НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ПУБЛІЧНОГО ПРАВА
НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ПУБЛІЧНОГО ПРАВА

Кваліфікаційна наукова
праця на правах рукопису

ВДОВІН ІЛЛЯ ОЛЕКСАНДРОВИЧ

УДК 342.9 (477)

ДИСЕРТАЦІЯ

ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

12.00.07 – адміністративне право і процес;
фінансове право; інформаційне право

Подається на здобуття наукового ступеня кандидата юридичних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело _____ **І.О. Вдовін**

Науковий керівник **Червякова Оксана Вікторівна**, кандидат юридичних наук

Київ – 2024

АНОТАЦІЯ

Вдовін І.О. Організаційно-правові засади реалізації інформаційної безпеки України. − *Кваліфікаційна наукова праця на правах рукопису.*

Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». – Науково-дослідний інститут публічного права, Науково-дослідний інститут публічного права, Київ, 2024.

У дисертації наведено теоретичне узагальнення та нове вирішення наукового завдання, яке полягає у з'ясуванні сутності та розкритті особливостей організаційно-правових засад реалізації інформаційної безпеки України, а також опрацюванні напрямків вдосконалення організаційно-правового забезпечення відповідної сфери суспільних відносин.

Констатовано, що тільки після початку агресії російської федерації проти України, яка в тому числі здійснюється в інформаційному просторі, українське суспільство та публічна влада почали по-справжньому уважно і відповідально ставитися до питання забезпечення інформаційної безпеки. Від визнання деяких окремих загроз і викликів, що стоять перед Україною в інформаційній сфері, а також від визначення певних напрямків їх подолання, влада перейшла до: формулювання комплексу концептуальних засад, стратегічних пріоритетів, цілей і напрямків щодо забезпечення інформаційної безпеки України, як на глобальному, так і національному рівні; закріплення на законодавчому рівні основних засад організації та функціонування адміністративно-правового механізму забезпечення інформаційної безпеки із розподілом відповідних завдань і повноважень між суб'єктами публічної влади. Саме на цьому етапі розвитку інформаційної безпеки, вона реально розкрилася як необхідна умова не просто протидії злочинності, а збереження української державності, територіальної цілісності та національної ідентичності.

Виокремлено та детально охарактеризовано наступні ключові напрямки

забезпечення реалізації інформаційної безпеки України: 1) ідеологічний; 2) нормативно-правовий; 3) організаційно-управлінський; 4) культурно-освітній; 5) налагодження ефективної, системної та систематичної внутрішньодержавної взаємодії та міжнародної співпраці з питань інформації та інформаційної безпеки; 6) інноваційний. Надано змістовну характеристику кожному напрямку.

Доведено, що окрім Законів, значну частину нормативно-правового підґрунтя реалізації інформаційної безпеки України складають підзаконні нормативно-правові акти, які умовно можна розподілити на декілька груп: 1) концептуальні. До цієї категорії підзаконних нормативно-правових актів належать ті, в яких викладені концептуальні та стратегічні засади державної політики у сфері забезпечення інформаційної безпеки, програмні цілі та завдання з її реалізації; 2) статусні – це підзаконні нормативно-правові акти, в яких визначається правовий статус (цілі, завдання, функції, права та обов'язки тощо) суб'єктів публічної влади, які у тій чи іншій мірі займаються питаннями забезпечення реалізації інформаційної безпеки; 3) функціональні – підзаконні нормативно-правові акти, положеннями яких визначаються безпосередні заходи з реалізації інформаційної безпеки, врегульовуються і конкретизуються форми та процедури її здійснення.

Сучасний стан нормативно-правового регулювання забезпечення реалізації інформаційної безпеки України охарактеризовано як такий, що потребує подальшого вдосконалення. Відмічено, що наразі інформаційна безпека на офіційному рівні визнана неодмінною і вкрай важливою складовою забезпечення національної, державної та воєнної безпеки держави, а нормативно-правові засади механізму забезпечення реалізації безпосередньо самої інформаційної безпеки розраховані не лише на боротьбу із конкретними нагальними загрозами і небезпеками, а на всебічне зміцнення і розвиток інформаційної сфери України з урахуванням як національних, так і міжнародних інтересів нашої держави. Обґрунтована доцільність розробки та прийняття Закону України «Про інформаційну безпеку України», який мав би

стати стрижневим у системі нормативно-правових актів з питань інформаційної безпеки та сприяв би узгодженій та послідовній реалізації цієї безпеки.

Узагальнено, що правове регулювання забезпечення реалізації інформаційної безпеки є явищем комплексним і його не можна звести до засобів та (або) методів якоїсь окремої правової галузі, оскільки у механізмі цього забезпечення задіяна ціла низка суб'єктів різного рівня і статусу, а інструменти реалізації інформаційної безпеки мають і юридичний, і управлінський, і технічний, і культурний й інший характер, використання яких опосередковується правовідносинами, що мають як управлінську, так й іншу природу.

З'ясовано, що система суб'єктів забезпечення реалізації інформаційної безпеки являє собою складний механізм, тобто сукупність активних, взаємопов'язаних і взаємодіючих суб'єктів, що перебувають у певній ієрархії та виконують відведене їм функціональне призначення. Обсяги і характер компетенції зазначених суб'єктів у досліджуваній сфері різняться, залежно від того, чи є для них забезпечення реалізації інформаційної безпеки основним (одним із декількох основних) чи супутнім напрямом діяльності. До основних суб'єктів забезпечення реалізації інформаційної безпеки віднесено: 1) суб'єкти загальної компетенції, до яких належать Верховна Рада України, Президент України, Кабінет Міністрів України, місцеві державні адміністрації, органи місцевого самоврядування; 2) суб'єкти забезпечення реалізації інформаційної безпеки України міжгалузевої компетенції (суди та органи прокуратури); 3) суб'єкти галузевої компетенції; 4) суб'єкти спеціальної компетенції (Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України та Служба безпеки України).

Доведено, що форми реалізації інформаційної безпеки України являють собою зовнішній прояв практичної діяльності спеціально уповноважених суб'єктів, яка спрямована на створення правових та організаційних умов для

забезпечення конфіденційності, цілісності та доступності інформації, а також на захист інформаційних ресурсів від несанкціонованого доступу, втрати, зміни, руйнування або розголошення. Вказані методи запропоновано поділити на: 1) нормативно-правові; 2) організаційно-управлінські; та 3) спеціальні методи.

Наголошено, що розробка прогнозів і програм у сфері забезпечення інформаційної безпеки є фундаментальною діяльністю в контексті захисту інформації в сучасному світі. Її сутність полягає в тому, щоб систематично підходити до питань інформаційної безпеки, а саме: визначати потенційні загрози, аналізувати ризики та розробляти стратегії та програми, спрямовані на запобігання цим загрозам та забезпечення інформаційної безпеки. Прогнозування в цьому контексті дає можливість передбачити можливі ризики та загрози для інформаційної інфраструктури, а також визначити майбутні тенденції в інформаційних технологіях та загрозах, які можуть виникнути в результаті цих тенденцій.

Доведено, що під методами реалізації інформаційної безпеки України найбільш доцільно розуміти сукупність визначених у нормах чинного законодавства механізмів, інструментів та засобів, які використовують в своїй діяльності спеціально-уповноважені суб’єкти задля досягнення кінцевої мети у відповідній сфері. Відповідні методи запропоновано поділити на дві групи: 1) загальні (переконання та примусу); та 2) спеціальні, зокрема: шифрування даних, аудит інформаційної безпеки, кіберзахист, управління доступом, інформаційна гігієна, моніторинг і виявлення загроз, метод кризисного управління.

Акцентовано увагу на тому, що забезпечення інформаційної безпеки у всіх сферах суспільного життя, особливо в умовах сьогодення, є важливим та надскладним викликом для будь-якої сучасної держави, і Україна у даному контексті не є виключенням. Втім, технологічний прогрес по-різному торкнувся різних держав, а відтак і механізм забезпечення реалізації інформаційної безпеки також відрізняються один

від одного. З огляду на це, для українського законодавця важливим є вивчення позитивного зарубіжного досвіду, запровадження якого дозволить якісно покращити правові та організаційні засади забезпечення реалізації інформаційної безпеки в реаліях, яких опинилась наша країна сьогодні.

Доведено, що забезпечення інформаційної безпеки в США має глибокі коріння. У XX столітті, ця держава відіграли ключову роль у розвитку інформаційних технологій, що дозволило їй бути «першопрохідником» у боротьбі з інформаційними загрозами. А відтак, саме США була однією із перших країн, яка розробила державну політику і систему державного регулювання в інформаційній сфері. На сьогоднішній день, ця система забезпечує ефективне використання інформаційних технологій для прискорення розвитку американської економіки, а також забезпечує національну безпеку через контроль і захист важливих інформаційних інфраструктур.

Узагальнено, що на сьогоднішній день всі провідні держави Європи та Світу прагнуть створити належні правові та організаційні умови для забезпечення інформаційної безпеки. А відтак, виділено найбільш позитивний зарубіжний досвід, який варто використати вітчизняному законодавцю в рамках удосконалення правового регулювання забезпечення реалізації інформаційної безпеки в українських реаліях.

Доведено, що переважна більшість теоретичних розробок у сфері забезпечення реалізації інформаційної безпеки: по-перше, втратили свою актуальність, оскільки були написані ще до повномасштабного вторгнення, а відтак вони не враховують всю специфіку сучасної інформаційної війни, яка наразі відбувається у медійному просторі; по-друге, переважна більшість робіт спрямована на покращення саме організаційного забезпечення інформаційної безпеки, в той час я покращенню норм чинного законодавства увага приділялась досить поверхнево.

Запропоновано авторське бачення щодо напрямів покращення правових та організаційно-управлінських засад забезпечення реалізації

інформаційної безпеки України.

Ключові слова: інформація, інформаційна безпека, державна політика, правове регулювання, адміністративне право, інформаційне право, суб'єкти, форми, методи, міжнародний досвід, вдосконалення, правові засади, організаційні засади.

SUMMARY

Vdovin I. O. Organizational and legal principles of implementation of information security of Ukraine. – *Qualification scientific work on the rights of the manuscript*.

Thesis for obtaining a scientific degree of Candidate of Juridical Science, specialty 12.00.07 «Administrative Law and Procedure; Financial Law; Information Law». – Scientific Institute of Public Law, Scientific Institute of Public Law, Kyiv, 2024.

The thesis provides a theoretical generalization and a new solution to the scientific task, which consists in clarifying the essence and revealing the peculiarities of the organizational and legal principles of implementation of information security in Ukraine, as well as working out directions for improving the organizational and legal provision of the relevant sphere of public relations.

It is established that only after the beginning of the aggression of the Russian Federation against Ukraine, which is also carried out in the information space, Ukrainian society and public authorities began to take a really careful and responsible approach to the issue of ensuring information security. From the recognition of some individual threats and challenges facing Ukraine in the information sphere, as well as from the determination of certain directions for overcoming them, the authorities moved to: formulating a set of conceptual principles, strategic priorities, goals and directions for ensuring Ukraine's information security, as on the global level, and at the national level; consolidation at the legislative level of the basic principles of the organization and functioning of the administrative and legal mechanism for ensuring information security with the distribution of relevant tasks and powers between public authorities. It was at this stage of the development of information security that it really revealed itself as a necessary condition not just for combating crime, but for the preservation of Ukrainian statehood, territorial integrity and national identity.

The following key areas of ensuring the implementation of information

security of Ukraine are singled out and characterized in detail: 1) ideological; 2) normative and legal; 3) organizational and managerial; 4) cultural and educational; 5) establishment of effective, systemic and systematic intrastate interaction and international cooperation on information and information security issues; 6) innovative. A meaningful description of each area is provided.

It is proven that, in addition to the Laws, a significant part of the legal basis for the implementation of information security of Ukraine consists of subordinate legal acts, which can be conventionally divided into several groups: 1) conceptual. This category of subordinate regulatory legal acts includes those that outline the conceptual and strategic principles of state policy in the field of information security, program goals and tasks for its implementation; 2) status - these are subordinate legal acts, which determine the legal status (goals, tasks, functions, rights and obligations, etc.) of public authorities, which to one degree or another deal with issues of ensuring the implementation of information security; 3) functional - subordinate legal acts, the provisions of which determine direct measures for the implementation of information security, regulate and specify the forms and procedures for its implementation.

The current state of regulatory and legal regulation of ensuring the implementation of information security in Ukraine is characterized as requiring further improvement. It is noted that currently information security at the official level is recognized as an indispensable and extremely important component of ensuring the national, state and military security of the state, and the regulatory and legal foundations of the mechanism for ensuring the implementation of information security itself are designed not only to combat specific urgent threats and dangers, but also comprehensive strengthening and development of the information sphere of Ukraine, taking into account both national and international interests of our state. The expediency of the development and adoption of the Law of Ukraine "On Information Security of Ukraine", which should become a cornerstone in the system of normative legal acts on information security and would contribute to the coordinated and consistent implementation of this security,

is substantiated.

It is summarized that legal regulation of information security is a complex phenomenon and cannot be reduced to the means and/or methods of any particular legal branch, since the mechanism of this provision involves a number of entities of different levels and status, and the tools for implementing information security are of legal, managerial, technical, cultural and other nature, and their use is mediated by legal relations of both managerial and other nature.

It is found that the system of entities ensuring the implementation of information security is a complex mechanism, i.e., a set of active, interconnected and interacting entities that are in a certain hierarchy and perform their assigned functional purpose. The scope and nature of the competence of these entities in the area under study vary, depending on whether ensuring the implementation of information security is their main (one of several main) or related activities. The main subjects of ensuring the implementation of information security include: 1) subjects of general competence, which include the Verkhovna Rada of Ukraine, the President of Ukraine, the Cabinet of Ministers of Ukraine, local state administrations, local self-government bodies; 2) subjects of ensuring the implementation of information security of Ukraine of inter-sectoral competence (courts and prosecutor's offices); 3) subjects of sectoral competence; 4) subjects of special competence (the State Service of Special Communications and Information Protection of Ukraine, the National Police of Ukraine and the Security Service of Ukraine).

It is proven that the forms of implementation of information security of Ukraine are an external manifestation of the practical activities of specially authorized entities aimed at creating legal and organizational conditions for ensuring confidentiality, integrity and availability of information, as well as at protecting information resources from unauthorized access, loss, alteration, destruction or disclosure. It is proposed to divide these methods into: 1) regulatory and legal; 2) organizational and managerial; and 3) special methods.

It is emphasized that the development of forecasts and programs in the field

of information security is a fundamental activity in the context of information protection in the modern world. Its essence is to systematically approach information security issues, namely, to identify potential threats, analyze risks and develop strategies and programs aimed at preventing these threats and ensuring information security. Forecasting in this context makes it possible to anticipate possible risks and threats to the information infrastructure, as well as to identify future trends in information technology and threats that may arise as a result of these trends.

It is proven that the methods of implementing information security of Ukraine are best understood as a set of mechanisms, tools and means defined in the current legislation and used by specially authorized entities in their activities to achieve the ultimate goal in the relevant area. It is proposed to divide the relevant methods into two groups: 1) general (persuasion and coercion); and 2) special, in particular: data encryption; information security audit; cyber defense; access control; information hygiene; monitoring and detection of threats; crisis management method.

