпека: проблема визначення понять. *Юриспруденція: теорія і практика*. 2009. № 8. С. 11 – 18.
63. Грабар Н. С. Інформаційна безпека в умовах становлення глобального інформаційного суспільства. *Державне управління: удосконалення та розвиток*. 2019. № 7. URL: <http://www.dy.nayka.com.ua/?op=1&z=1461> (дата звернення: 20.04.2022).
64. Данильян О. Г., Дзьобань О. П., Панов М. І. Національна безпека України: структура та напрямки реалізації: [навчальний посібник]. Харків : Фоліо, 2002. 285 с.

65. Проданюк Р. І. Інформаційна безпека в соціологічному контексті: до постановки проблеми. *Грані (науково-теоретичний альманах)*. 2018. Т. 21. № 4. С. 84 – 90.

66. Довгань О. Д., Ткачук Т. Ю. Концептуальні засади законодавчого забезпечення інформаційної безпеки України. *Інформація і право*. 2019. № 1 (28). С. 86 – 99.

67. Гончаров М. В. Сутність інформаційної безпеки в умовах розвитку сучасного суспільства. *Міжнародний науковий журнал «Інтернаука». Серія: «Юридичні науки»*. 2022. № 4. URL : <https://doi.org/10.25313/2520-2308-2022-4-8004>.

68. Луценко С. М. Особливості інформаційного забезпечення в державно-управлінській діяльності. *Держава та регіони : зб. наук. пр. Запоріжжя : Класичний приватний університет*, 2010. № 2. С. 41–45. (Серія “Державне управління”).

69. Хом’яков Д. О. Нормативно-правове регулювання інформаційної безпеки. *Актуальні проблеми управління інформаційною безпекою держави: збірник тез наукових доповідей науково-практичної конференції (Київ, 30 березня 2018 р.)*. Київ: НА СБУ, 2018. С. 182 – 184.

70. Гончаров М. В. Тенденції наукових поглядів у сфері нормативно-правового забезпечення інформаційної безпеки України. *Науковий вісник Ужгородського національного університету. Серія: «Право»*. 2022. № 70. С. 24 – 28.

71. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки. Закон України від 9.01.2007 р. *Відомості Верховної Ради України*. 2007. № 12. Ст. 102.

72. Про електронні комунікації. Закон України від 26 грудня 2020 р. № 1089-IX. URL : <https://zakon.rada.gov.ua/laws/card/1089-20>.

73. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України: дис. ... канд. юрид. наук: 12.00.01: теорія та історія держави і права; історія політичних і правових учень. Київ, 2007. 236 с.
74. Ліпкан В. А. Національна безпека України: навч. посіб. 2-ге вид. Київ : КНТ, 2009. 576 с.
75. Олійник О. В. Нормативно-правове забезпечення інформаційної безпеки в Україні. *Право і суспільство*. 2021. № 3. С. 132 – 137.
76. Золотар О. О. Інформаційна безпека людини: теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с.
77. Лисенко С. О. Конституційні засади розуміння інформаційної безпеки. *Публічне урядування*. 2016. № 4. С. 154–161.
78. Енциклопедія сучасної України. URL : <https://esu.com.ua/article-43500>.
79. Горобець К. В. Аксиосфера права: філософський і юридичний дискурс : монографія. Одеса : Фенікс, 2013. 218 с.
80. Горобець К. В. Аксиологічний підхід у кримінальному праві: зміст та значення. *Підприємництво, господарство і право*. 2016. № 12. С. 222 – 226.
81. Калінін С. А. Методологічний вимір аксіології права. *Наукові праці Національного університету «Одеська юридична академія»*. Одеса, 2011. С. 269 – 279.
82. Брижко В. М. Філософія права: аксіологія в сфері інформаційного права. *Інформація і право*. 2014. № 1 (10). С. 26 – 34.
83. Дзьобань О. П., Мануйлов Є. М. Інформаційна безпека в контексті інформаційної культури. *Інформація і право*. 2017. № 1 (20). С. 74 – 81.
84. Дзьобань О. П., Мануйлов Є. М. Соціокультурні аспекти інформаційної безпеки. *Матеріали IX Симпозіуму «Соціально-економічний розвиток системи фінансів і управління в інноваційному середовищі : проблеми, ефективність, перспективи»*. Харків, 2016. С. 368 – 369.
85. Milton B. G. Making Sense or Non-sense : Key Issues in the Information Age. *Canadian Vocational Journal*. 1989. Vol. 24. № 3. P. 5 – 9.

86. Предборський В. А. Економічна безпека держави : монографія. Київ : Кондор, 2005. 391 с.

87. Біленчук П. Д., Борисова Л. В., Неклонський І. М., Собина В. О. Правові засади інформаційної безпеки України : монографія. [за ред. П. Д. Біленчука]. Харків, 2018. 289 с.

88. Тихомиров О. О. Забезпечення інформаційної безпеки як функція сучасної держави : монографія. [заг. ред. Р. А. Калюжний]. Київ : Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. 196 с.

89. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції : навч. посіб. Київ : КНТ, 2006. 280 с.

90. Ткачук Т. Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України : дис. ... д-ра юрид. наук : 12.00.07. Ужгород, 2019. 487 с.

91. Шемчук В. В. Механізм забезпечення інформаційної безпеки держави: теоретично-методологічні основи. *Філософські та методологічні проблеми права*. 2019. № 1 (17). С. 51 – 60.

92. 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 р. № 287/2015 URL : <http://zakon.rada.gov.ua/laws/show/287/2015>.

93. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.

94. Абрамов В., Мошинський Р. Теорія безпеки та інститути (про вибір методологічної основи наукового дослідження системи національної безпеки). *Вісник Національної академії державного управління при Президентові України*. 2011. № 3. С. 5 – 13.

95. Ортинський В. Л. Удосконалення державної політики у сфері інформаційних технологій у контексті діяльності органів виконавчої влади.

Вісник Національного університету «Львівська політехніка». Юридичні науки. 2014. № 801. С. 3 – 8.

96. Дзьобань О. П., Панфілов О. Ю., Чемчекаленко Р. А. Методологічний контекст дослідження проблеми інформаційної безпеки. *Зовнішня торгівля: економіка, фінанси, право.* 2014. № 2. С. 171 – 180.

97. Про особливості державної політики із забезпечення державного суверенітету України на тимчасово окупованих територіях у Донецькій та Луганській областях. Закон України від 18.01.2018 р. № 2268-VIII. *Відомості Верховної Ради України.* 2018. № 10. Ст. 54.

98. 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 р. № 47/2017 URL : <http://zakon3.rada.gov.ua/laws/show/47/2017>.

99. Довгань О. Д., Ткачук Т. Ю. Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс. *Інформація і право.* 2018. № 2 (25). С. 73 – 85.

100. Ткачук Т. Ю. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. *Підприємництво, господарство і право.* 2017. № 10. С. 182 – 186.

101. Калюжний Р. А., Баєв О. О. Нормативно-правове забезпечення інформаційної безпеки України. *Правова інформатика.* 2009. № 4 (24). С. 5 – 12.

102. Про Стратегію інформаційної безпеки. Указ Президента України від 15.10.2021 № 685/2021. URL : <https://www.president.gov.ua/documents/6852021-41069>.

103. Про схвалення Стратегії розвитку інформаційного суспільства в Україні. Розпорядження Кабінету Міністрів України від 15.05.2013 р. № 386-р. URL : <http://zakon3.rada.gov.ua/laws/show/386-2013-%D1%80>.

104. Гнатюк С. Л. Проблеми впровадження сучасних стандартів інформаційної безпеки в умовах становлення національної системи кібербезпеки

України. Травень 2018 року. Аналітична записка. Національний інститут стратегічних досліджень при Президенті України. URL : http://www.niss.gov.ua/content/articles/files/1_cPPP-standarts_27-04_Gn_var_FIN732b6.pdf.

105. Тарасенко Н. Доктрина інформаційної безпеки України в оцінках експертів. *Резонанс*. 2017. № 18. С. 3 – 14. URL. <http://nbuviap.gov.ua/images/rezonans/2017/rez18.pdf>.

106. 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 р. № 47/2017 URL : <http://zakon3.rada.gov.ua/laws/show/47/2017>.

107. Григорчук М. В. Правовий захист суб'єктів господарювання (теорія і практика): монографія. Київ : Університет «КРОК», 2020. 376 с.

108. Торічний В. О. Інформаційне забезпечення державної політики як найважливіший фактор безпеки держави. *Pressing problems of public administration* 1(55)/2019. С. 77–85.

109. Макаренко Є. А. Міжнародне співробітництво у сфері інформаційної безпеки: регіональний контекст. *Актуальні проблеми міжнародних відносин*. 2011. Випуск 102 (Частина І). С. 51 – 62.

110. Фролова О. М. Роль ООН в системі міжнародної інформаційної безпеки. *Міжнародні відносини. Серія Політичні науки*. 2018. № 18–19. URL : http://journals.iir.kiev.ua/index.php/pol_n/article/view/3468.

111. Загальна Декларація прав людини від 10 грудня 1948 р. URL : https://zakon.rada.gov.ua/laws/show/995_015#Text.

112. Міжнародний пакт про економічні, соціальні і культурні права від 16 грудня 1966 р. URL : https://zakon.rada.gov.ua/laws/show/995_042#Text.

113. Міжнародний пакт про громадянські і політичні права від 16 грудня 1966 р. URL : https://zakon.rada.gov.ua/laws/show/995_043#Text.

114. Європейська конвенція з прав людини від 4 листопада 1950 р. URL : https://zakon.rada.gov.ua/laws/show/995_004?find=1&text.
115. Dadgeon V. United Kingdom, 4 E.H.H.R. 149. p. 60.
116. Маркова М. В., Марков А. Р. Інформаційно-психологічна війна проти населення України як сучасна реальність: стан проблеми і шляхи подолання наслідків. *Інтегровані комунікації*. 2016. № 2. С. 73 – 85.
117. Черкашин П. С. Концепція «вільного потоку інформації» та питання інформаційної безпеки держави: міжнародно-правові аспекти. *Наука і молодь. Гуманітарна серія. Збірник наукових праць*. 2012. Вип. 11-12. С. 135 – 138.
118. Устав Организации Объединённых Наций и Устав Международного Суда. Офіційний інтернет-сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/995_010.
119. Про ратифікацію Конвенції про кіберзлочинність. Закон України від 07.09.2005 р. № 2824-IV. *Відомості Верховної Ради України*. 2006. № 5. Ст. 71.
120. Конвенція ООН про використання електронних повідомлень у міжнародних договорах від 23 листопада 2005 р. URL: https://www.un.org/ru/documents/decl_conv/conventions/elect_com.shtml.
121. Бойченко О. В. Міжнародна інформаційна безпека: проблеми і перспективи. *Форум права*. 2009. № 3. С. 74 – 79. URL: http://nbuv.gov.ua/UJRN/FP_index.htm_2009_3_13.
122. Резолюція 60/45, прийнята Генеральною Асамблеєю Організації Об'єднаних Націй «Досягнення у галузі інформатизації та телекомунікацій в контексті міжнародної безпеки» від 8 грудня 2005 р. URL: https://zakon.rada.gov.ua/laws/show/995_e45/card2#Card.
123. Резолюція 64/211, прийнята Генеральною Асамблеєю Організації Об'єднаних Націй «Створення глобальної культури кібербезпеки та оцінка національних зусиль із захисту найважливіших інформаційних інфраструктур» від 21 грудня 2009 р. URL: <https://undocs.org/ru/A/RES/64/211>.

124. Резолюція 65/141, прийнята Генеральною Асамблеєю Організації Об'єднаних Націй «Використання інформаційно-комунікаційних технологій з метою розвитку» від 20 грудня 2010 р. URL: <https://undocs.org/ru/A/RES/65/141>.