It is emphasized that ensuring information security in all spheres of public life, especially in today's conditions, is an important and extremely difficult challenge for any modern state, and Ukraine is no exception in this context. However, technological progress has affected different countries in different ways, and therefore the mechanism for ensuring the implementation of information security also differs from each other. In view of this, it is important for the Ukrainian legislator to study positive foreign experience, the implementation of which will qualitatively improve the legal and organizational framework for ensuring the implementation of information security in the realities in which our country finds itself today.

It is proven that information security in the United States has deep roots. In the XX century, this country played a key role in the development of information technology, which allowed it to be a "pioneer" in the fight against information threats. Consequently, the United States was one of the first countries to develop a

state policy and a system of state regulation in the information sphere. Today, this system ensures the effective use of information technology to accelerate the development of the American economy, and also ensures national security through the control and protection of important information infrastructures.

It is summarized that today all the leading countries of Europe and the world strive to create appropriate legal and organizational conditions for ensuring information security. Therefore, the the most positive foreign experience, which should be used by the national legislator in the framework of improving the legal regulation of information security in the Ukrainian context, is singled out.

It is proven that the vast majority of theoretical developments in the field of ensuring the implementation of information security: firstly, have lost their relevance, since they were written before the full-scale invasion, and therefore they do not take into account all the specifics of the modern information warfare currently taking place in the media space; secondly, the vast majority of works are aimed at improving the organizational support of information security, while attention was paid to improving the norms of current legislation rather superficially.

The author's vision of the ways to improve the legal, organizational and managerial framework for ensuring the implementation of information security in Ukraine is proposed.

Keywords: information, information security, state policy, legal regulation, administrative law, information law, subjects, forms, methods, international experience, improvement, legal framework, organizational principles.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

1. Вдовін І.О. До характеристики напрямків розвитку державної політики у сфері забезпечення реалізації інформаційної безпеки України. *Юридичний науковий електронний журнал.* 2022. № 10. С. 847–849. http://www.lsej.org.ua/10_2022/213.pdf

2. Вдовін І. Сучасний розвиток інформаційної безпеки України. *KELM*. 2022. № 7(51). С. 259–263.

3. Вдовін І.О. До характеристики сучасного стану правового регулювання забезпечення реалізації інформаційної безпеки України. *Науковий вісник публічного та приватного права.* 2023. Вип. 4. С. 86–90.

4. Вдовін І.О. До проблеми розмежування галузей права у правовому регулюванні забезпечення реалізації інформаційної безпеки України. *Науковий вісник публічного та приватного права.* 2023. Вип. 5. С. 91–95.

5. Vdovin I.O. The place of the Security Service of Ukraine in the system of entities ensuring information security. *Entrepreneurship, Economy and Law*. 2023. № 9. pp. 67–73.

які засвідчують апробацію матеріалів дисертації:

6. Вдовін І.О. До характеристики ідеологічного напрямку державної політики у сфері забезпечення реалізації інформаційної безпеки України. *Виклики сучасності та наукові підходи до їх вирішення*: матеріали міжнародної науково-практичної конференції (Київ, 12–13 серп. 2020 р.). Київ: Науково-дослідний інститут публічного права, 2020. С. 88–90.

7. Вдовін І.О. До характеристики правового статусу суб’єктів спеціальної компетенції забезпечення реалізації інформаційної безпеки України. *Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення:* матеріали міжнародної науково-практичної конференції (Київ, 22–23 верес. 2021 р.). Київ: Науково-дослідний інститут публічного права, 2021. С. 71–74.

8. Вдовін І.О. Проблеми нормативно-правового напрямку формування та розвитку державної політики у сфері забезпечення реалізації інформаційної безпеки України. *Актуальні проблеми імплементації наукових досягнень у практичну діяльність:* матеріали міжнародної науково-практичної конференції, (Київ, 19–20 січ. 2022 р.). Київ: Науково-дослідний інститут публічного права, 2022. С. 57–59.

ЗМІСТ

ВСТУП

Обґрунтування вибору теми дослідження. В цифрову епоху, в якій ми зараз живемо, одним із найцінніших ресурсів людства є інформація. Остання, в свою чергу, може використовуватись як для розвитку суспільства, так і з метою вчинення протиправних дій, які порушують права, свободи та інтереси інших людей. Саме тому ключовим завданням будь-якої сучасної та розвиненої держави є створення ефективної системи забезпечення інформаційної безпеки, яка в умовах сьогодення є надважливою та невід'ємною складовою національної безпеки. Втім постійний розвиток та вдосконалення інформаційної галузі значно ускладнює процес створення механізмів реалізації інформаційної безпеки.

Варто зауважити, що в останні роки в Україні було розроблено та прийнято низку стратегічних та концептуальних нормативно-правових актів, які були покликані якісно покращити правові та організаційні аспекти забезпечення реалізації інформаційної безпеки в нашій країні. Разом із тим, розробка і введення в дію вказаних нормативно-правових актів жодним чином не применшує актуальність проблематики забезпечення інформаційної безпеки, а також не вирішує всіх проблем її реалізації в Україні, а особливо сьогодні, в умовах повномасштабної війни на території нашої держави. Зазначене в тому числі пояснюється тим, що значна частина протистояння України та рф відбувається саме в інформаційному просторі. Саме тому, і українському законодавцю, і вітчизняним науковцям, слід вести активну роботу у напрямку покращення організаційно-правових засад реалізації інформаційної безпеки України.

Зв'язок теми дисертації із сучасними дослідженнями. Справедливим буде відзначити, що в останні декілька десятиліть проблема інформаційної безпеки ставала предметом дослідження багатьох науковців. Зокрема їй приділяли увагу: С.Є. Антонова, М.В. Баран, І.О. Валюшко, М.В. Грайворонський, Д.В. Дубов, А.О. Іванов, Р.А. Калюжний,

М.О. Кириченко, Ю.О. Корнєєв, О.М. Косогов, О.В. Левченко, Л.С. Любохинець, А.І. Марущак, О.А. Моргунов , О.А. Панченко, О.М. Ситніченко, М.В. Сунгуровський, О.В. Червякова , Я.І. Чмир, П.О. Яковлєв та багато інших. Втім, незважаючи на значну кількість теоретичних здобутків, слід відзначити декілька важливих моментів: по-перше, більшість теоретичних розробок вже втратили свою актуальність, що обумовлено повномасштабною військовою агресією рф; по-друге, в роботах вказаних науковців питання організаційно-правових засад реалізації інформаційної безпеки розглядалось досить поверхнево, в межах більш широких проблематик.

Таким чином, наявність низки прогалин та недоліків у чинному законодавстві, норми якого спрямовані на закріплення реалізації інформаційної безпеки України, а також відсутність сучасних комплексних монографічних досліджень, присвячених вказаній проблематиці, обумовлюють актуальність та своєчасність представленого дисертаційного дослідження.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертаційне дослідження узгоджується з основними положеннями: «Стратегії інформаційної безпеки на період до 2025 року», затвердженої розпорядженням Кабінету Міністрів України від 30 березня 2023 р. № 272-р.; «Стратегії національної безпеки України», схваленої Указом Президента України від 14 вересня 2020 р. № 392/2020; «Стратегії кібербезпеки України», що була введена в дію Указом Президента України від 26 серпня 2021 р. № 447/2021; «Стратегії воєнної безпеки України», затвердженої Указом Президента України від 25 березня 2021 р. № 121/2021; «Стратегії кібербезпеки України», схваленої Указом Президента України від 16 березня 2016 р. № 96/2016; «Стратегії забезпечення державної безпеки», затвердженої Указом Президента України від 16 лютого 2022 р. № 56/2022; «Стратегії комунікації з питань євроатлантичної інтеграції України на період до 2025 року» затвердженої Указом Президента України від 11 вересня

2021 р. № 348/2021. Дисертацію виконано відповідно до плану науково-дослідної роботи Науково-дослідного інституту публічного права «Правове забезпечення прав, свобод та законних інтересів суб'єктів публічно-правових відносин» (номер державної реєстрації 0120U105390).

Мета і завдання дослідження. *Мета* дисертаційного дослідження полягає у тому, щоб на основі аналізу наукових поглядів вчених, норм чинного законодавства, а також практики його реалізації, з'ясувати сутність та особливості організаційно-правових засад реалізації інформаційної безпеки України, а також, спираючись на позитивний вітчизняний та зарубіжний досвід, опрацювати напрями вдосконалення організаційно-правового забезпечення відповідної діяльності.

Для досягнення зазначеної мети у процесі дослідження необхідно вирішити такі *завдання:*

– охарактеризувати становлення та розвиток інформаційної безпеки України;

– розкрити напрямки розвитку державної політики у сфері забезпечення реалізації інформаційної безпеки України;

– оцінити сучасний стан правового регулювання забезпечення реалізації інформаційної безпеки України;

– здійснити розмежування галузей права у правовому регулюванні забезпечення реалізації інформаційної безпеки України;

– розкрити систему суб'єктів забезпечення реалізації інформаційної безпеки України та встановити місце серед них Служби безпеки України;

– визначити форми та методи реалізації інформаційної безпеки України;

– узагальнити міжнародний досвід правового регулювання забезпечення реалізації інформаційної безпеки та опрацювати можливості його використання в Україні;

– запропонувати напрямки вдосконалення організаційно-правового забезпечення реалізації інформаційної безпеки України.

Об'єктом дослідження є суспільні відносини, які виникають в процесі реалізації інформаційної безпеки України.

Предметом дослідження є організаційно-правові засади реалізації інформаційної безпеки України.

Методи дослідження. Методологічною основою роботи є сукупність загальнонаукових і спеціально-наукових методів та прийомів наукового пізнання, застосування яких зумовлюється специфікою предмета дослідження. Так, використання *історико-правового* методу дозволило надати характеристику становленню та розвитку інформаційної безпеки України (підрозділ 1.1). Розкрити напрямки розвитку державної політики у сфері забезпечення реалізації інформаційної безпеки України (підрозділ 1.2); оцінити сучасний стан правового регулювання забезпечення реалізації інформаційної безпеки України (підрозділ 1.3), а також здійснити розмежування галузей права у правовому регулюванні забезпечення реалізації інформаційної безпеки України (підрозділ 2.1) вдалось за допомогою *аналітичного* методу та методу *документального аналізу*. *Структурно-логічний* та *системно-функціональний* методи використовувалися для того, щоб надати характеристику системі суб'єктів забезпечення реалізації інформаційної безпеки України та встановити місце серед них Служби безпеки України (підрозділ 2.2), а також встановити форми та методи реалізації інформаційної безпеки України (підрозділ 2.3). Для узагальнення міжнародного досвіду правового регулювання забезпечення реалізації інформаційної безпеки та опрацювання можливостей його використання в Україні (підрозділ 3.1) було використано *порівняльно-правовий* метод. З'ясувати напрямки вдосконалення організаційно-правового забезпечення реалізації інформаційної безпеки України (підрозділ 2.1) вдалось за допомогою використання методів *моделювання* та *прогнозування*.

Науково-методологічну основу дисертаційної роботи складає сукупність загальних та спеціальних методів наукового пізнання,

застосування яких обумовлюється системним підходом, що надало можливість досліджувати проблеми в єдності їх соціального змісту і юридичної форми.

Нормативно-правову основу складають нормативно-правові акти різної юридичної сили, норми яких спрямовані на правове регулювання забезпечення реалізації інформаційної безпеки України.

Науково-теоретичне підґрунтя дисертації складають наукові праці фахівців в галузі адміністративного права, загальної теорії держави і права, конституційного права, а також інших галузевих наук, зокрема: соціології, політології, філософії тощо.

Наукова новизна отриманих результатів полягає у тому, що дисертаційне дослідження є однією із перших спроб комплексно, на монографічному рівні, з'ясувати сутність та особливості організаційно-правових засад реалізації інформаційної безпеки України, на основі чого розробити пропозиції та рекомендації щодо вдосконалення організаційно-правових засад здійснення відповідної діяльності. До основних наукових положень, що характеризують новизну отриманих результатів й виносяться на захист, належать такі:

уперше:

– на доктринальному рівні акцентовано увагу на тому, що тільки після початку агресії російської федерації проти України, яка в тому числі здійснюється в інформаційному просторі, українське суспільство та публічна влада почали по-справжньому уважно і відповідально ставитися до питання забезпечення інформаційної безпеки, зокрема, від визнання деяких окремих загроз і викликів, що стоять перед Україною в інформаційній сфері, а також від визначення певних напрямків їх подолання, влада перейшла до: формулювання комплексу концептуальних засад, стратегічних пріоритетів, цілей і напрямків щодо забезпечення інформаційної безпеки України, як на глобальному, так і національному рівні; закріплення на законодавчому рівні основних засад організації та функціонування адміністративно-правового

механізму забезпечення інформаційної безпеки із розподілом відповідних завдань і повноважень між суб'єктами публічної влади;

– комплексно виокремлено коло форм реалізації інформаційної безпеки України, які запропоновано поділити на три великі групи: 1) нормативно-правові (нормотворча, установча та правозастосовна форми); 2) організаційно-управлінські (проведення зборів (нарад); науково-практичних конференцій; розробка прогнозів, програм у сфері забезпечення інформаційної безпеки; матеріально-технічне забезпечення); та 3) спеціальні (інформаційний патронат; інформаційна кооперація; інформаційне протиборство);

– акцентовано увагу на тому, що в Україні на прикладі провідних держав Європи та світу варто розширити співпрацю не тільки між різними органами державної влади у сфері інформаційної безпеки, а й іншими недержавними суб'єктами, зокрема фахівцями IT-сфери, а також різними підприємствами, організаціями, які здійснюють свою діяльність у галузі використання інформаційних технологій;

удосконалено:

– теоретичний підхід щодо розуміння видів підзаконних нормативно-правових актів, які складають підґрунтя реалізації інформаційної безпеки України, які зокрема поділено на: 1) концептуальні, до яких належать ті акти, в яких викладені концептуальні та стратегічні засади державної політики у сфері забезпечення інформаційної безпеки, програмні цілі та завдання з її реалізації; 2) статусні – в яких закріплюється адміністративно-правовий статус (цілі, завдання, функції, права та обов'язки тощо) суб'єктів публічної влади, які у тій чи іншій мірі виконують коло завдань, спрямованих на забезпечення реалізації інформаційної безпеки; 3) функціональні – підзаконні нормативно-правові акти, положеннями яких закріплюються безпосередні заходи з реалізації інформаційної безпеки, врегульовуються і конкретизуються форми та процедури її здійснення;

– класифікацію суб'єктів забезпечення реалізації інформаційної безпеки, які поділено на дві групи: 1) суб'єкти загальної компетенції, до яких належать Верховна Рада України, Президент України, Кабінет Міністрів України, місцеві державні адміністрації, органи місцевого самоврядування; 2) суб'єкти забезпечення реалізації інформаційної безпеки України міжгалузевої компетенції (суди та органи прокуратури); 3) суб'єкти галузевої компетенції; 4) суб'єкти спеціальної компетенції (Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України та Служба безпеки України);

– тезу про те, що правове регулювання забезпечення реалізації інформаційної безпеки є явищем комплексним і його не можна звести до засобів та (або) методів якоїсь окремої правової галузі, оскільки у механізмі цього забезпечення задіяна ціла низка суб'єктів різного рівня і статусу, а інструменти реалізації інформаційної безпеки мають юридичний, управлінський, технічний, культурний та інший характер, використання яких опосередковується правовідносинами, що мають як управлінську, так й іншу природу;

дістало подальшого розвитку:

– обґрунтування наукової думки про те, що нормативно-правовий напрямок розвитку державної політики у сфері забезпечення реалізації інформаційної безпеки України включає: а) забезпечення своєчасного оновлення нормативно-правового підґрунтя механізму забезпечення інформаційної безпеки в Україні, приводячи його у відповідність до перспектив подальшого розвитку та актуальних викликів і загроз; б) гармонійне поєднання дотримання прав і свобод людини та громадянина в інформаційній сфері з національними інтересами держави; в) забезпечення нормативно-правових засад для ефективного просвітництва населення, підвищення їх медійної грамотності, правової культури та свідомості; г) створення сприятливих та нормативно-правових умов для розвитку економічної активності населення у інформаційній сфері;

г) вдосконалення матеріально-правових та процедурних засад контролю в інформаційній сфері, своєчасне виявлення та оцінювання ризиків; д) створення сприятливого нормативно-правового середовища для взаємодії публічної влади всіх рівнів із громадськістю з питань інформації та інформаційної діяльності;

– обґрунтування необхідності розширення системи законодавчих актів у сфері забезпечення реалізації інформаційної безпеки шляхом прийняття таких Законів України: «Про захист інформації в сфері охорони здоров'я»; «Про електронний підпис»; «Про мережу та інформаційну безпеку»; «Про кіберзахист критичних інфраструктур»; «Про кіберзахист урядових систем». Прийняття цих документів, як вбачається: а) розширить сферу забезпечення інформаційної безпеки; б) створить сприятливі умови для захисту інформації в окремих важливих галузях, наприклад, діяльності уряду, а також критичних інфраструктур.