125. Про друковані засоби масової інформації (пресу) в Україні. Закон України від 16.11.1992 № 2782-XII. *Відомості Верховної Ради України*. 1993. № 1. Ст. 1.

126. Про науково-технічну інформацію. Закон України від 25.06.1993 № 3322-XII. *Відомості Верховної Ради України*. 1993. № 33. Ст. 345.

127. Про телебачення і радіомовлення. Закон України від 21.12.1993 № 3759-XII. *Відомості Верховної Ради України*. 1994. № 10. Ст. 43.

128. Про авторське право і суміжні права. Закон України від 23.12.1993 № 3792-XII. *Відомості Верховної Ради України*. 1994. № 13. Ст. 64.

129. Про державну таємницю». Закон України від 21.01.1994 р. № 3855-12. *Відомості Верховної Ради України*. 1994. № 16. Ст. 93.

130. Про захист інформації в автоматизованих системах. Закон України від 05.07.1994 № 80/94-ВР. *Відомості Верховної Ради України*. 1994. № 31. Ст. 286.

131. Про інформаційні агентства. Закон України від 28.02.1995 № 74/95-ВР. *Відомості Верховної Ради України*. 1995. № 13. Ст. 83.

132. Про рекламу. Закон України від 03.07.1996 № 270/96-ВР. *Відомості Верховної Ради України*. 1996. № 39. Ст. 181.

133. Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації. Закон України від 23.09.1997 № 539/97-ВР. *Відомості Верховної Ради України*. 1997. № 49. Ст. 299.

134. Про державну підтримку засобів масової інформації та соціальний захист журналістів. Закон України від 23.09.1997 № 540/97-ВР. *Відомості Верховної Ради України*. 1997. № 50. Ст. 302.

135. Про Концепцію Національної програми інформатизації. Закон України від 04.02.1998 № 75/98-ВР. *Відомості Верховної Ради України*. 1998. № 27-28. Ст. 182.

136. Про Національну програму інформатизації. Закон України від 04.02.1998 № 74/98- ВР. *Відомості Верховної Ради України*. 1998. № 27-28. Ст. 182.

137. Про захист суспільної моралі. Закон України від 20.11.2003 № 1296-IV. *Відомості Верховної Ради України*. 2004, № 14, ст.192.

138. Про електронні документи та електронний документообіг. Закон України від 22.05.2003 № 851-IV. *Відомості Верховної Ради України*. 2003. № 36. Ст. 275.

139. Про електронний цифровий підпис. Закон України від 22.05.2003 № 852 IV. *Відомості Верховної Ради України*. 2003. № 36. Ст. 276.

140. Про звернення громадян: Закон України від 02.10.1996 № 393/96- ВР. *Відомості Верховної Ради України*. 1996. № 47. Ст. 256.

141. Про затвердження Концепції технічного захисту інформації в Україні» від 08.10.1997 № 1126. URL : <http://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF>.

142. Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації систем і засобів автоматизованої обробки та передачі даних» від 04.02.1998 №121. URL : <http://zakon.rada.gov.ua/laws/show/121-98-%D0%BF/ed20110903>.

143. Про заходи щодо посилення контролю за обґрунтованістю проектів інформатизації діяльності центральних органів виконавчої влади» від 16.02.1998 № 160. URL : <http://zakon.rada.gov.ua/laws/show/160-98-%D0%BF/ed20110903>.

144. Про затвердження Положення про формування та виконання Національної програми інформатизації» від 31.08.1998 № 1352. URL : <http://zakon.rada.gov.ua/laws/show/1352-98-%D0%BF>.

145. Про затвердження Порядку локалізації програмних продуктів (програмних засобів) для виконання Національної програми інформатизації» від 16.11.1998 № 1815. URL : <http://zakon.rada.gov.ua/laws/show/1815-98-%D0%BF>.

146. Про затвердження Порядку формування та виконання регіональної програми і проекту інформатизації» від 12.04.2000 № 644. URL : <http://zakon.rada.gov.ua/laws/file/644-2000-%D0%BF>.

147. Про Урядову комісію з питань інформаційно-аналітичного забезпечення діяльності органів виконавчої влади» від 07.05.2000 № 777. URL : <http://zakon.rada.gov.ua/laws/show/777-2000-%D0%BF>.

148. Про затвердження Порядку формування та виконання галузевої програми і проекту інформатизації» від 18.12.2001 № 1702. URL : <http://zakon.rada.gov.ua/laws/show/1702-2001-%D0%BF>.

149. Про Концепцію національної інформаційної політики» від 03.04.2003 № 687-IV. URL : <http://zakon2.rada.gov.ua/laws/show/687-15>.

150. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 09.01.2007 № 537-V. *Відомості Верховної Ради України*. 2007. № 12. Ст. 102.

151. Про захист персональних даних. Закон України від 01.06.2010 № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481.

152. Про адміністративні послуги. Закон України від 06.09.2012 № 5203-VI. *Відомості Верховної Ради України*. 2013. № 32. Ст. 409.

153. Литвин Н. А. Адміністративно-правове забезпечення інформаційної діяльності органів державної фіскальної служби України : дис. ... канд. юрид. наук: 12.00.07. Ірпінь, 2018. 497 с.

154. Про правила планування та координації політики національної безпеки. Закон Грузії від 03 квітня 2015 р. № 1300000000.05.001.017637. URL : <https://matsne.gov.ge/ka/document/view/2764463?publication=9>.

155. Види джерел загроз. URL : https://stud.com.ua/21603/ekonomika/vidi_dzherel_zagroz.

156. Горбулін В. П., Биченок М. М. Проблеми захисту інформаційного поля України: монографія. Київ : Інтертехнологія, 2009. 136 с.

157. Нехай В. А. Інформаційна безпека як складова економічної безпеки підприємств. *Науковий вісник Міжнародного гуманітарного університету. Серія: Економіка і менеджмент*. 2017. Вип. 24 (2). С. 137 – 140.

158. Богуш В. М., Кривуца В. Г., Кудін А. М. Інформаційна безпека: Термінологічний навчальний довідник. Київ : ООО «ДВК», 2004. 508 с.

159. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи». URL : <http://www.justinian.com.ua/article.php?id=3222>.

160. Marutian R. R. Recommendations for improving the information security policy of Ukraine [Rekomendatsii shchodo vdoskonalennia polityky zabezpechennia informatsiinoi bezpeky Ukrainy]. URL : http://www.dsaua.org/index.php?option=com_content&view=article&id=198%3A2014-08-13-12-55-48&catid=66%3A2010-12-13-08-48-53&Itemid=90&lang=uk.

161. Марущак А. І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки. *Державна безпека України*. 2011. № 21. С. 92 – 95.

162. Євтушевська О. А. Інформаційна безпека як елемент підвищення ефективності комплексного контролю підприємств водного транспорту. *Зовнішня торгівля: економіка, фінанси, право. Науковий журнал. Серія: Економічні науки*. 2015. № 5-6 (82-83). С. 157 – 162.

163. Актуальні виклики та загрози регіональній безпеці: висновки для України ; [за заг. ред. К. А. Кононенка: аналіт. доп. Б. Парахонський, Г. Яворська]. Київ : НІСД, 2014. 48 с.

164. Борисова Л. В., Тулупов В. В. Інформаційна безпека як визначальний компонент національної безпеки України. *Право і безпека*. 2013. № 1 (48). С. 39 – 42.

165. Олійник О. В. Організаційно-правові засади захисту інформаційних ресурсів України : автореф. дис. ... канд. юрид. наук : 12.00.07. Київ, 2006. 20 с.

166. Гуржій Т. О. Інформаційне право: виклики гібридної війни. *Зовнішня торгівля: економіка, фінанси, право*. 2018. № 4. С. 16 – 26.

167. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України : дис. на здобуття наукового ступеня д-ра юрид. наук. : 12.00.07. Харків, 2004.

168. Стратегія національної безпеки України. Указ Президента України від 14 вересня 2020 року № 392/2020. URL : <https://www.president.gov.ua/documents/3922020-35037>.

169. Стратегія інформаційної безпеки. Указ Президента України від 28 грудня 2021 року № 685/2021. URL : <https://zakon.rada.gov.ua/laws/show/685/2021#Text>.

170. Стратегія кібербезпеки України. Указ Президента України від 26 серпня 2021 року № 447/2021. URL : <https://www.president.gov.ua/documents/4472021-40013>.

171. Любохинець Л. С., Поплавська О. В. Світова практика забезпечення інформаційної безпеки в сучасному глобалізованому середовищі. *Бізнес-навігатор*. 2017. Вип. 4-1. С. 93 – 97.

172. Онищенко С. В., Білько С. С. Загрози інформаційній безпеці національної економіки. *Науковий вісник Одеського національного економічного університету. Збірник наукових праць*. 2022. №11-12 (300-301). С. 50 – 56.

173. Еделєва М. А. Забезпечення інформаційної безпеки в контексті реалізації державної інформаційної політики. *Вісник Маріупольського державного університету*. 2017. Вип. 19. С. 133 – 141.

174. Оніщенко Н. С. Сприйняття права в умовах демократичного розвитку: проблеми, реалії, перспективи: монографія. [відповід. ред. Ю. С. Шемшученко]. Київ : ТОВ Видавництво «Юридична думка», 2008. 320 с.

175. Європейські критерії безпеки інформаційних технологій. URL : <http://um.co.ua/12/12-7/12-73899.html>.

176. Common Criteria for Information Technology Security Evaluation. URL : https://www.commoncriteriaportal.org/files/ccfiles/CCPART_2V3.1R4.pdf.

177. Нестеряк Ю. В. Міжнародні критерії інформаційної безпеки держави: теоретико-методологічний аналіз. *Вісник НАДУ*. 2013. № 3. С. 40 – 45.

178. Communication from the European Commission: Network and Information Security: Proposal for a European Policy Approach. COM (2001) 298. URL : http://ec.europa.eu/information_society/eeurope/2002/news_library/pdf_files/netsec_en.pdf.

179. Safer Internet Programme. URL : http://ec.europa.eu/information_society/activities/sip/policy/programme/current_prog/index_en.

180. Communication from the Commission: Towards a general policy on the fight against cyber crime. COM (2007). URL : http://eurlex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf.

181. Communication from the Commission on Critical Information Infrastructure Protection: Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience. COM (2009)149. URL : http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm.

182. Костенко О. В. Європейські стандарти правового регулювання обігу інформації з обмеженим доступом у роботі органів прокуратури. *Науковий вісник Ужгородського національного університету: серія «Право»*. 2015. Випуск 34, том 3. С. 109 – 114.

183. Про доступ до інформації, яка знаходиться в розпорядженні державних органів: Рекомендації Ради Європи № R (81)19. URL : <http://medialaw.org.ua/library/rekomendatsiya-r-81-19-pro-dostup-doinformatsiyi-shho-znahodytsya-u-rozporyadzhenni-derzhavnyh-organiv>.

184. General Assembly Resolution «The right to privacy in the digital age», A/RES/68/167: URL : <http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx>.

185. Гнатюк С. Л. Особливості захисту персональних даних в сучасному кіберпросторі: правові та техніко-технологічні аспекти: Аналітична доповідь. Київ : Нац. ін-т стратегічних досліджень, 2013. 51 с.

186. Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року. URL : http://zakon2.rada.gov.ua/laws/show/994_242.

187. Nigel Waters, Graham. Interpreting the Security Principle. URL : <http://www.cyberlawcentre.org/ipp/wp/WP1%20Security.pdf>.

188. Василенко Д. П., Маслак В. І. Законодавство провідних країн світу в сфері захисту інформації. *Вісник КДУ імені Михайла Остроградського*, 2010. Випуск № 61, частина 1. С.128 – 132.

189. Ткачук Т. Ю. Дисертація на здобуття наук. ступеня д-ра юрид. наук за спеціальністю 12.00.07. Ужгород, 2019. 487 с.