Практичне значення отриманих результатів полягає в тому, що сформульовані в дисертації пропозиції та висновки можуть бути використані у:

– *науково-дослідній сфері* – для подальшого наукового опрацювання теоретико-прикладних питань, пов'язаних із організаційно-правовими засадами реалізації інформаційної безпеки України;

– *правотворчості* – під час розробки нових та вдосконалення діючих нормативно-правових актів, норми яких спрямовані на регулювання суспільних відносин, які виникають в процесі реалізації інформаційної безпеки в Україні;

– *правозастосовній діяльності* – для покращення практичної діяльності суб'єктів, що уповноважені реалізовувати заходи у сфері забезпечення реалізації інформаційної безпеки України;

– *освітньому процесі* – під час підготовки лекційних, навчально- та науково-методичних матеріалів, підручників та навчальних посібників з

дисципліни «Адміністративне право», а також інших дисциплін адміністративно-правового характеру.

Апробація матеріалів дисертації. Підсумки розробки проблеми у цілому, окремі її аспекти, одержані узагальнення і висновки були оприлюднені на міжнародних конференціях: «Виклики сучасності та наукові підходи до їх вирішення» (м. Київ, 12–13 серпня 2020 року); «Актуальні проблеми імплементації наукових досягнень у практичну діяльність» (м. Київ, 19–20 січня 2022 року); «Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення» (м. Київ, 22–23 вересня 2021 р.)

Структура та обсяг дисертації. Дисертація складається зі вступу, трьох розділів, які містять вісім підрозділів, висновків, списку використаних джерел і додатків. Загальний обсяг дисертації становить 223 сторінки. Список використаних джерел містить 165 найменувань на 18 сторінках.

РОЗДІЛ 1.
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАБЕЗПЕЧЕННЯ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

1.1. Становлення та розвиток інформаційної безпеки України.

Питання забезпечення національної безпеки є одним із основних для кожної держави, яка прагне залишатися суверенною, зберегти свою територіальну цілісність, захистити свій конституційний лад і національні інтереси від різного роду загроз. Це у повній мірі стосується й України, яка сьогодні як раз перебуває у стані відбиття такого роду загроз, обумовлених військовою агресією по відношенню до нашої держави з боку російської федерації. Забезпечення національної безпеки – це складна, багаторівнева і багатоаспектна діяльність, що передбачає запровадження комплексу заходів у всіх основоположних сферах суспільного життя. З цього приводу слід відмітити позицію О. В. Сосніна, який зазначає, що забезпечення всіх рівнів національної безпеки, у тому числі й безпеки суспільства, полягає в реалізації збалансованих інтересів особистості, суспільства і держави у внутрішньополітичній, економічній, соціальній, міжнародній, інформаційній, військовій, екологічній та інших сферах [147]. Кожна із зазначених сфер національної безпеки і відповідні їй групи національних інтересів можуть і мають бути предметом окремого дослідження, у межах же представленої праці ми зупинимося на інформаційній безпеці як складовій національної безпеки України.

Проблематика забезпечення інформаційної безпеки України не втрачає своєї актуальності вже багато років, втім сьогодні, в умовах інформаційної війни, яка ведеться російською федерацією проти нашої держави на рівні з повномасштабним військовим вторгненням, вона постала особливо гостро. Однак перед тим, як проводити науково-теоретичне опрацювання нагальних проблемних питань інформаційної безпеки та засобів її забезпечення,

доцільно поглянути на історико-правові умови становлення і розвитку зазначеної безпеки.

16 липня 1990 року Верховна Рада Української РСР (ВРУ СРС) прийняла Декларацію про державний суверенітет України, в якій проголошувався державний суверенітет України як верховенство, самостійність, повноту і неподільність влади Республіки в межах її території та незалежність і рівноправність у зовнішніх зносинах [28]. А вже 24 серпня 1991 року ВРУ СРС своєю Постановою затвердила Акт проголошення незалежності України [4], в якому було проголошено створення самостійної української держави – УКРАЇНИ, територія якої є неподільною і недоторканною. Зрозуміло, що у жодному із цих нормативно-правових актів не йшлося про інформаційну безпеку, втім очевидно, що суверенна, незалежна держава має запроваджувати власну інформаційну політику і захищати свій інформаційний простір. Слід відмітити, що у Декларації про Державний суверенітет України зазначалося, що Українська РСР як суб'єкт міжнародного права здійснює безпосередні зносини з іншими державами, укладає з ними договори, обмінюється дипломатичними, консульськими, торговельними представництвами, бере участь у діяльності міжнародних організацій в обсязі, необхідному для ефективного забезпечення національних інтересів Республіки у політичній, економічній, екологічній, інформаційній, науковій, технічній, культурній і спортивній сферах [28]. Тобто інформаційна сфера була визначена як окрема і пріоритетна галузь державних інтересів України.

З метою відповідного нормативно-правового управлінського забезпечення інформаційної сфери України, у жовтні 1992 року Верховна Рада України (ВРУ) прийняла закон «Про інформацію» № 2657-XII, який діє й сьогодні та має майже три десятки редакцій (одна із них – нова редакція нормативно-правового акту в цілому). У преамбулі першої редакції цього Закону зазначалося, що він закріплює право громадян України на інформацію, закладає правові основи інформаційної діяльності. Ґрунтуючись

на Декларації про державний суверенітет України та Акті проголошення її незалежності, Закон стверджує інформаційний суверенітет України і визначає правові форми міжнародного співробітництва в галузі інформації [101]. Як видно навіть із вступної часину (преамбули) Закону, інформація та інформаційна діяльність є основоположною сферою суспільного життя, яка має особливе значення як для окремої особи, так і суспільства та держави в цілому. В якості мети та завдань зазначеного закону «Про інформацію» було визначене наступне: «Закон встановлює загальні правові основи одержання, використання, поширення та зберігання інформації, закріплює право особи на інформацію в усіх сферах суспільного і державного життя України, а також систему інформації, її джерела, визначає статус учасників інформаційних відносин, регулює доступ до інформації та забезпечує її охорону, захищає особу та суспільство від неправдивої інформації [101]. Слід відмітити, що у момент появи Закону України «Про інформацію» у його тексті не було такого поняття як «інформаційна безпека», втім, як у вище згаданій цілях і завданнях цього нормативно-правового акту, так і ряді його інших положень йдеться про охорону і захист інформації. Зокрема у цьому законі зазначалося, що державна інформаційна політика – це сукупність основних напрямів і способів діяльності держави по одержанню, використанню, поширенню та зберіганню інформації. А до головних напрямів і способів державної інформаційної політики належать: зміцнення матеріально-технічних, фінансових, організаційних, правових і наукових основ інформаційної діяльності; забезпечення ефективного використання інформації; сприяння постійному оновленню, збагаченню та зберіганню національних інформаційних ресурсів; створення загальної системи охорони інформації [101]. Важливо підкреслити, що визначивши інформацію та інформаційну діяльність як одну із пріоритетних сфер державного управління, нормотворець не обмежився лише вказівкою на рівні Закону на те, що інформація захищається державою, але й перебачив конкретні нормативно-правові гарантії та засади її охорони і захисту. Зокрема у 5-му

розділі першої редакції закону «Про інформацію» було закріплено, що право на інформацію охороняється законом. Держава гарантує всім учасникам інформаційних відносин рівні права і можливості доступу до інформації. Ніхто не може обмежувати права особи у виборі форм і джерел одержання інформації, за винятком випадків, передбачених законом. Суб'єкт права на інформацію може вимагати усунення будь-яких порушень його права. Забороняється вилучення друкованих видань, експонатів, інформаційних банків, документів із архівних, бібліотечних, музейних фондів та знищення їх з ідеологічних чи політичних міркувань. Однак володіння інформацією супроводжується не лише правом (правами), але й накладає певні обов'язки. Зокрема у законі «Про інформацію» в редакції від 1992 року було передбачено, що інформація не може бути використана для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання расової, національної, релігійної ворожнечі, посягання на права і свободи людини. Не підлягають розголошенню відомості, що становлять державну або іншу передбачену законодавством таємницю. Не підлягають розголошенню відомості, що стосуються лікарської таємниці, грошових вкладів, прибутків від підприємницької діяльності, усиновлення (удочеріння), листування, телефонних розмов і телеграфних повідомлень, крім випадків, передбачених законом [101]. Задля захисту права суб'єктів на інформацію, а також недопущення зловживання цим правом і належного виконання обов'язку, що йому кореспондує, у законі було встановлено юридичну відповідальність за порушення інформаційного законодавства. При цьому в Законі містилося не лише загальне положення про те, що за порушення законодавства про інформацію тягне юридичну відповідальність, але й були передбачені види такої відповідальності, а також і конкретні випадки поведінки, що розцінюються як протизаконні. Зокрема цьому нормативно-правовому акті закріплювалося, що за порушення законодавства України про інформацію тягне за собою дисциплінарну, цивільно-правову, адміністративну або

кримінальну відповідальність згідно з законодавством України. Відповідальність за порушення законодавства про інформацію несуть особи, винні у вчиненні таких порушень, як: необґрунтована відмова від надання відповідної інформації; надання інформації, що не відповідає дійсності; несвоєчасне надання інформації; навмисне приховування інформації; примушення до поширення або перешкоджання поширенню чи безпідставна відмова від поширення певної інформації; поширення відомостей, що не відповідають дійсності, ганьблять честь і гідність особи; використання і поширення інформації стосовно особистого життя громадянина без його згоди особою, яка є власником відповідної інформації внаслідок виконання своїх службових обов'язків; розголошення державної або іншої таємниці, що охороняється законом, особою, яка повинна охороняти цю таємницю; порушення порядку зберігання інформації; навмисне знищення інформації; необґрунтоване віднесення окремих видів інформації до категорії відомостей з обмеженим доступом [101]. Окрім цього у Законі України «Про інформацію» в редакції від 1992 року були також викладені загальні засади оскарження протиправних дій у інформаційній сфері та відшкодування завданої ними шкоди.

Отже, аналіз положень закону «Про інформацію», що був прийнятий в нашій державі у жовтня 1992 року, переконливо свідчить про досить чітке усвідомлення владою того, що інформаційна сфера є вкрай важливою і необхідною умовою розвитку як окремої особи, так і суспільства і держави в цілому, а також того, що інформація та інформаційна діяльність можуть застосовуватися як із благими намірами, так і у злочинних цілях. А тому вкрай важливо не лише затвердити право осіб на інформацію (її вироблення, збирання, зберігання, використання, розповсюдження), але й закріпити гарантії та інструменти забезпечення безпеки інформаційної сфери. Однак, у той же час не можна говорити про те, що приймаючи закон «Про інформацію» на початку 90-х років XX-го століття, українська влада приділяла суттєву увагу інформаційній безпеці українського суспільства і

держави. Звісно можна відмітити статті 53-54 цього нормативно-правового акту, в яких йшлося про інформаційний суверенітет нашої держави та його гарантії, зокрема у вказаних статтях було закріплено, що основою інформаційного суверенітету України є національні інформаційні ресурси. Україна самостійно формує інформаційні ресурси на своїй території і вільно розпоряджається ними, за винятком випадків, передбачених законами і міжнародними договорами. Інформаційний суверенітет України забезпечується: виключним правом власності України на інформаційні ресурси, що формуються за рахунок коштів державного бюджету; створенням національних систем інформації; встановленням режиму доступу інших держав до інформаційних ресурсів України; використанням інформаційних ресурсів на основі рівноправного співробітництва з іншими державами [101]. Однак, навіть у статтях присвячених інформаційному суверенітету держави, немає жодної вказівки на те, що забезпечення цього суверенітету є питанням національної безпеки. Натомість зазначений закон був орієнтований, переважно, на захист прав приватних суб'єктів в інформаційній сфері, та їх взаємини з цього приводу з органами публічної влади.

Наступним важливим кроком у напрямку становлення і розвитку інформаційної сфери в нашій державі стало прийняття у 1993 році законів «Про науково-технічну інформацію» від 25.06.1993 р. № 3322-XII та «Про друковані засоби масової інформації (пресу) в Україні» від 06.11.1992 р. № 2782-XII. Перший нормативно-правовий акт (тобто закон «Про науково-технічну інформацію») визначив основи державної політики в галузі науково-технічної інформації, порядок її формування і реалізації в інтересах науково-технічного, економічного і соціального прогресу країни. Метою Закону було визначене наступне: створення в Україні правової бази для одержання та використання науково-технічної інформації. Закон врегулював правові і економічні відносини громадян, юридичних осіб, держави, що виникають при створенні, одержанні, використанні та поширенні науково-технічної інформації, а також визначаються правові форми міжнародного

співробітництва в цій галузі. Дія цього Закону була поширена на підприємства, установи, організації незалежно від форм власності, а також громадян, які мають право на одержання, використання та поширення науково-технічної інформації. Однак положення зазначеного закону на стосувалися інформації, що містить державну та іншу охоронювану законом таємницю. Важливим моментом цього закону є те, що саме в ньому чи не вперше було використана понятійно-термінологічна конструкція «інтереси національної безпеки» саме у розрізі інформаційної сфери та інформаційної діяльності. Зокрема у цьому законі було закріплено, що національна система науково-технічної інформації має функціонувати з урахуванням інтересів національної безпеки. Національна система науково-технічної інформації – це організаційно-правова структура, за допомогою якої формується державна інформаційна політика, а також здійснюється координація робіт по створенню, користуванню, зберіганню та поширенню національних ресурсів науково-технічної інформації [107].

Закон «Про друковані засоби масової інформації (пресу) в Україні» від 06.11.1992 р. № 2782-XII був покликаний створити правові основи діяльності друкованих засобів масової інформації (преси) в Україні, встановити державні гарантії їх свободи відповідно до Конституції України, Закону України «Про інформацію» та інших актів чинного законодавства і визнаних Україною міжнародно-правових документів [89]. Прийняття цього нормативно-правового акту відіграло дуже суттєву роль для забезпечення свободи слова та розвитку механізмів функціонування інформаційної сфери в Україні, втім, я к і у випадку із вище згаданим законом «Про інформацію», законодавство про друковані ЗМІ (пресу), не містило положень, які б прямо свідчили про те, що цей законодавчий акт в тому в тому числі орієнтований на забезпечення інформаційної безпеки держави. Те ж саме стосується і закону «Про телебачення і радіомовлення» від 21.12.1993 р. N 3759-XII, в якому прямо не йшлося про національну безпеку. Одна, разом із тим, слід відмітити, що у цьому нормативно-правовому акті містилися деякі

положення, які стосувалися державних інтересів та територіальної цілісності, а саме того, що інформаційна діяльність не повинна їм загрожувати чи посягати на них. Зокрема у статті 2 закону N 3759-XII були закріплені основні принципи діяльності телерадіоорганізацій, а саме: «Телерадіоорганізації України у своїй діяльності реалізують принципи об'єктивності, достовірності інформації, компетентності, гарантування права кожного громадянина на доступ до інформації, вільне висловлювання своїх поглядів та думок, забезпечення ідеологічного та політичного плюралізму, дотримання телерадіопрацівниками професійної етики та загальнолюдських норм моралі. Телерадіоорганізації не мають права у своїх програмах розголошувати дані, що становлять державну таємницю або іншу таємницю, яка охороняється законодавством, закликати до насильницької зміни або повалення існуючого державного і суспільного ладу, порушення територіальної цілісності України, вести пропаганду війни, насильства і жорстокості, розпалювання расової, національної, релігійної ворожнечі, поширювати порнографію або іншу інформацію, яка підриває суспільну мораль або підбурює до правопорушень, принижує честь і гідність людини» [131]. Крім того, у цьому ж законі у статті, що стосується ліцензування каналів мовлення, зазначається, що під час проведення конкурсного відбору між заявниками на отримання ліцензії Національна рада враховує: інтереси телеглядачів і радіослухачів; необхідність захисту загальнонаціональних інтересів, поширення культурних цінностей; необхідність більш повного висвітлення позицій різних соціальних груп в теле- і радіопрограмах; відповідність умов, зазначених у заяві про видачу ліцензії, конкурсним умовам; відповідність технічних можливостей та творчого потенціалу в організації телерадіомовлення заявленим характеристикам, зобов'язанням телерадіоорганізацій щодо ведення соціального мовлення [131].

Важливим кроком на шляху забезпечення інформаційної безпеки в Україні стало прийняття у січні 1994 року закону «Про державну таємницю», в якому зазначалося, що виходячи з інформаційного суверенітету України та

загальновизнаних принципів міжнародного порядку у сфері інформації цей Закон регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, її засекречуванням та охороною з метою захисту життєво важливих інтересів України у сфері оборони, економіки, зовнішніх відносин, державної безпеки і охорони правопорядку [87]. Даний закон став логічним продовженням закону «Про інформацію», зокрема статті 30 останнього, що стосувалася інформації з обмеженим доступом. Однак у цій статті положення щодо такого роду інформації (тобто з обмеженим доступом) статті викладені у досить загальному вигляді. Втім у законі «Про державну таємницю» вже було більш детально врегульовано засади поводження з таємною інформацією, що має особливе значення для держави і суспільства. Державною таємницею, відповідно до цього закону визнається вид таємної інформації, що охоплює відомості у сфері оборони, економіки, зовнішніх відносин, державної безпеки і охорони правопорядку, розголошення яких може завдати шкоди життєво важливим інтересам України і які визнані у порядку, встановленому цим Законом, державною таємницею та підлягають охороні з боку держави [87]. Вжалим моментами Закону України «Про державну таємницю» є те, що в ньому, по-перше, нарешті на офіційному чітко було визнано, що інформація може становити загрозу для державної безпеки, зокрема це слідує із статті 3 вказаного нормативно-правового акту, в якій записано, що державну політику щодо державної таємниці як складову частину загальнонаціональної інформаційної політики та політики забезпечення безпеки України від внутрішніх та зовнішніх загроз формує Верховна Рада України; по-друге, у цій же статті зазначаються суб’єкти, які опікуються питаннями державної таємниці, а отже й інформаційної безпеки країни, а саме: Верховна рада України, яка, як зазначалося вище, формує відповідну державну політику, Президент України, Кабінет Міністрів України, Рада Міністрів Республіки Крим, інші органи державної виконавчої влади, а також органи місцевого і регіонального самоврядування, які забезпечують реалізацію цієї політики в межах своєї компетенції,

передбаченої законодавством. Спеціально уповноваженим центральним органом державної виконавчої влади у сфері забезпечення охорони державної таємниці є Державний комітет України з питань державних секретів. Положення про Державний комітет України з питань державних секретів затверджується Кабінетом Міністрів України. Окремі функції у цій сфері, в тому числі щодо технічного захисту інформації, оперативних заходів охорони державної таємниці, фельд'єгерського зв'язку, охорони державної таємниці у засобах масової інформації, виконують відповідні державні органи в межах повноважень, передбачених законодавством [87].

На початку липня 1994 року парламент України прийняв закон «Про захист інформації в інформаційно-комунікаційних системах», який був спрямований на охорону інформації, втім його положення стосувалися прав фізичних та юридичних осіб у інформаційній сфері і не торкався питань інформаційної безпеки як складової національної безпеки України. Зокрема у цьому законі було закріплено, що його метою є встановлення основ регулювання правових відносин щодо захисту інформації в автоматизованих системах за умови дотримання права власності громадян України і юридичних осіб на інформацію та права доступу до неї, права власника інформації на її захист, а також встановленого чинним законодавством обмеження на доступ до інформації [98].

Також слід відмітити закон № 74/95-ВР, ВРУ «Про інформаційні агентства» прийнятий парламентом України 28.02.1995 р., який закріплював правові основи діяльності в Україні інформаційних агентств та їх міжнародного співробітництва. У контексті проблематики представленого дослідження слід відмітити статтю 2 цього нормативно-правового акту, в якій закріплені гарантії свободи діяльності інформаційних агентств. У вказаній статті закріплено, що забороняється цензура інформації, поширюваної інформаційними агентствами. Однак, у той же час, інформаційні агентства не мають права у своїх матеріалах розголошувати дані, що становлять державну таємницю, або іншу інформацію, яка охороняється законодавством, закликати

до насильницької зміни або повалення існуючого конституційного ладу, порушення територіальної цілісності України, підриву її безпеки, вести пропаганду війни, насильства і жорстокості, розпалювати расову, національну, релігійну ворожнечу, розповсюджувати порнографію або іншу інформацію, яка підриває суспільну мораль або підбурює до правопорушень, принижує честь і гідність людини, а також інформацію, яка ущемляє законні права й інтереси громадян, давати оцінку щодо винуватості осіб у здійсненні злочину, вказувати на особу, яка ніби скоїла злочин до рішення суду, публікувати матеріали, які розкривають тактику і методику розслідування [100].

28 червня 1996 року в нашій державі нарешті був прийнятий новий Основний закон – Конституція України, в якому, окрім іншого, йшлося і про інформаційну безпеку. Зокрема у статті 17 Конституції було закріплено, що захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу [51].

Отже, період від проголошення державного суверенітету до прийняття Конституції України включно, тобто 1990 - 1996 роки 20-го століття, можемо умовно позначити як перший етап становлення та розвитку інформаційної безпеки України. Характерними властивостями того часу стало: по-перше, визнання офіційною владою інформаційної сфери як окремої, самостійної і вкрай важливої галузі суспільного життя; по-друге, закріплення того, що інформація та інформаційна діяльність не лише сприяють розвитку держави і суспільства, але можуть становити суттєву загрозу для їх інтересів; по-третє, встановлення організаційно-правових засад державної політики в інформаційній сфері, при цьому окрема увага приділена охороні і захисту інформації, яка має особливе значення для забезпечення безпеки українського суспільства і держави; по-четверте, окреслення владних інституцій, які опікуються питаннями державної інформаційної політики, і наділені відповідними повноваженнями.

Втім, попре зазначені позитивні кроки у напрямку забезпечення інформаційної безпеки України, зроблені протягом 1990 - 1996 років, говорити про те, що саме у цей час почалося формування цілісного механізму забезпечення зазнаної безпеки, навряд чи доцільно, адже тоді ще не існувало чіткого розуміння сутності інформаційної безпеки як складової національної безпеки, не було закладено концептуальних і стратегічних засад організації, функціонування та розвитку механізму інформаційної безпеки. Тож, визначивши зазначений період деякі засади функціонування інформаційного простору в Україні та здійснення державної політики щодо цього простору, управління ним, влада заклала необхідні підвалини для формування механізму забезпечення інформаційної безпеки України.

Наступний етап становлення і розвитку інформаційної безпеки України розпочався у 1998 році разом із прийняттям Концепції Національної програми інформатизації, затвердженої Законом України від 04.02.1998 р. № 75/98-ВР. У цьому документі було викладено цілу низку важливих положень щодо інформаційної безпеки держави, зокрема зазначається, що першочергові пріоритети надаються створенню нормативно-правової бази інформатизації, включаючи систему захисту авторських прав і особистої інформації, розробленню національних стандартів у галузі інформатизації; формуванню телекомунікаційної інфраструктури, перш за все оптимізації діючої мережі магістралей передачі даних, будівництву нових сучасних каналів, включаючи волоконно-оптичні та супутникові системи зв'язку; формуванню комп'ютерної мережі освіти, науки та культури як частини загальносвітової мережі INTERNET; здійсненню заходів щодо інформаційної безпеки. Головною метою зазначеної Програми стало забезпечення громадян та суспільства своєчасною, достовірною та повною інформацією на основі широкого використання інформаційних технологій, забезпечення інформаційної безпеки держави. При цьому Програма формується виходячи з довгострокових пріоритетів економічного, науково-технічного, соціального, національно-культурного розвитку країни з урахуванням світових досягнень

науки та тенденцій у сфері інформатизації і спрямована на розв'язання найважливіших загальносуспільних проблем, а саме: охорони довкілля та здоров'я людини, розвитку систем освіти та науки, економічного реформування, демократизації суспільства та створення умов для інтеграції України у світовий інформаційний простір згідно з сучасними тенденціями інформаційної геополітики, забезпечення обороноздатності та державної безпеки [103]. Та чи не найважливішим положенням Концепції Національної програми інформатизації у світлі досліджуваної нами проблематики є те, в якому зазначається, що інформаційна безпека є невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки. Об'єктами інформаційної безпеки є інформаційні ресурси, канали інформаційного обміну і телекомунікації, механізми забезпечення функціонування телекомунікаційних систем і мереж та інші елементи інформаційної інфраструктури країни [103].

Затвердження вище згаданої Концепції Національної програми інформатизації стало таким важливим і таким необхідним поштовхом на шляху подальшого становлення і розвитку інформаційної безпеки. С. Є. Антонова, Г. Ф. Мартинюк наголошують, що саме після прийняття зазначеної Концепції проблемам інформаційної діяльності та інформаційного суверенітету країни починає приділятися значна увага, в результаті чого відбувається активний процес прийняття нормативно-правових документів та інституційних змін у сфері забезпечення інформаційної безпеки [8]. Разом із зазначеною Концепцією Національної програми інформатизації був прийнятий і Закон України «Про Національну програму інформатизації» від 04.02.1998 р. № 74/98-ВР, в якому було закріплено, що інформаційний суверенітет держави – це здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави. Національна програма інформатизації, згідно Закону спрямована на розв'язання найважливіших загальносуспільних проблем, а саме:

забезпечення розвитку освіти, науки, культури, охорони довкілля та здоров'я людини, державного управління, національної безпеки та оборони держави та демократизації суспільства та створення умов для інтеграції України у світовий інформаційний простір відповідно до сучасних тенденцій інформаційної геополітики. Головною метою Національної програми інформатизації є створення необхідних умов для забезпечення громадян та суспільства своєчасною, достовірною та повною інформацією шляхом широкого використання інформаційних технологій, забезпечення інформаційної безпеки держави. А забезпечення інформаційної безпеки держави у статті 6 Закон України «Про Національну програму інформатизації» було прямо закріплено як одну із ключових функцій держави [110].

Також варто відмітити закон «Про телекомунікації» № 1280-IV, прийнятий українським парламентом 18 листопада 2003 року. У цьому нормативно-правовому документі було визначено, що інформаційна безпека телекомунікаційних мереж – здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації. Закон передбачав гарантії охорони таємниці телефонних розмов, телеграфної та іншої кореспонденції, безпека телекомунікацій. Зокрема у законі встановлювалося, що охорона таємниці телефонних розмов, телеграфної чи іншої кореспонденції, що передаються технічними засобами телекомунікацій, та інформаційна безпека телекомунікаційних мереж гарантуються Конституцією та законами України. Зняття інформації з телекомунікаційних мереж заборонене, крім випадків, передбачених законом. Оператори, провайдери телекомунікацій зобов'язані вживати відповідно до законодавства технічних та організаційних заходів із захисту телекомунікаційних мереж, засобів телекомунікацій, інформації з обмеженим доступом про організацію телекомунікаційних мереж та інформації, що передається цими мережами. В якості мети державного регулювання у сфері

телекомунікацій в закону було встановлене наступне: максимальне задоволення попиту споживачів на телекомунікаційні послуги, створення сприятливих організаційних та економічних умов для залучення інвестицій, збільшення обсягів послуг та підвищення їх якості, розвитку та модернізації телекомунікаційних мереж з урахуванням інтересів національної безпеки. Законом прямо заборонялося використання кінцевого обладнання споживача для вчинення протиправних дій або дій, що суперечать інтересам національної безпеки, оборони та охорони правопорядку [132].

Важливим заходом у розрізі досліджуваної проблематики стало прийняття Закону України «Про державну службу спеціального зв’язку та захисту інформації України» від 23.0.2.2006 р. № 3475-IV. Державна служба спеціального зв'язку та захисту інформації України є державним органом, який призначений для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації. Діяльність Державної служби спеціального зв'язку та захисту інформації України спрямовується Кабінетом Міністрів України, який здійснює заходи щодо забезпечення її функціонування. Державна служба спеціального зв'язку та захисту інформації України підконтрольна Верховній Раді України. З питань, пов'язаних із забезпеченням національної безпеки України, Державна служба спеціального зв'язку та захисту інформації України підпорядковується і підконтрольна Президентові України [86]. Тобто в Україні нарешті було створено спеціальний суб’єкт публічної влади, який має опікуватися питаннями захисту інформації, що є важливою для забезпечення інтересів України.