190. Рябоконь О. Державна інформаційна політика з формування інформаційного суспільства: зарубіжний досвід. *Наукові праці Національної бібліотеки України імені В. І. Вернадського*. 2016. Вип. 43. С. 97–114.

191. Чухно А. А. Национальные и мировые программы создания информационного общества. *Наукове пізнання: методологія та технологія*. 2008. № 10. С. 94 – 102.

192. The Data Protection Act. URL : <https://www.gov.uk/data-protection>.

193. National cyber security strategy 2016-2021. URL : <https://www.cipfa.org/~media/files/services/ccfc/hm%2520government%2520national%2520cyber%2520security%2520strategy%25202016%25202021.pdf+&cd=7&hl=ru&ct=clnk&gl=ua>.

194. Угода про політичне співробітництво, вільну торгівлю і стратегічне партнерство між Україною та Сполученим Королівством Великої Британії і Північної Ірландії (ратифіковано Законом № 1100-IX від 16.12.2020). URL : https://zakon.rada.gov.ua/laws/show/826_001-

20?find=1&text=%D0%BF%D0%B0%D1%80%D1%82%D0%BD%D0%B5%D1%80#w1_20.

195. A Global Model: UK's «National Cyber Security Strategy» URL : <https://www.securityroundtable.org/global-model-uks-national-cyber-securitystrategy>.

196. National cyber security strategy of Spain. URL : https://www.enisa.europa.eu/topics/national-cyber-securitystrategies/ncss-map/NCSS_ESen.pd.

197. Digital agenda 2020 for Estjnia. URL : https://www.mkm.ee/sites/default/files/digital_agenda_2020_estonia_engf.pdf.

198. Брижко В. До питання сучасної інформаційної політики. *Вісник Академії управління МВС*. 2009. № 2. С. 27 – 47.

199. Горелихина О. А., Шлиньков А. А. Правовий захист персональних даних в Німеччині. *Проблеми економіки і права*. 2012. № 3. С. 322 – 326.

200. Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (IuKDG) vom 20.12.1990. URL : <http://www.gesetze-iminternet.de>.

201. Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes vom 14.08.2009. URL : <https://www.bsi.bund.de>.

202. Cyber-Sicherheitsstrategie für Deutschland vom 23.02.2011. URL : <https://www.bsi.bund.de>.

203. Gesetz zur Regelung der Rahmenbedingungen für Informationsund Kommunikationsdienste (IuKDG) vom 20.12.1990. URL : <http://www.gesetzeiminternet.de>.

204. Чернухін І. О. Досвід Федеративної республіки Німеччини в побудові системи захисту інфраструктури від кібернетичних загроз. *Міжнародний досвід у сфері забезпечення інформаційної безпеки людини, суспільства, держави*. 2014. № 1 (14). С. 27 – 43.

205. Information systems defence and security. France's strategy. URL : https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_

Information_system_defence_and_security_-_France_s_strategy.pdf (дата звернення 27.03.2023).

206. Шевченко А. Є., Павлюх О. А., Санжаров В. А. Питання кібербезпеки в сучасному Італійському законодавстві: національний безпековий периметр. *Наукові тренди постіндустріального суспільства: матеріали IV Міжнародної наукової конференції. (м. Суми, 31 березня 2023 р.)*. Міжнародний центр наукових досліджень. Вінниця: Європейська наукова платформа, 2023. С. 80 – 82.

207. National cyber security strategy - NIS Capacities. URL : <https://cyberwiser.eu/italy-it>.

208. Europe's Way to the Information Society. An Action Plan. URL : <http://i.lekciya.com.ua/doc/3177/index.html?page=17> (accessed 12 January 2020).

209. The National plan for cyberspace protection and ICT security. URL : <https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italiannational-cyber-security-plan.pdf>.

210. Тихомирова Є. Б., Смик Р. П. Інформаційна політика Польщі. *Матеріали V Всеукраїнської науково-практичної конференції «Сучасні проблеми гуманітаристики: світоглядні пошуки, комунікативні та педагогічні стратегії»*. Рівне, 2015. С.113 – 115.

211. Across Europe? Nations Mold Cyber Defenses. URL : <http://archive.defensenews.com/article/20130709/DEFREG01/307090008/AcrossEurope-Nations-Mold-Cyber-Defenses>.

212. Countering cyberterrorism. URL : http://msz.gov.pl/en/foreign_policy/security_policy/international_terrorism/countering_cyber_terrorism/&printMode=true.

213. Доктрина кібербезпеки Польщі. URL : constitutions.ru/?p=11083.

214. Концепції та стратегії міжнародної інформаційної безпеки. URL : <http://international-relations-tourism.karazin.ua/themes/irtb/resources/001ff6a35a7dfe2b845cf670db0c828b.pdf>.

215. Biuro Bezpieczeństwa Narodowego. URL : en.bbn.gov.pl.
216. У Польщі створили центр боротьби з російською пропагандою. URL : https://zaxid.net/u_polshhistvorili_tsentr_borotbi_z_rosiyskoyu_propagandoyu_n1424662.
217. Laura Chappell, Palgrave Macmillan. Germany, Poland and the Common Security and Defence Policy. Converging Security and Defence Perspectives in an Enlarged EU. 29 august 2012. 232 p.
218. Баранов А. А., Брижко В. М., Базанов Ю. К. Права людини і захист персональних даних. URL: http://library.khpg.org/files/docs/Kn_L_.pdf.
219. Nemzeti Adatvédelmi és Információszabadság Hatóság (Hungarian National Authority for Data Protection and Freedom of Information): URL : <http://www.naih.hu/uegyfelszolgalat,--kapcsolat.html>.
220. Ткачук Т. Ю. Забезпечення інформаційної безпеки в країнах Центральної Європи. *Юридичний науковий електронний журнал*. 2017. № 5. С. 105 – 110.
221. Телеховський Ю. Г. Досвід трансформації спецслужб в Угорщині: висновки для України. *Стратегічні пріоритети*. 2013. № 3 (28). С. 151 – 156.
222. Затинайко О., Павленко В., Бочарніков В., Свешніков С. Політика безпеки і воєнно-політичні відносини Угорщини. *Наука і оборона*. 2014. № 1. С. 9 – 18.
223. Act on the Electronic Information Security of Central and Local Government Agencies): URL : http://njt.hu/cgi_bin/njt_doc.cgi?docid=160206.240508.
224. Hungary's National Security strategy (2012). URL : <http://2010-2014.kormany.hu/download/4/32/b0000/National%20Security%20Strategy.pdf>.
225. National Cyber Security Strategy of Hungary (2013): URL : <http://www.nbf.hu/anyagok/Government%20Decision%20No%20>.
226. Ковтун С. В. Інформаційна безпека: підручник. Харків: Вид. ХНЕУ, 2009. 368 с.

227. Шляхи удосконалення системи державного управління забезпеченням національної безпеки України: монографія. [Г. П. Ситник, В. І. Абрамов, О. Г. Бортнікова, М. М. Шевченко та ін.] ; [за ред. Г. П. Ситника, В. І. Абрамова]. Київ : НАДУ, 2012. 536 с.

228. Шатун В. Т. Інформаційна безпека – невід’ємна складова національної безпеки України. *Наукові праці Чорноморського державного університету імені Петра Могили комплексу «Києво-Могилянська академія»*. 2016. Т. 267. Вип. 255. С. 174 – 180.

229. Політанський В. С. Інформаційне суспільство в Україні: від зародження до сьогодення. *Науковий вісник Ужгородського національного університету: серія «Право»*. 2017. Випуск 42. С. 16 – 22.

230. Конах В. К. Національний інформаційний простір України: проблеми формування та державного регулювання: аналітична доповідь. Київ : НІСД, 2014. 76 с.

231. Курбан О. В. Основи сучасної національної інформаційної безпеки України. *Вісник ХДАК*. 2017. Вип. 50. С. 55 – 66.

232. Левченко О. В. Нормативно-правове регулювання інформаційної безпеки України: стан та шляхи вирішення проблем. URL : www.hups.mil.gov.ua/periodic-app/article/4075/zhups2014.pdf.

233. Піскорська Г. А. Роль сучасних інформаційних технологій у забезпеченні інформаційної безпеки України. *Актуальні проблеми міжнародних відносин: [зб. наук. пр.]*. Київ. нац. ун-т ім. Т. Шевченка, Ін-т міжнар. відносин; [редкол.: Л.В. Губерський (голов. ред.) та ін.]. Київ, 2008. Вип. 74, ч. 1. С. 123 – 127.

234. Кобко Є. В. Моніторинг загроз національній безпеці держави: зарубіжний досвід та українські реалії. *Науковий вісник Національної академії внутрішніх справ*. 2018. № 1 (106). С. 123 – 134.

235. Державна політика забезпечення національної безпеки України: основні напрямки та особливості здійснення. : монографія. [М. Ф. Криштанович, Я. Я. Пушак, М. І. Флейчук, В. І. Франчук]. Львів : Сполом, 2020. 418 с.

236. Іващенко О. В., Гельман В. М. Фінансово-економічна безпека держави. *Збірник наукових праць Таврійського державного агротехнологічного університету*. 2013. № 2 (1). С. 121 – 131.

237. Француз А. Й., Кудін С. В., Федорчук О. В. Сутність інформаційної безпеки України. *Право.ua*. 2022. № 4. С. 5–10.

238. Новицька Н. Б., Петрик В. М., Кудико В. М. Дезінформування як засіб ведення інформаційної війни російської федерації проти України *Ірпінський юридичний часопис: науковий журнал*. 2022. Вип. 1 (8). С.118–130.

239. Косілова О. І., Солодовнікова Х. К. Права і свободи людини і громадянина v. s. штучний інтелект: проблемні аспекти. *Інформація і право*. 2020. № 4(35). С. 56–66.

240. Косілова О. І., Федірко І. П. Розвиток е-урядування в Україні на шляху до реалізації прав і свобод громадян. *Журнал східноєвропейського права*. 2020. № 82. С. 57–68.

«ЗАТВЕРДЖУЮ»

Директор Навчально-наукового

інституту права

Державного податкового університету,

докреєтор юридичних наук, професор

Топчій В.В.

2023 року

АКТ

**впровадження результатів дисертаційного дослідження
в наукову діяльність**

Комісія у складі: завідувача кафедри теоретико-правових дисциплін Державного податкового університету, д.ю.н., професора Шевченка А.Є.; професора кафедри теоретико-правових дисциплін Державного податкового університету, д.ю.н., професора Кудіна С.В.; доцента кафедри теоретико-правових дисциплін Державного податкового університету, к.політ.н., доцента Косілової О.І. склала цей акт про те, що під час виконання науково-дослідної роботи на тему «Забезпечення дії права в процесі реалізації державної політики» (номер державної реєстрації 0117U006224), яка виконується на кафедрі теоретико-правових дисциплін Державного податкового університету, було використано матеріали дисертаційної роботи Гончарова Миколи Вікторовича на тему «Теоретико-правові основи регулювання інформаційної безпеки в Україні»:

1. Гончаров М. В. Сутність інформаційної безпеки в умовах розвитку сучасного суспільства. *Міжнародний науковий журнал «Інтернаука»*. Серія: «Юридичні науки». 2022. № 4 <https://doi.org/10.25313/2520-2308-2022-4-8004>
2. Гончаров М. В. Тенденції наукових поглядів у сфері нормативно-правового забезпечення інформаційної безпеки України. *Науковий вісник Ужгородського національного університету*. Серія: «Право». 2022. № 70. С. 24–28.
3. Гончаров М. В. Досвід нормативно-правового забезпечення інформаційної безпеки в країнах Європейського Союзу. *Наше право*. № 2. 2023. С. 144–150.
4. Andrii M. Blahodarnyi, Olha O. Barabash, Andrii V. Honcharov, Mykola V. Honcharov, Volodymyr A. Shatilo. Local Self-government in European Countries: General Characteristics, Comparison and Ukrainian Realities. *LEX LOCALIS - journal of local self-government* Vol. 21, No. 3, pp. 683-706, July 2023.
5. Гончаров М. В. До питання використання інформаційних систем та технологій у сучасному суспільстві. *Кибербезпека в Україні: правові та організаційні питання : матеріали всеукр. наук.-практ. конф., м. Одеса, 30 листопада 2018 р.* – Одеса : ОДУВС, 2018 – С. 94–95.
6. Гончаров М. В. Сутність інформаційної безпеки в умовах розвитку сучасного суспільства. *Кибербезпека в Україні: правові та організаційні питання: матеріали міжн. наук. практ. конф., м. Одеса, 22 листопада 2019 р.* Одеса : ОДУВС, 2019. С. 4–5.