Доцільним буде відмітити й Указ Президента України «Про воєнну доктрину України» від 15.06.2004 р. № 648/2004. В цій доктрині містилося ряд важливих положень щодо ролі інформації у сучасній воєнно-політичній обстановці та значенні забезпечення інформаційної безпеки. Зокрема у

доктрині зазначалося, що воєнно-політична обстановка у світі є динамічною і розвивається під впливом низки тенденцій, в тому числі такої як прискорення розвитку інформаційних технологій, збільшення спроможностей держав щодо проведення інформаційних та інформаційно-психологічних операцій, посилення чутливості суспільства до загибелі мирного населення та втрат особового складу військових формувань у воєнних конфліктах. Україна розглядає як воєнно-політичні ризики або виклики, що підвищують рівень загрози застосування воєнної сили проти України, такі наміри чи дії держав, коаліцій держав як проведення інформаційно-психологічних заходів щодо дестабілізації соціально-політичної обстановки, міжетнічних та міжконфесійних відносин в Україні або її окремих регіонах і місцях компактного проживання національних меншин [85]. Також у доктрині відмічається, що сучасним воєнним конфліктам притаманні такі риси: підвищення ролі політичних, економічних, інформаційних засобів під час підготовки і в ході воєнного конфлікту; збільшення ролі інформаційно-психологічних операцій у досягненні цілей воєнних конфліктів. А одним із шляхів запобігання виникненню воєнних конфліктів є забезпечення інформаційної безпеки [85].

Окрім прийняття вище зазначених нормативно-правових актів, слід відзначити такий важливий крок у напрямку удосконалення та розвитку нормативно-правових засад інформаційної безпеки України як ратифікація у 2005 році Конвенції про кіберзлочинність [50]. У концепції акцентувалася увага на тому, що по-перше, наразі суттєво зросли ризики того, що комп'ютерні мережі та електронна інформація можуть також використовуватися для здійснення кримінальних правопорушень, і того, що докази, пов'язані з такими правопорушеннями, можуть зберігатися і передаватися такими мережами; по-друге, нагальною є необхідність співробітництва між Державами і приватними підприємствами для боротьби з кіберзлочинністю і необхідність захисту законних інтересів у ході використання і розвитку інформаційних технологій [50].

Отже, другий період становлення і розвитку інформаційної безпеки України, який припадає на 1998 – 2006 роки, був не такий насичений за кількістю прийнятих нових нормативно-правових актів з питань інформації та інформаційної діяльності, однак він ознаменувався перш за все тим, що саме на цьому етапі українська влада нарешті прямо позначила інформаційну безпеку як неодмінну і вкрай важливу складову національної безпеки. Також на даному етапі були вперше, з моменту проголошення незалежності України, сформульовані та закріплені на офіційному рівні деякі концептуальні засади та програмні цілі і завдання забезпечення інформаційної безпеки в нашій державі. Крім того, в якості позитивних моментів, що властиві даному етапу становлення і розвитку інформаційної безпеки України, слід відмітити те, що: по-перше, українська влада почала усвідомлювати загрози інформаційній безпеці держави, які несе в собі широке впровадження і активне використання інформаційно-комп'ютерних технологій; по-друге, Україна приєдналася до міжнародних документів з питань протидії злочинності в кіберпросторі та захисту інформації; по-третє, було створено спеціальний орган публічної влади з питань захисту інформації, що становить особливе значення для українського суспільства і держави; по-четверте, визнано інформацію та інформаційні технології потужнім засобом дестабілізації суспільно-політичної обстановки в країні, що застосовується для підвищення ефективного та ведення воєнних конфліктів. Відповідно ефективний механізм забезпечення інформаційної безпеки є одним із важливих інструментів протидії воєнним конфліктам.

Наступний етап становлення і розвитку інформаційної безпеки України розпочався у 2007 році, коли були прийняті такі нормативно-правові акти як: Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 09.01.2007 р. № 537-V та Указу Президента України «Про Стратегію національної безпеки України» від 12.02.2007 р.№ 105/2007. У законі від 09.01.2007 р. № 537-V зазначається, що одним з головних пріоритетів України є прагнення побудувати орієнтоване на

інтереси людей, відкрите для всіх і спрямоване на розвиток інформаційне суспільство, в якому кожен міг би створювати і накопичувати інформацію та знання, мати до них вільний доступ, користуватися і обмінюватися ними, щоб надати можливість кожній людині повною мірою реалізувати свій потенціал, сприяючи суспільному і особистому розвиткові та підвищуючи якість життя. Україна має власну історію розвитку базових засад інформаційного суспільства: діяльність всесвітньо відомої школи кібернетики; формування на початку 90-х років минулого століття концепції та програми інформатизації; створення різноманітних інформаційно-комунікаційних технологій (ІКТ) і загальнодержавних інформаційно-аналітичних систем різного рівня та призначення [112]. У законі підкреслюється, що попередні роки в нашій державі були сформовані певні правові засади побудови інформаційного суспільства: прийнято ряд нормативно-правових актів, які, зокрема, регулюють суспільні відносини щодо створення інформаційних електронних ресурсів, захисту прав інтелектуальної власності на ці ресурси, впровадження електронного документообігу, захисту інформації. Однак разом з тим ступінь розбудови інформаційного суспільства в Україні порівняно із світовими тенденціями є недостатнім і не відповідає потенціалу та можливостям України, в тому числі і через проблеми безпеки в інформаційній сфері [112]. До основних стратегічних цілей розвитку інформаційного суспільства в Україні віднесено, окрім іншого, вдосконалення законодавства з регулювання інформаційних відносин, а також покращення стану інформаційної безпеки в умовах використання новітніх ІКТ. А національна політика розвитку інформаційного суспільства в Україні ґрунтується на засадах забезпечення інформаційної безпеки [112]. Особливу увагу слід звернути на те, що у цьому Законі закріплене визначення поняття «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 [112]. Також у цьому нормативно-правовому акті відмічається, що за умов швидкого розвитку глобального інформаційного суспільства, широкого використання ІКТ у всіх сферах життя особливого значення набувають проблеми інформаційної безпеки [112]. Вирішення наявних проблеми інформаційної безпеки пропонувалося здійснювати наступними шляхами: створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів; підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань; вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері; розгортання та розвитку Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація [112].

Що ж стосується другого нормативно-правового акту, тобто Указу Президента України «Про Стратегію національної безпеки України» від 12.02.2007 р. № 105/2007, то у цьому документі зауважується на тому, що на тлі посилення загроз і зростання нестабільності у світі постають нові виклики міжнародній безпеці у сировинній, енергетичній, фінансовій, інформаційній, екологічній, продовольчій сферах [128]. Тобто сфера інформації та інформаційної діяльності визнані як пріоритетний об’єкт державного забезпечення і захисту. Власне для забезпечення інформаційної безпеки у Стратегії визначені наступні пріоритети і напрямки роботи: стимулювання впровадження новітніх інформаційних технологій і виробництва конкурентоспроможного національного інформаційного

продукту, зокрема сучасних засобів і систем захисту інформаційних ресурсів; забезпечення безпеки інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, кредитно-банківської та інших сфер економіки, систем управління об'єктами критичної інфраструктури; розробка та впровадження національних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих із відповідними стандартами держав-членів ЄС, у тому числі згідно з вимогами Конвенції про кіберзлочинність [128].

Наступними важливими нормативно-правовими актами у розрізі досліджуваної проблематики стали закони «Про захист персональних даних» від 01.06.2010 р. № 2297-VI та «Про засади внутрішньої і зовнішньої політики» від 01.07.2010 р. № 2411-VI. Перший закон регулює правові відносини, пов’язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних, тобто він орієнтований переважно забезпечення особистої інформаційної безпеки населення України [99]. Однак, у той же час у Законі «Про захист персональних даних» закріплено, що навіть інформація, що охороняється відповідно до цього може бути оброблена і поширена без згоди відповідної особи, якої ця інформація стосується, якщо йдеться про питання забезпечення національної безпеки. У вище згаданому законі «Про засади внутрішньої і зовнішньої політики» зазначається, що однією із основних засад внутрішньої політики у сфері національної безпеки і оборони є забезпечення життєво важливих інтересів людини і громадянина, суспільства і держави, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам в інформаційній сфері. Держава піклується про: забезпечення свободи медіа та безперешкодного доступу до публічної інформації, створення умов для розвитку інформаційних технологій та інформаційного суспільства, широкої

інтеграції і доступу громадян до світового інформаційного простору; створення суспільного мовлення та надання державної підтримки національному інформаційному продукту, здійснення заходів щодо захисту національного інформаційного простору [91].

Суттєвою подією третього етапу становлення і розвитку інформаційної безпеки України стало прийняття у 2011 році нової редакції Закону України «про інформацію», в якому було закріплено, що одним із основних напрямів державної інформаційної політики є забезпечення інформаційної безпеки України. Також у новій редакції вказаного закону передбачено, що право на інформацію може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку, з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя. Не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини. До конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження [101].

В цілому третій етап становлення та розвитку інформаційної безпеки, який тривав протягом 2007 до 2014 років характеризується тим що:

- було сформульоване і закріплене на законодавчому рівні поняття інформаційної безпеки;

- інформаційна безпека була віднесена до однієї із ключових і пріоритетних на даному етапі суспільного розвитку сфер державної політики;

- закріплений пріоритет національних інтересів у сфері інформаційної безпеки перед індивідуальними;

- визначені основні проблеми забезпечення інформаційної безпеки в

Україні, а також засоби і шляхи їх усунення та подальшого удосконалення механізму інформаційної безпеки;

- починають впроваджуватися міжнародні стандарти і норми протидії злочинній активності у інформаційному (зокрема кібернетичному) просторі.

Однак, попри безумовно позитивні та такі важливі зміни у державній інформаційні й політиці, слід відмітити, що ті її завдання і аспекти, які стосуються саме забезпечення інформаційної безпеки все ще не склалися у комплексний підхід до врегулювання цього боку інформаційної сфери. Йдеться про те, що влада сфокусувалася на розвитку інформаційних технологій, їх активному впровадженні в усі ключові сфери суспільного життя, підвищенні інформаційної освіченості населення, а питанням інформаційної безпеки приділялася хоча і суттєва, втім вторинна увага, як необхідному кроку для протидії тим можливим ризикам і загрозам, що можуть нести у собі інформатизація та цифровізації суспільства.

Наступний, тобто четвертий, етап становлення і розвитку інформаційної безпеки України розпочався у 2014 році після російської агресії проти нашої держави і триває до теперішнього часу. Саме ця подія досить чітко вказала на те: що війна може бути не лише у вигляді збройного протистояння, але й інформаційною, а фронт, відповідно може бути як військовий, так й інформаційний; що інформаційний суверенітет – це не якесь абстрактне, а цілком реальне явище, від забезпечення якого залежать і державність, і територіальна цілісність, і національна ідентичність; що для того, щоб захистити національні інтереси не достатньо запровадити заходи протидії лише окремим проявам злочинної активності в інформаційній сфері, натомість має бути сформований цілісний, комплексний, дієвий механізм, який би дозволяв вчасно виявляти та ефективно протистояти інформаційним загрозам будь-якого характеру і масштабу.

На даному етапі вже було прийнято цілий ряд важливих нормативно-правових актів, як законів, так і підзаконного характеру, спрямованих на забезпечення інформаційної безпеки нашої держави. Одним із перших серед

таких нормативно-правових актів став Указ Президента України «Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України»» від 01.05.2014 р. № 449/2014 [122]. У Рішенні РНБО України констатувалося, що Російська Федерація поширює недостовірну, неповну, упереджену інформацію про Україну, через що намагається маніпулювати суспільною свідомістю в Україні та за її межами. Тому, виходячи з необхідності вдосконалення нормативно-правового забезпечення та попередження й нейтралізації потенційних і реальних загроз національній безпеці в інформаційній сфері, Рада національної безпеки і оборони України доручила здійснити ряд заходів уряду України, Службі безпеці України та Державній службі спеціального зв'язку та захисту інформації України. І. О. Валюшко відмічає, що вказаний документ поставив завдання розроблення Стратегії кібернетичної безпеки України, Доктрини інформаційної безпеки України, механізму протидії негативному інформаційно-психологічному впливу, в тому числі шляхом заборони ретрансляції телевізійних каналів та ін.. Цей указ розпочав формування якісно іншої нормативно-правової бази України у сфері інформаційної безпеки [12, с.33]. І. О. Валюшко цілком справедливо наголошує на тому, що саме страшні наслідки російського втручання в Україну актуалізували питання інформаційної безпеки України. У цьому документі наголошено на необхідності прийняття основоположних документів в інформаційній сфері та внесення необхідних змін до вже існуючих. З початком агресії Росії на Сході нашої держави та окупації Криму гостро постало питання перегляду основних принципів до забезпечення її оборони та територіальної цілісності та переосмислення ролі інформаційної безпеки [12, с.33].

У травні 2015 року Президент України своїм Указом затвердив нову Стратегію національної безпеки України, в якій відмічалося, що до актуальних загроз нацбезпеки України належить інформаційно-психологічна

війна, приниження української мови і культури, фальшування української історії, формування російськими засобами масової комунікації альтернативної до дійсності викривленої інформаційної картини світу. Загрози інформаційній безпеці: ведення інформаційної війни проти України; відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства. Загрози кібербезпеці і безпеці інформаційних ресурсів: уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом. Пріоритетами забезпечення інформаційної безпеки у цій Стратегії було визначене наступне: забезпечення наступальності заходів політики інформаційної безпеки на основі асиметричних дій проти всіх форм і проявів інформаційної агресії; створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них; протидія інформаційним операціям проти України, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації, захист національних цінностей та зміцнення єдності українського суспільства; розробка і реалізація скоординованої інформаційної політики органів державної влади; виявлення суб'єктів українського інформаційного простору, що створені та/або використовуються Росією для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності; створення і розвиток інститутів, що відповідають за інформаційно-психологічну безпеку, з урахуванням практики держав-членів НАТО; удосконалення професійної підготовки у сфері інформаційної безпеки, упровадження загальнонаціональних освітніх програм з медіакультури із залученням громадянського суспільства та бізнесу [125]. Крім того у тексті Стратегії були визначені пріоритети забезпечення кібербезпеки і безпеки інформаційних ресурсів, а саме: розвиток інформаційної інфраструктури держави; створення системи забезпечення кібербезпеки, розвиток мережі реагування на комп'ютерні надзвичайні події (CERT); моніторинг кіберпростору з метою своєчасного виявлення,

запобігання кіберзагрозам і їх нейтралізації; розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів; забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, відмова від програмного забезпечення, зокрема антивірусного, розробленого у Російській Федерації; реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав – членів НАТО та ЄС; створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, зокрема в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки [125]. Дослідники відмічають, що вперше за всю історію створення таких документів ця Стратегія містить конкретний варіант програмних дій з точки зору забезпечення стратегії національної безпеки України. Ніколи попередні стратегії не завершувались механізмом виконання всією державною структурою управління безпеки країни. У цій же Стратегії останні рядки чітко визначають, що головне керівництво питаннями, пов'язаними з національною безпекою країни, здійснює Президент, консолідацію і контроль виконує РНБО, безпосередню реалізацію програмних завдань виконує Кабінет Міністрів [12, с.35-36].

Також у вересні 2015 року була прийнята нова редакція Воєнної доктрини України, в якій вже йшлося про інформаційну війну російської федерації проти України. У документі: підкреслюється, що модернізація та вдосконалення спеціальними службами іноземних держав систем і комплексів технічної розвідки, нарощування їх можливостей підвищують вразливість інформаційної інфраструктури України; акцентовано увагу на недостатності та непрофесійності зусиль органів державної влади України у сфері протидії пропаганді та інформаційно-психологічним операціям

Російської Федерації; наголошено на необхідності удосконалення державної інформаційної політики у воєнній сфері [118]. Зазначається, що необхідними є: взаємоузгоджене використання політико-дипломатичних, інформаційних та силових інструментів держави для протидії деструктивному тиску агресора на Україну та примушення його до дотримання норм міжнародного права та власних зобов'язань; посилення розвідувальної діяльності в інтересах підготовки та проведення Україною стратегічних комунікацій, контрпропагандистських заходів та інформаційно-психологічних операцій; підвищення ефективності спеціальних інформаційних заходів впливу в районі проведення антитерористичної операції в Донецькій та Луганській областях і на тимчасово окупованій території та зосередження сил і засобів для організації ефективної протидії проведенню ворожих інформаційно-психологічних операцій проти України [118].

Важливим доповненням до двох вище згаданих документів, тобто Воєнної доктрини України та Стратегії національної безпеки України стала Стратегія кібербезпеки України від 27.01.2016 р. Адже у Воєнній доктрині та стратегії нацбезпеки України йшлося про загрози кібербезпеці нашої держави і необхідність її посилення, втім вони не містили детального підходу до бачення концептуальних засад забезпечення безпеки кіберпростору нашої держави. Метою Стратегії кібербезпеки України є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [121]. Розвиток безпечного, стабільного і надійного кіберпростору має полягати, насамперед, у: виробленні і оперативній адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягненні сумісності з відповідними стандартами ЄС та НАТО; створенні вітчизняної нормативно-правової та термінологічної бази у цій сфері, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної та кібербезпеки відповідно до міжнародних стандартів і стандартів ЄС та НАТО; формуванні конкурентного середовища у сфері електронних

комунікацій, наданні послуг із захисту інформації та кіберзахисту та ін. [121].

У березні 2021 року Воєнна доктрина України у редакції від 2015 року припинила свою дію, а замість неї було затверджено Стратегію воєнної безпеки України [120]. Також у лютому 2022 року Президента України своїм Указом ввів у дію рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки» [124]. А нову Стратегію кібербезпеки України було введено в дію 26.08.2021 року, відповідно до Указу Президента України № 447/2021. Ми не будемо зараз детально вдаватися у положення цих документів, оскільки далі більш детально розглядатимемо нормативно-правові засади та напрямки сучасної державної політики у сфері забезпечення інформаційної безпеки, які власне і закріплені у цих стратегічних документах. Також у цьому контексті слід відмітити Розпорядження КМУ від 2018 року «Про схвалення Стратегії інформаційної реінтеграції Автономної Республіки Крим та м. Севастополя» (№ 1100-р) та «Про схвалення Стратегії інформаційної реінтеграції Донецької та Луганської областей» (539-р).

Особливо важливим кроком на 4-ому, тобто нинішньому, етапі становлення і розвитку інформаційної безпеки України стало прийняття і затвердження наступних двох документів в інформаційній сфер:

- по-перше, це Доктрина інформаційної безпеки України, затверджена Указом Президента України від 25.02.2017 р. № 47/2017, в якій було акцентовано увагу на тому що застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Саме проти України Російська Федерація використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України. Комплексний характер актуальних загроз національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до

формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації [123]. У цій Доктрині були визначені національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері. А її мета полягала в уточненні засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни [123]. Прийняття цієї Доктрини було вкрай важливим та необхідним кроком на шляху розвитку інформаційної безпеки України, однак у той же час не можна не відмітити, що вона була створена швидше як акт реагування на гібриду війну з боку росії, аніж як документ, який має закласти загальні концептуальні засади у зазначеній сфері, визначити найбільш важливі та принципові положення державної політики у ній, незалежно від того, про яку саме загрозу національним інтересам в інформаційні сфері йдеться;

по-друге, Стратегія інформаційної безпеки, яка замінила вище згадану Доктрину. У Стратегії окреслюються як глобальні і національні загрози та виклики інформаційній безпеці України, так і цілі та шляхи протидії їм, а також заходи щодо зміцнення інформаційної безпеки нашої держави. Основними напрямами забезпечення інформаційної безпеки України є стійкість та взаємодія, для досягнення яких необхідним є виконання таких стратегічних цілей та завдань [117]. Більш детально про зміст цієї Стратегії, закріплені у ній цілі та пріоритети, ми поговоримо у наступних підрозділах представленого дослідження. Окрім цього у період із 2014 року і до сьогодні було прийнято ще ряд важливих законів і підзаконних актів як то: закони «Про основні засади забезпечення кібербезпеки України» (2017), «Про національну безпеку України» (2018), «Про медіа» (2022), Постанова КМУ «Про утворення територіального органу Національної поліції» (2015), якою утворено Департамент кіберполіції та ін..

В цілому, підсумовуючи вище викладене, можемо констатувати, що

тільки після початку агресії російської федерації проти України, яка в тому числі здійснюється в інформаційному просторі, українське суспільство та публічна влада почали по-справжньому уважно і відповідально ставитися до питання забезпечення інформаційної безпеки. Зокрема йдеться про те, що від визнання деяких окремих загроз і викликів, що стоять перед Україною в інформаційній сфері, а також від визначення певних напрямків їх подолання, влада перейшла до: формулювання комплексу концептуальних засад, стратегічних пріоритетів, цілей і напрямків щодо забезпечення інформаційної безпеки України, як на глобальному, так і національному рівні; закріплення на законодавчому рівні основних засад організації та функціонування адміністративно-правового механізму забезпечення інформаційної безпеки із розподілом відповідних завдань і повноважень між суб'єктами публічної влади. Саме на цьому етапі інформаційної безпеки реально розкрилася як необхідна умова не просто протидії злочинності, а збереження української державності, територіальної цілісності та національної ідентичності.

1.2. Напрямки розвитку державної політики у сфері забезпечення реалізації інформаційної безпеки України.

Майже три десятиліття та агресія з боку російської федерації знадобилися для того, щоб українська влада почала розглядати питання інформаційної безпеки держави як самостійну і вкрай важливу галузь державної політики, від ефективності здійснення якої залежить національна безпека України, тобто захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних і потенційних загроз. Під національними інтересами слід розуміти життєво важливі інтереси людини, суспільства і держави, реалізація яких забезпечує державний суверенітет України, її прогресивний демократичний розвиток, а також безпечні умови

життєдіяльності і добробут її громадян [108]. Сьогодні, як і раніше, в нашій країні особлива увага приділяється розвитку інформаційного суспільства, комп'ютерних технологій та кіберпростору, однак при цьому, у реаліях війни росії проти України, яка ведеться як на фізичному полі бою, так і в інформаційному просторі (при чому інформаційний фронт проти нашої держави росія відкрила набагато раніше, аніж здійснила військове вторгнення), особливий акцент робиться на забезпеченні інформаційної безпеки держави та національних інтересів. Саме тому у цьому підрозділі ми більш детально розглянемо напрямки розвитку державної політики у сфері забезпечення реалізації інформаційної безпеки України.

Перш за все визначимося і з тим, що ж таке власне державна політика у сфері інформаційної безпеки. Під державною політикою, пише І. В. Розпутенко, слід розуміти дії системи органів державної влади згідно з визначеними цілями, напрямами, принципами для розв'язування сукупності взаємопов'язаних проблем у певній сфері суспільної діяльності. Державний курс – це пропонований курс діяльності уряду для задоволення потреб чи використання можливостей, сформульований із зазначенням очікуваних результатів та їх впливу на наявний стан справ і конкретне розв'язання проблем [34, с.144-145]. В. І. Андріяш вважає, що державну політику можна визначити, як напрямок дій (або бездіяльність), що обирає державна влада (або орган державної влади, що має повноваження: правові, політичні й фінансові) для вирішення певної проблеми або сукупності взаємозалежних проблем. Державна політика – це реакція держави на конкретні проблеми суспільства, або груп у цьому суспільстві, наприклад, громадян, неурядових організацій. Вона покликана погоджувати інтереси, знаходити консенсус, необхідний для стабільності суспільства [7]. О. В. Лаврук визначає державну політику як безперервний циклічний процес, котрий включає сукупність послідовних дій, взаємодію різних взаємопов'язаних елементів і інституцій з притаманними їм функціями й засобами досягнення кінцевих результатів (схвалення політики) [61, с.260]. Н.Р. Нижник, С.Д. Дубенко,

В.І. Мельниченко стверджують, що державна політика – це сукупність цілей і завдань, що практично реалізується державою, і засобів, які використовуються при цьому [30, с. 157]. Ю.В. Ковбасюк, К.О. Ващенко, Ю.П. Сурмін пропонують під державною політикою слід розуміти сукупність ціннісних цілей, державно-управлінських заходів, рішень і дій, порядок реалізації державно-політичних рішень (поставлених державною владою цілей) і системи державного управління розвитком країни [29, с.8]. В.Є. Романов, О. М. Рудік, Т. М. Брус, визначають державну політику як відносно стабільну, організовану та цілеспрямовану діяльність уряду стосовно певної проблеми або предмета розгляду, яка здійснюється ним безпосередньо або опосередковано через уповноважених агентів і впливає на життя суспільства [135, с. 12].

Отже, як видно із наведених наукових позицій, існує багато визначень поняття «державна політика», втім більшість дослідників тлумачать її як діяльність (сукупність дій чи процес), що здійснюється компетентними суб'єктами публічної влади, і яка спрямована на вирішення певних проблемних питань у тій чи іншій сфері суспільного життя, забезпечення її належного функціонування та розвитку, згідно поставлених цілей і пріоритетів. Це, у повній мірі стосується і державної політики у сфері забезпечення інформаційної безпеки України, під якою слід розуміти діяльність (дії, комплекс дій, рішення тощо) суб'єктів публічної влади щодо визначення мети (цілей), завдань, пріоритетів, напрямків засобів досягнення стабільності та захищеності національного інформаційного простору та інформаційних ресурсів від різного роду загроз як внутрішнього, так і зовнішнього характеру. Слід відмітити, що у чинній на сьогодні Стратегії інформаційної безпеки України закріплене визначення інформаційної безпеки України, під якою розуміється складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином

забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом [117].

Основні засади державної політики завжди визначаються на законодавчому рівні. Якщо говорити про державну політику з реалізації інформаційної безпеки України, то ключовими нормативно-правовими актами тут є вище згадана Стратегії інформаційної безпеки України, затвердженій Указом Глави держави від 28.12.2021 року №685/2021, в якій закріплено, що забезпечення інформаційної безпеки України є однією з найважливіших функцій держави. Стратегія інформаційної безпеки визначає актуальні виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних [117]. Метою цієї Стратегії визначене наступне: «посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина» [117]. Як видно із наведеного, навіть мета Стратегії орієнтована не просто на протистояння якомусь конкретному ворогу, зокрема російській федерації, як це було закріплено у Доктрині інформаційної безпеки від 2017 року, а розвиток і зміцнення усієї інформаційної сфери України в цілому, доведення стану її безпекових механізмів і засобів до такого рівня, за якого вона б могла вчасно та ефективно реагувати на внутрішні та зовнішні загрози і виклики. Разом із

тим до вище наведеної мети Стратегії інформаційної безпеки України є певні зауваження, а саме – це зміст деяких із тих явищ, на охорону і захист яких спрямовано дію засобів: «політична стабільність», «життєво важливі інтереси людини, суспільства і держави»). З цього приводу досить справедливо зауважує А. Сафаров, який вказує, що окрім іншого метою Стратегії визнано забезпечення інформаційної безпеки України, спрямованої на захист життєво важливих інтересів громадянина, суспільства та держави у протидії внутрішнім та зовнішнім загрозам, забезпечення захисту державного суверенітету і територіальної цілісності України, підтримка соціальної та політичної стабільності, забезпечення прав та свобод кожного громадянина. Однак, справедливо акцентує увагу А. Сафаров, законодавство України не містить визначень щодо «життєво важливих інтересів громадянина, суспільства та держави», «політичної стабільності» тощо. Одним з прикладів «політичної стабільності» можна назвати владу Путіна в Російській Федерації. Натомість постійна зміна влади в Україні через виборчий процес має ознаки «політичної нестабільності» [139]. Очевидно, що невизначеність змісту цих понятійно-термінологічних конструкцій, розмиває підстави і межі законності втручання влади у інформаційну діяльність інших суб'єктів і створює сприятливі умови для обмеження свободи у цій сфері. За таких обставин, одним із важливих моментів на шляху подальшого удосконалення та розвитку державної політики у сфері забезпечення реалізації інформаційної безпеки України є забезпечення більш ретельного підходу до визначення кола і, що вкрай важливо, змісту тих явищ, на охорону і захист яких спрямовуються засоби і механізми інформаційної безпеки.

Далі, розглядаючи напрямки розвитку реалізації державної політики у досліджуваній сфері, звернемося до розділу чинної Стратегії інформаційної безпеки України, в якому викладені цілі та напрямки реалізації Стратегії. Зокрема тут зазначається, що основними напрямами забезпечення інформаційної безпеки України є стійкість та взаємодія, для досягнення яких необхідним є виконання ряду стратегічних цілей та завдань. Так, наприклад,

до зазначених цілей віднесено наступне: «1) протидія дезінформації та інформаційним операціям, насамперед держави-агресора, спрямованим, серед іншого, на ліквідацію незалежності України, повалення конституційного ладу, порушення суверенітету і територіальної цілісності держави, пропаганду війни, насильства, жорстокості, розпалювання національної, міжетнічної, расової, релігійної ворожнечі та ненависті, вчинення терористичних актів, посягання на права і свободи людини; 2) забезпечення всебічного розвитку української культури та утвердження української громадянської ідентичності; 3) підвищення рівня медіакультури та медіаграмотності суспільства. Українське суспільство повинне бути захищене від деструктивного впливу дезінформації та маніпулятивної інформації, а медіасередовище - бути соціально відповідальним і функціонувати стабільно; 4) забезпечення дотримання прав особи на збирання, зберігання, використання та поширення інформації, свободу вираження своїх поглядів і переконань, захист приватного життя, доступ до об'єктивної та достовірної інформації, а також забезпечення захисту прав журналістів, гарантування їх безпеки під час виконання професійних обов'язків, протидія поширенню незаконного контенту; 5) інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих територіях та на прилеглих до них територіях України, до загальноукраїнського інформаційного простору, а також відновлення їх права на інформацію, що дає їм змогу підтримувати зв'язок з Україною; 6) створення ефективної системи стратегічних комунікацій; 7) розвиток інформаційного суспільства та підвищення рівня культури діалогу» [117]. Закріплені у Стратегії стратегічні напрямки та цілі її реалізації досить красномовно свідчать про те, що держава усвідомлює необхідність комплексного підходу до формування механізму забезпечення інформаційної безпеки, тобто йдеться не лише про створення і впровадження засобів та інструментів реагування на конкретні загрози, що вже у тому чи іншому вигляді віднайшли свій прояв в інформаційному просторі, а про формування

стійкого й одночасно гнучкого інформаційного середовища, учасники якого здатні: критично ставитися до інформації, її джерел та змісту; розуміти основні принципи і норми поводження в інформаційному просторі, користування інформаційними ресурсами; визначати пріоритети та розпізнавати загрози як для своїх приватних, такі публічних інтересів. За таких умов зміцнення інформаційної безпеки держави відбувається не тільки за рахунок безпосереднього державного втручання і боротьби з відповідними загрозами, але й завдяки тому, що саме спільнота інформаційного середовища стає більш стійкою до негативного інформаційного впливу, свідомо дотримуючись інформаційної гігієни.