7. Гончаров М. В. Деякі аспекти дослідження інформаційної безпеки в діяльності держави. *Правова наука і державотворення в Україні у світлі сучасних глобалізаційних викликів: історія, теорія, практика (до 25-ї річниці Конституції України): матеріали Всеукраїнської науково-практичної конференції (м. Маріуполь – м. Кривий Ріг, 11 червня 2021 року)*. Маріуполь : ДонДУВС, 2021. С. 133–135.

8. Гончаров М. В. Деякі аспекти дослідження сутності інформаційної безпеки. *Інформація та документ у сучасному науковому дискурсі: матеріали VII Всеукраїнської дистанційної науково-практичної конференції. (Івано-Франківськ, 20 травня 2022 р.)*. Івано-Франківськ: ІФНТУНГ, 2022. С. 13–16.

9. Honcharov A.V., Honcharov M.V. Some aspects the conceptual study of regulatory and legal ensurement of information security. *The IX International Scientific and Practical Conference «Analysis of the problems of science and modern education»*, 06 – 08 March, 2023. Prague, Czech Republic. P. 77–80.

10. Гончаров А. В., Гончаров М. В. Життєвий шлях, юридичні погляди та педагогічна діяльність В. Г. Кукольника (1765–1821). *Правовий часопис Донбасу*: Зб. наук. праць № 1(66). Кривий Ріг.: Донецький юридичний інститут МВС України, 2019. С. 13–18.

11. Zaiets O.M., Honcharov M.V. Internet of Things During the Pretrial Investigation of Criminal Offenses European Reforms Bulletin scientific peer-reviewed journal. 2021. № 4. С. 53–58.

Завідувач кафедри теоретико-правових дисциплін,
д.ю.н., професор



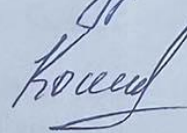
Анатолій Шевченко

Професор кафедри теоретико-правових дисциплін,
д.ю.н., професор



Сергій Кудін

Доцент кафедри теоретико-правових дисциплін,
к.політ.н., доцент



Ольга Косілова

«ЗАТВЕРДЖУЮ»

Директор Навчально-наукового

інституту права

Державного податкового університету,

доктор юридичних наук, професор

Гончаров Миколи Вікторовича

Гончаров М.В. 2023 року



АКТ

впровадження результатів дисертаційного дослідження в освітній процес

Комісія у складі: завідувача кафедри теоретико-правових дисциплін Державного податкового університету, д.ю.н., професора Шевченка А.Є.; професора кафедри теоретико-правових дисциплін Державного податкового університету, д.ю.н., професора Кудіна С.В.; доцента кафедри теоретико-правових дисциплін Державного податкового університету, к.політ.н., доцента Косілової О.І. склала цей акт про те, що основні результати дисертаційної роботи Гончарова Миколи Вікторовича, які викладені у його наукових роботах:

1. Гончаров М. В. Сутність інформаційної безпеки в умовах розвитку сучасного суспільства. *Міжнародний науковий журнал «Інтернаука»*. Серія: «Юридичні науки». 2022. № 4 <https://doi.org/10.25313/2520-2308-2022-4-8004>
2. Гончаров М. В. Тенденції наукових поглядів у сфері нормативно-правового забезпечення інформаційної безпеки України. *Науковий вісник Ужгородського національного університету*. Серія: «Право». 2022. № 70. С. 24–28.
3. Гончаров М. В. Досвід нормативно-правового забезпечення інформаційної безпеки в країнах Європейського Союзу. *Наше право*. № 2. 2023. С. 144–150.
4. Andrii M. Blahodarnyi, Olha O. Barabash, Andrii V. Honcharov, Mykola V. Honcharov, Volodymyr A. Shatilo. Local Self-government in European Countries: General Characteristics, Comparison and Ukrainian Realities. *LEX LOCALIS - journal of local self-government* Vol. 21, No. 3, pp. 683-706, July 2023.
5. Гончаров М. В. До питання використання інформаційних систем та технологій у сучасному суспільстві. *Кибербезпека в Україні: правові та організаційні питання : матеріали всеукр. наук.-практ. конф., м. Одеса, 30 листопада 2018 р.* – Одеса : ОДУВС, 2018 – С. 94–95.
6. Гончаров М. В. Сутність інформаційної безпеки в умовах розвитку сучасного суспільства. *Кибербезпека в Україні: правові та організаційні питання: матеріали міжн. наук. практ. конф., м. Одеса, 22 листопада 2019 р.* Одеса : ОДУВС, 2019. С. 4–5.
7. Гончаров М. В. Деякі аспекти дослідження інформаційної безпеки в діяльності держави. *Правова наука і державотворення в Україні у світлі сучасних глобалізаційних викликів: історія, теорія, практика (до 25-ї річниці Конституції*

України): матеріали Всеукраїнської науково-практичної конференції (м. Маріуполь – м. Кривий Ріг, 11 червня 2021 року). Маріуполь : ДонДУВС, 2021. С. 133–135.

8. Гончаров М. В. Деякі аспекти дослідження сутності інформаційної безпеки. *Інформація та документ у сучасному науковому дискурсі: матеріали VII Всеукраїнської дистанційної науково-практичної конференції. (Івано-Франківськ, 20 травня 2022 р.)*. Івано-Франківськ: ІФНТУНГ, 2022. С. 13–16.