Для досягнення зазначений цілей і забезпечення належного покращення інформаційної безпеки України, вважаємо, що держава має розвивати свою політику у сфері забезпечення реалізації інформаційної безпеки України за наступними напрямками:

1) ідеологічний. Ідеологія (грец. idea – поняття, logos –знання) – система концептуально оформлених уявлень, ідей і поглядів на політичне життя, принципи та форми державного устрою, яка відображає інтереси, ідеали, світогляд суб'єктів політики. Ідеологію можна назвати формою суспільної свідомості, за допомогою якої соціальні групи сприймають та розуміють навколишній світ. Слід відмітити, що ідея, є близькою до світогляду – філософське сприйняття людиною навколишнього світу; система життєвих цінностей, переконань, ідеалів, поглядів особистості на об'єктивний світ та своє місце в ньому) [34, с.272]. Водночас, наголошують дослідники, між світоглядом та ідеологією є й принципова різниця. Вона полягає в тому, що світогляд є характерною ознакою індивідуального світосприйняття, завжди статичного (що важко піддається будь-яким змінам), в той час як ідеологія притаманна, насамперед, соціальним спільнотам і має яскраво виражений динамічний характер, оскільки є основою організованої політичної діяльності із збереження, перетворення або руйнування суспільно-політичної дійсності. Ідеологія завжди базується на світогляді, але, зрештою,

спрямована на його перетворення (вдосконалення). Таким чином, якщо світогляд розглядати як ціннісну систему усвідомлення суспільно-політичної дійсності, то ідеологія виступатиме механізмом модернізації цієї системи [34, с.272]. Отже, ідеологія виражає ту систему ідей, цінностей, переконань, принципів, що несе у собі відповідна державна політика, до втілення яких має призвести цієї політики. Це, безумовно стосується й реалізації державної політики у сфері інформаційної безпеки. Тривалий час в нашій державі відбувається формування і впровадження ідеології інформаційного суспільства. М.О. Кириченко з цього приводу зазначає, що в усіх сферах управління (державного, регіонального, місцевого, господарського. військового, економічного) повинні відбуватися процеси формування ідеології інформаційного суспільства, так як сучасний етап розвитку суспільства характеризується зростаючою роллю інформаційної сфери, що є сукупністю інформації, інформаційної інфраструктури, суб'єктів, які здійснюють збирання, формування, розповсюдження і використання інформації, а також системи регулювання суспільних відносин, що при цьому виникають. Інформаційна система, виступаючи системоутворюючим фактором життя суспільства, активно впливає на стан суспільства, політичну, економічну, оборонну та безпекову діяльність України. Національна безпека України істотним чином залежить від забезпечення інформаційної безпеки і в процесі розгортання технічного прогресу ця залежність буде постійно зростати [44, с.79-80]. М.О. Кириченко підкреслює, що ідеологія інформаційного суспільства як фактор динамічного розвитку і безпеки сучасної України в XXI столітті є сукупністю інформаційних, організаційних, матеріально-технічних, кадрових ресурсів, призначених для вирішення будь-яких задач інноваційного науково-технічного розвитку як окремої особистості, так і держави. Сучасний стан динамічного розвитку України та її національної безпеки, справедливо вказує науковець, є результатом взаємодії цілого ряду факторів, що впливають на формування та розвиток ідеології інформаційного суспільства. В її числі помітне місце належить освіті, науці,

культурі, інтелігенції (національній еліті) України. Накопичення інноваційного та інтелектуального (наукового) потенціалу та міра його реалізації визначається якістю знань, ефективністю використання освітнього потенціалу у практичній діяльності та прагненням до формування ідеології інформаційного суспільства, яка б захищала на рівні держави потреби кожної особистості і формувалася як «ідеологія для всіх» [44, с.79-80]. Така позиція дослідника, висловлена ним у 2017 році у багатьох аспектах віднайшла свій прояв у чинній нині Стратегії інформаційної безпеки, в якій значна увага приділяється просвітництву, громадянській та медійній культурі, національній ідентичності тощо. Отже, враховуючи вище викладене, можемо дійти висновку про те, що ідеологія сучасної державної політики з реалізації інформаційної безпеки в Україні має враховувати цілу низку умов і факторів та, звичайно ж, не зводитися виключно до протистояння конкретному ворогу (у даний час це російська федерація, яка активно веде інформаційну війну проти України). В основі цієї ідеології мають бути як національні та громадянські, так і абсолютні (або всезагальні) цінності та принципи. Україна має прагнути сформувати і розвивати стійку і адаптивну інформаційну систему із широкими можливостями, яка здатна ефективно протистояти і національним, і глобальним загрозам. Ключовою ідеєю протидії зазначеним загрозам мають стати не стільки заборони і різного роду обмеження з метою відгородитися, закритися від усього, що є чи здається ворожим, небезпечним, незрозумілим, скільки високоефективна контрпропаганда та просвітницька робота, спрямована на виховання медійно грамотних людей, з високим рівнем інформаційної та громадянської культури, правової та національної свідомості, здатних критично ставитися до отриманої інформації та ідентифікувати відповідні загрози. Тож по-справжньому ефективний механізм забезпечення інформаційної безпеки не може спиратися на ізоляціонізм [13];

2) нормативно-правовий. У чинні Стратегії інформаційної безпеки України визначено, що однією із проблем, що негативно позначаються на цій безпеці є недосконаліть регулювання відносин у сфері інформаційної

діяльності та захисту професійної діяльності журналістів. У Стратегії відмічається, що регулювання відносин у сфері інформаційної діяльності не відповідає сучасним викликам та загрозам. Це перешкоджає розвитку українського медіа ринку, ускладнює ведення бізнесу у цій сфері, зберігає залежність засобів масової інформації від їх власників, не забезпечує додержання професійних стандартів діяльності журналістів. Актуальною проблемою є непоодинокі випадки втручання в професійну організаційно-творчу діяльність засобів масової інформації та в індивідуальну професійну творчу діяльність журналістів, інші посягання на свободу інформаційної діяльності, зокрема перешкоджання їх професійній діяльності, погрози, насильство щодо них, посягання на їх життя та власність. Зазначене позбавляє журналістів можливості належним чином інформувати суспільство про суспільно важливі події та явища [117]. Крім того, у зазначеній Стратегії відмічається, що її реалізація передбачає системного перегляду та внесення змін до відповідних законодавчих та інших нормативно-правових актів в інформаційній сфері [117]. На проблемах нормативно-правового (або законодавчого) характеру у сфері інформаційної безпеки увагу акцентують і ряд дослідників як то: Л.О. Кочубей, А.Ю. Нашинець-Наумова, М.О. Кириченко, Я. І. Чмир та ін.. Так, наприклад, Я. І. Чмир звертає увагу на недосконаліть законодавства щодо регулювання суспільних відносин в інформаційній сфері, недостатній рівень медіакультури нашого суспільства [157]. А, скажімо, А. Ю. Нашинець-Наумова стверджує, що протягом останніх років основною проблемою у галузі забезпечення вище згаданої безпеки, є непослідовність і нерозвиненість правового регулювання суспільних відносин у сфері інформації, що ускладнює дотримання необхідного балансу особистих, суспільних і державних інтересів у цій сфері. Недосконале правове регулювання не дає можливості завершити формування конкурентоспроможних українських інформаційних агентств і ЗМІ на території України [71, с.154].

Наразі ми не будемо детально вдаватися у проблеми правового

регулювання інформаційної безпеки України, оскільки стану цього регулювання у представленій роботі присвячений окремий підрозділ. Однак, з огляду на вище викладене, вважаємо, що розвиваючи свою політику щодо забезпечення інформаційної політики, держава повинна [14]:

- забезпечувати своєчасно оновлювати нормативно-правове підґрунтя механізму забезпечення інформаційної безпеки в Україні, приводячи його у відповідність до перспектив подальшого розвитку та актуальних викликів і загроз;

- забезпечити гармонійне поєднання прав і свобод людини та громадянина в інформаційній сфері з національними інтересами у ній;

- забезпечити нормативно-правові засади для ефективного просвітництва населення, підвищення їх медійної грамотності, правової культури та свідомості;

- забезпечити сприятливі нормативно-правові умови для розвитку економічної активності населення у інформаційній сфері;

- удосконалити матеріально-правові та процедурні засади контролю в інформаційній сфері, своєчасного виявлення та оцінювання ризиків;

- забезпечити сприятливе нормативно-праве середовище для взаємодії публічної влади всіх рівні із громадськістю з питань інформації та інформаційної діяльності;

3) організаційно-управлінський. Управлінська діяльність – це вид свідомо здійснюваної людської діяльності, спрямованої на ефективне функціонування здійснюваних робіт (індивідуально чи колективно) з досягнення тих чи інших цілей, вирішення відповідних завдань, виконання функцій [146, с. 197-212; 35, с.67]. Сутнісний зміст управлінської діяльності полягає у ефективній організації функціонування підпорядкованої або керованої системи задля належного виконання її завдань та функцій. У розрізі досліджуваної проблематики організаційно управлінський напрямок розвитку досліджуваної політики повинен передбачати:

- удосконалення системи суб’єктів забезпечення інформаційної

безпеки;

- поліпшення якості кадрового забезпечення суб’єктів, які займаються забезпеченням інформаційної безпеки;

- покращення механізмів контролю за інформаційною діяльністю. Зокрема слід відмітити, що у Стратегії інформаційної безпеки України закріплено, що до пріоритетних завдань держави, окрім іншого, належить: створення системи раннього виявлення, прогнозування та запобігання гібридним загрозам, зокрема, створення системи протидії дезінформації та інформаційним операціям, спрямованої на запобігання, максимально швидке виявлення та реагування держави і суспільства на інформаційні загрози; ужиття заходів щодо запобігання та протидії поширенню дезінформації та деструктивної пропаганди стосовно європейської та євроатлантичної інтеграції України [117];

- удосконалення механізмів координації діяльності суб’єктів із забезпечення інформаційної безпеки. Координація являє собою – метод управління, суттю якого є встановлення між суб’єктами та об’єктами державного управління горизонтальних зв’язків, тобто поєднання двох і більше однорівневих з точки зору визначеного критерію дій, що забезпечують досягнення запланованого результату. Координаційні відносини розрізняються за видами: узгодження, предметно-технологічна взаємодія, ієрархічна або складна взаємодія [34, с.346]. А. В. Шегда відмічає, що координація забезпечує узгодженість у часі й просторі дій органів управління та посадових осіб, а також між системою в цілому і зовнішнім середовищем. Вона, тобто координація, відіграє в управлінні роль, яку образно можна порівняти з роллю диригента в оркестрі. Саме завдяки їй забезпечується динамізм системи, створюється гармонія взаємозв'язків підрозділів, здійснюється маневр матеріальними та трудовими ресурсами всередині системи залежно від специфіки завдань. Об'єктом функції координація є як управляюча система, так і система якою управляють. Призначення діяльності органів управління — забезпечити єдність дій усіх управлінських підрозділів,

працівників управління та спеціалістів для найбільш ефективного впливу на відповідний робочий процес. Координація означає синхронізацію зусиль усього колективу, інтеграцію їх у єдине ціле, тобто це процес розподілу діяльності в часі, приведення окремих елементів у таке поєднання, яке дало б змогу найбільш ефективно та оперативно досягати поставленої мети. Координація — це головна функція процесу управління, яка забезпечує, по-перше, його єдність та безперервність і, по-друге, взаємозв'язок усіх функцій [160]. На відсутності належної координації як на одній із проблем, що негативно позначаються на ефективності забезпечення інформаційної безпеки акцентується увага і в Стратегії інформаційної безпеки. Зокрема у ній йдеться про те, що в Україні триває процес становлення системи стратегічних комунікацій. Органами державної влади України здійснено низку організаційних та практичних заходів зі зміцнення власної інституційної спроможності у сфері стратегічних комунікацій, однак не створено дієвого механізму координації і взаємодії між усіма органами державної влади, залученими до здійснення заходів із протидії загрозам в інформаційній сфері. Зазначене послаблює можливості до розбудови комплексного стратегічного планування інформаційного потоку, здійснення системної комунікативної діяльності Кабінету Міністрів України, об'єднання всіх ключових суб'єктів у сфері інформаційних відносин, суб'єктів формування і реалізації державної політики щодо ефективного захисту національного інформаційного простору, утвердження позитивного іміджу України, реалізації цілей захисту національної безпеки України в інформаційній сфері [117]. Слід відмітити, що у плані заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року передбачено в якості одно із заходів розроблення механізму міжвідомчої координації органів державної влади з протидії загрозам та викликам національній безпеці в інформаційній сфері [92];

4) культурно-освітній. Даний напрям державної політики у досліджуваній сфері стосується проведення роботи щодо підвищення

медійної грамотності населення і культури поводженні в інформаційному середовищі. Також важливим питанням, яке має вирішуватися за цим напрямком зазначеної політики, є утвердження національної ідентичності;

5) налагодження ефективної, системної та систематичної внутрішньодержавної взаємодії та міжнародної співпраці з питань інформації та інформаційної безпеки;

6) інноваційний. Даний аспект державної політики передбачає який передбачає стимулювання інновацій та забезпечення всебічного розвитку й захисту національної інформаційної інфраструктури, зокрема її телекомунікаційної складової, як сукупності різноманітних інформаційних (автоматизованих) систем, інформаційних ресурсів, телекомунікаційних (електронних комунікаційних) мереж, засобів комунікацій і управління інформаційними потоками, а також організаційно-технічних структур, механізмів, що забезпечують їх функціонування [117].

Так на нашу думку виглядають основні напрямки розвитку державної політики у сфері забезпечення реалізації інформаційної безпеки України. Наведений перелік звісно ж не є виключним і цілком може бути доповнений іншими напрямками розвитку зазначеної політики, втім переконані, що ті, які були нами запропоновані вище, мають доволі актуальний характер і цілком узгоджуються із цілями та завданнями чинної Стратегії інформаційної безпеки [14].