9. Honcharov A.V., Honcharov M.V. Some aspects the conceptual study of regulatory and legal ensurement of information security. *The IX International Scientific and Practical Conference «Analysis of the problems of science and modern education»*, 06 – 08 March, 2023. Prague, Czech Republic. P. 77–80.

10. Гончаров А. В., Гончаров М. В. Життєвий шлях, юридичні погляди та педагогічна діяльність В. Г. Кукольника (1765–1821). *Правовий часопис Донбасу*: 36. наук. праць № 1(66). Кривий Ріг.: Донецький юридичний інститут МВС України, 2019. С. 13–18.

11. Zaiets O.M., Honcharov M.V. Internet of Things During the Pretrial Investigation of Criminal Offenses European Reforms Bulletin scientific peer-reviewed journal. 2021. № 4. С. 53–58.

використовуються в освітньому процесі кафедри теоретико-правових дисциплін Державного податкового університету під час викладання дисциплін: «Історія держави і права України», «Теорія держави і права», «Історія вчень про державу і право», «Історія українського права», «Конституційного права України» і мають важливе теоретичне значення при підготовці навчальних посібників, лекцій, методичних матеріалів.

Комісія дійшла висновку, що результати дисертаційної роботи на здобуття наукового ступеня доктора філософії за спеціальністю 081 Гончарова Миколи Вікторовича на тему «Теоретико-правові основи регулювання інформаційної безпеки в Україні»: можна вважати впровадженими в освітній процес кафедри теоретико-правових дисциплін Державного податкового університету.

Завідувач кафедри теоретико-правових дисциплін,
д.ю.н., професор

Анатолій Шевченко

Професор кафедри теоретико-правових дисциплін,
д.ю.н., професор

Сергій Кудін

Доцент кафедри теоретико-правових дисциплін,
к.політ.н., доцент

Ольга Косілова

Додаток В

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

1. Гончаров М. В. Сутність інформаційної безпеки в умовах розвитку сучасного суспільства. *Міжнародний науковий журнал «Інтернаука»*. Серія: «Юридичні науки». 2022. № 4. С. 77–82. URL: <https://www.inter-nauka.com/issues/law2022/4/8004>
2. Гончаров М. В. Тенденції наукових поглядів у сфері нормативно-правового забезпечення інформаційної безпеки України. *Науковий вісник Ужгородського національного університету*. Серія: «Право». 2022. № 70. С. 24–28. URL: <http://visnyk-pravo.uzhnu.edu.ua/article/view/257287/254189>
3. Гончаров М. В. Досвід нормативно-правового забезпечення інформаційної безпеки в країнах Європейського Союзу. *Наше право*. № 2. 2023. С. 144–150. URL: http://nashe-pravo.unesco-socio.in.ua/wp-content/uploads/archive/NP-2023-2/NP_2023_2_144.pdf
4. Andrii M. Blahodarnyi, Olha O. Barabash, Andrii V. Honcharov, Mykola V. Honcharov, Volodymyr A. Shatilo. Local Self-government in European Countries: General Characteristics, Comparison and Ukrainian Realities. *LEX LOCALIS - journal of local self-government* Vol. 21, No. 3, pp. 683-706, July 2023. URL: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85165207079&origin=resultslist&sort=plf-f> (Scopus).

які засвідчують апробацію результатів дисертації:

5. Гончаров М. В. До питання використання інформаційних систем та технологій у сучасному суспільстві. *Кібербезпека в Україні: правові та організаційні питання : матеріали всеукр. наук.-практ. конф., м. Одеса, 30 листопада 2018 р.* Одеса : ОДУВС, 2018. С. 94–95.
6. Гончаров М. В. Сутність інформаційної безпеки в умовах розвитку

сучасного суспільства. *Кібербезпека в Україні: правові та організаційні питання: матеріали міжн. наук. практ. конф., м. Одеса, 22 листопада 2019 р.* Одеса : ОДУВС, 2019. С. 4–5.

7. Гончаров М. В. Деякі аспекти дослідження інформаційної безпеки в діяльності держави. *Правова наука і державотворення в Україні у світлі сучасних глобалізаційних викликів: історія, теорія, практика (до 25-ї річниці Конституції України): матеріали Всеукраїнської науково-практичної конференції (м. Маріуполь – м. Кривий Ріг, 11 червня 2021 року).* Маріуполь : ДонДУВС, 2021. С. 133–135.

8. Гончаров М. В. Деякі аспекти дослідження сутності інформаційної безпеки. *Інформація та документ у сучасному науковому дискурсі: матеріали VII Всеукраїнської дистанційної науково-практичної конференції. (Івано-Франківськ, 20 травня 2022 р.).* Івано-Франківськ: ІФНТУНГ, 2022. С. 13–16.

9. Гончаров М. В. Концептуальні засади сутності інформаційної безпеки України. *Міжнародне право XXI століття: сучасність та майбутнє: Збірник тез доповідей Міжнародної науково-практичної конференції «Міжнародне право XXI століття: сучасність та майбутнє». (м. Ірпінь, 25 травня 2022 р.).* Ірпінь: Державний податковий університет, 2022. С. 51–56.

10. Honcharov A.V., Honcharov M.V. Some aspects the conceptual study of regulatory and legal ensurement of information security. *The IX International Scientific and Practical Conference «Analysis of the problems of science and modern education», 06 – 08 March, 2023. Prague, Czech Republic.* P. 77–80.

які додатково відображають результати дисертації:

11. Гончаров А. В., Гончаров М. В. Життєвий шлях, юридичні погляди та педагогічна діяльність В. Г. Кукольника (1765–1821). *Правовий часопис Донбасу:* Зб. наук. праць № 1(66). Кривий Ріг.: Донецький юридичний інститут МВС України, 2019. С. 13–18. URL: <https://ljd.dnuvs.in.ua/wp-content/uploads/2022/01/2-goncharov-goncharov.pdf>