1.3. Сучасний стан правового регулювання забезпечення реалізації інформаційної безпеки України.

Ефективне забезпечення інформаційної безпеки вимагає запровадження складного механізму, однією із основоположних ланок якого є нормативно-правове підґрунтя. Досліджуючи етапи становлення інформаційної безпеки України ми відмічали, що правова основа цієї безпеки протягом років

незалежності розвивалася нерівномірно і суттєві зрушення та зміни на цьому шляху відбувалися, як правило, під впливом або навіть прямим тиском зовнішніх факторів, тому не дивно що саме після початку російської агресії по відношенню до України, нормативно-правові засади інформаційної безпеки України зазнали суттєвого перегляду і відповідної трансформації. Однак це не означає, що існуючий на сьогодні механізм правового регулювання інформаційної безпеки України позбавлений недоліків, на яких акцентують увагу дослідники. Так, для прикладу, Р.А. Калюжний та О.О. Баєв у своїх наукових роздумах з приводу інформаційної безпеки зазначають, що стан нормативно-правового забезпечення інформаційної безпеки України визначається ступенем урегульованості національним законодавством, нормами міжнародного права, міжнародними угодами України суспільних відносин у галузі протидії загрозам її національним інтересам в інформаційній сфері. У цілому, нормативно-правове 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 безпеки України [41, с.5]. Правники переконані, що удосконалення нормативно-правової бази забезпечення інформаційного суспільства в Україні дозволить врегулювати нормативні аспекти діяльності щодо впровадження та використання інформаційних технологій продукування та розповсюдження електронної інформації, створення та використання національних інформаційних ресурсів та радіочастотного ресурсу, розвитку телекомунікацій, створення системи стандартизації у сфері інформатизації, забезпечення інформаційної безпеки тощо [41, с.10-11]. Однією з основних перешкод на шляху побудови інформаційного суспільства в Україні, зауважують Р. А. Калюжний та О. О. Баєв, є неузгодженість норм національного законодавства між собою, а також з нормами міжнародного права у цій сфері. Потребує впорядкованості понятійний апарат та

термінологія нормативно-правової бази забезпечення розвитку інформаційного суспільства в Україні. Необхідно нормативно встановити такий порядок підготовки законів і підзаконних актів щодо сфери інформатизації, який забезпечить попередній аналіз проектів законів та підзаконних актів експертами трьох секторів (громадського, приватного і державного). Відсутність такої процедури призводить до того, що більшість законів, які формують теоретичну основу галузі, не узгоджуються один з одним і тому виникають проблеми в їх практичному застосуванні [41, с.10-11]. О. В. Левченко вважає, що в умовах швидкого формування і розвитку інформаційного суспільства в Україні та глобального інформаційного простору, широкого використання інформаційно-комунікаційних технологій у всіх сферах життя особливого значення набувають проблеми інформаційної безпеки [62]. На цей час в Україні, наголошує О. В. Левченко, існує ціла низка таких проблем у сфері інформаційно-психологічної безпеки, що мають загальносистемний характер. Зазначена складна ситуація, на думку дослідника, стала можливою, насамперед, через відсутність узгодженої, послідовної та зваженої державної політики у сфері інформаційної безпеки України, низьку ефективність системи державного регулювання національним інформаційним простором, а також недосконаліть та фрагментарність вітчизняного нормативно-правового поля у сфері інформаційної безпеки [62]. О. В. Левченко цілком слушно відмічає, що існуючі виклики у сфері інформаційної безпеки зумовлюють необхідність подальшого комплексного вирішення всього спектра проблем в інформаційній сфері та ліквідації відставання у розвитку інформаційного законодавства з метою створення належних умов для організації заходів протидії інформаційно-психологічному впливу та забезпеченню інформаційної безпеки нашої держави. Зазначене набуває особливої актуальності в умовах недосконалості нормативно-правових засад забезпечення інформаційної безпеки [62].

О.М. Капля, аналізуючи питання правового регулювання інформаційної безпеки громадянина в умовах воєнного стану, відмічає, що у такий період захист суспільства від деструктивного інформаційного впливу з боку держави агресора та ряду терористичних організацій, які задіяні в процесі дестабілізації нашої країни, а також від інших негативних інформаційних факторів, які руйнують вітчизняний інформаційний простір, необхідно уточнити форми та методи забезпечення інформаційної безпеки громадян. Протистояння новим загрозам в інформаційній сфері, зазначає О.М. Капля, потребує нових шляхів вирішення, які пов'язані із розробкою потрібних організаційних, правових, а також технологічних засобів аналізу, пошуку, поширення, зберігання та використання інформації у всіх сферах життєдіяльності суспільства. Такі заходи, підкреслює правознавець, мають бути регламентовані та контролюватись на законодавчому рівні. Негативні явища інформаційного характеру у воєнний час, можна вважати такими, що ставлять під загрозу основні принци забезпечення безпеки громадян, в основі яких лежать чинні принципи та норми права на міжнародному рівні. Тому, основним завданням державної політики, підкреслює науковець, пов'язаної із забезпеченням безпеки в інформаційній сфері є створення умов для надання кожному громадянину права на інформаційну безпеку [42, с.17]. О. М. Капля справедливо звертає увагу на те, що інформаційна безпека громадянин закріплена в низці нормативних документів та є конституційною нормою. Проте, це поняття не достатньо деталізовано та законодавчо врегульовано та потребує його виокремлення із таких категорій, як інформаційна безпека держави, інформаційна безпека суспільства, національна безпека. Для вирішення цієї проблеми потрібні зміни в деяких законодавчих актах, з метою забезпечення ефективної реалізації конституційних засад інформаційної безпеки держави, суспільства та громадянина, як окремих категорій. Стан інформаційної безпеки громадянина у воєнний час, суттєво відрізняється від мирного часу, оскільки пріоритети в протидії загроз більше

спрямовані до захисту саме держави, її територіальної цілісності та незалежності в цей період [42, с.19-20].

О. М. Ситніченко наголошує, що нині однією із серйозних проблем діяльності органів публічної адміністрації у сфері забезпечення інформаційної безпеки є, перш за все, невизначеність та незбалансованість окремих складових частин правового регулювання [141, с.86]. При цьому дослідниця зауважує, що нині в Україні вдалося досягти значних успіхів щодо нормативно-правового регулювання забезпечення інформаційної безпеки. Це насамперед зумовлено тим, що забезпечення інформаційної безпеки стало одним із пріоритетних напрямів діяльності органів публічної адміністрації, адже сучасне інформаційне середовище активно впливає на стан політичної, економічної, військової та інших складових частин національної безпеки України. Аналіз нормативно-правового забезпечення свідчить, що сучасна інформаційна безпека є самостійною сферою національної безпеки, в якій необхідно забезпечити захист інформаційних ресурсів, систем їх формування, поширення і використання, інформаційної інфраструктури, захист таємної та службової інформації, інформації про особу [141, с.89].. Правове регулювання діяльності органів публічної адміністрації щодо забезпечення інформаційної безпеки, на думку О.М. Ситніченко, має цілісний характер, тобто ця діяльність регулюється як законами, так і указами, постановами, розпорядженнями, наказами – понад 70 нормативними актами. Проте, наголошує вона, незважаючи на позитивні моменти, проаналізовані нормативно-правові акти мають ряд недоліків. По-перше, встановлено, що різні нормативно-правові акти, норми яких регулюють суспільні відносини, об’єктом яких є інформаційна безпека, приймалися в різний час без узгодження понятійного апарату, вони мають низку не досить коректних термінів або взагалі не мають чіткого визначення змісту; по-друге, нині існує низка нормативно-правових актів, що регулюють таку діяльність. Така кількість чинних нормативно-правових актів призводить до труднощів у застосуванні поданих норм; по-третє, нечітке нормативно-

правове регулювання діяльності органів публічного адміністрування значно знижує їх готовність до реалізації закріплених повноважень [141, с.89]. Отже, підсумовує О. М. Ситніченко, з метою вдосконалення нормативно-правового регулювання забезпечення інформаційної безпеки пропонуємо провести відповідну роботу щодо систематизації та скасування «формально чинних» норм [141, с.89]. М.В. Сунгуровський, досліджуючи проблемні питання забезпечення ефективної інформаційної безпеки, доходить цілком справедливого висновку, що нормативно-правове забезпечення для цієї мети є надзвичайно важливим етапом на рівні із фінансовим, технічним, кадровим, забезпечення процесів створення та функціонування системи захисту [150, с.14]. Д.В. Дубов у своїх працях стверджує, що захист українського інформаційного простору від деструктивної інформаційної ворожої діяльності залишається актуальним завданням, яке стоїть перед органами державної влади та сектором безпеки зокрема. Заходи протидії, які були вжиті Україною (в частині припинення трансляції російських телеканалів, мовного квотування, функціонування російських соціальних мереж тощо) вирішили лише частину питань в цій сфері. Істотною проблемою, що залишилась на порядку денному, є комплексна протидія деструктивній інформаційній діяльності, що здійснюється або за допомогою внутрішніх суб'єктів інформаційної діяльності, або через канали інформування, власники яких безпосередньо не є суб'єктами (резидентами) України, але при цьому здійснюють тут свою діяльність (іноземні соціальні сервіси). Хоча органи державної влади, зокрема контррозвідувальні та правоохоронні органи, здійснюють заходи з протидії ворожій інформаційній діяльності в межах своїх повноважень, але в багатьох випадках їх дії виявляються обмеженими через низку чинників. Одна з важливих причин браку ефективності, на думку Д.В. Дубова, – це недосконалість нормативно-правової бази, яка б регламентувала протидію інформаційній підривній діяльності проти української державності [32, с.14-15]. М. В. Баран, розглядаючи питання принципів правового регулювання інформаційної

безпеки, наголошує, що розвиток інформаційного суспільства, цифрової трансформації технологій перед вченими-правознавцями ставить завдання, які стосуються пошуку можливостей правового регулювання таких явищ, як робототехніка, штучний інтелект, Інтернету речей, розвиток інформаційно-освітніх платформ. Існуюче нормативно-правове регулювання, підкреслює М. В. Баран, не стоїть на місці, у ньому знаходить відображення розвиток теоретичних уявлень про систему правового забезпечення інформаційної безпеки в Україні. Сьогодні виникають нові суспільні відносини, пов'язані із забезпеченням критичної інформаційної інфраструктури, вносяться зміни до інформаційного, в інше галузеве законодавство. Аналогічна ситуація склалася у сфері захисту персональних даних громадян, на яку вплив робить прийняття міжнародних правових актів [10, с.130]. Важливе місце у правовому забезпеченні інформаційної безпеки відіграють принципи. М.В. Баран звертає увагу на необхідність удосконалення правового регулювання інформаційної безпеки, зокрема пропонується закріпити в інформаційному законодавстві принцип презумпції безпеки об'єктів критичної інформаційної інфраструктури, який встановлює, що об'єкти критичної інформаційної інфраструктури вважаються захищеними, поки організаційно-правове забезпечення безпеки зазначених об'єктів відповідає вимогам, закріпленим в нормативно-правових актах у сфері забезпечення інформаційної безпеки. Широкий спектр проблем забезпечення інформаційної безпеки особи, суспільства та держави, розвитку культури кібербезпеки, забезпечення недоторканності приватного життя та захисту прав на доступ до інформації, захисту інформаційних систем, ресурсів і мереж, розширення застосування інформаційних технологій в публічному управлінні, при наданні адміністративних послуг, інші проблеми інформаційної безпеки потребують ретельного вивчення. Відповідно, перспективним завданням юридичної науки є вироблення пропозицій задля удосконалення відповідних актів законодавства [10, с.130].

Підтримуючи позиції дослідників щодо важливості запровадження

більш якісного підходу до формування нормативно-правового підґрунтя інформаційної безпеки, розглянемо детальніше стан правового регулювання забезпечення реалізації інформаційної безпеки України. Базовим нормативно-правовим актом і сфері інформації та інформаційної діяльності є Закон України «Про інформацію», в якій протягом його існування було внесена ціла низка правок, а у 2011 році парламент України прийняв повністю нову редакцію цього закону, яка діє і на сьогодні. Цей Закон регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації [101]. Оскільки вказаний закон не орієнтований спеціально на питання інформаційної безпеки, то в ньому не багато положень, які стосуються досліджуваної проблематики. Тим не менш, у цьому законі прямо передбачено, що інформаційна безпека є одним із основних напрямків державної політики в інформаційній сфері [101]. Також у ньому викладене визначення захисту інформації, під яким розуміється сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї. До ключових принципів інформаційних відносин, згідно вказаного закону належать такі: гарантованість права на інформацію; відкритість, доступність інформації, свобода обміну інформацією; достовірність і повнота інформації; свобода вираження поглядів і переконань; правомірність одержання, використання, поширення, зберігання та захисту інформації; захищеність особи від втручання в її особисте та сімейне життя [101]. Із переліку принципів видно, що свобода і взаємна повага (до прав, поглядів, інтересів один одного) є одними із ключових пріоритетів інформаційних відносин в Україні. Разом із тим, у цьому ж законі передбачені деякі ситуації, за яких можливі певні відступи від вище наведених принципів і пріоритетів. Так, у законі «Про інформацію», встановлено, що будь-які обмеження чи інші дії у інформаційній сфері, які мають чи можуть мати негативний характер для осіб, допускаються виключно у порядку, межах та на підставах визначених Законом та в інтересах національної безпеки,

територіальної цілісності або громадського порядку, з метою запобігання заворушенням чи кримінальним правопорушенням, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя, в інтересах економічного добробуту та захисту прав людини [101].

Інші нормативно-правові акти у сфері інформації та інформаційної діяльності мають більш спеціальний характер на відміну від закону «Про інформацію», оскільки орієнтовані на врегулювання окремих питань функціонування інформаційних відносин і здійснення інформаційної діяльності. Так, в першу чергу слід відмітити Закони України «Про державну таємницю» та «Про захист персональних даних». Перший нормативно-правовий акт орієнтований на регулювання суспільних відносин, пов'язаних з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України. Під державною таємницею (або секретною інформацією) у цьому законі розуміється вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою [87]. Даний закон розвиває та конкретизує положення та ідеї вище згаданого закону «Про інформацію» в частині того, що певні дані (відомості), в силу специфіки їх змісту мають особливе значення для держави та суспільства, а тому їх довільне отримання, розповсюдження, використання може призвести до негативних наслідків для національних інтересів, створити нові чи посилити вже існуючі загрози для них. Саме тому така інформація має особливий режим доступу і використання. О. Г. Семенюк з цього приводу пише, що сучасні суспільно-політичні умови висувають на перший план тезу про первинність та

природність інформаційної свободи як нормального стану суспільства. З кожним роком, наголошує правник, набирає своїх обертів науковий дискурс щодо шляхів вдосконалення законодавства, яке забезпечує реалізацію права громадян на доступ до інформації, у зв'язку з чим до цієї проблеми долучається дедалі більша кількість учених та експертів, які висловлюють, з одного боку, різні міркування стосовно шляхів подальшого розвитку інформаційних відносин, з іншого – запровадження нових механізмів обмеження права на доступ до державної таємниці у суспільних інтересах [140, с.35]. О. Г. Семенюк підкреслює, що існування законодавчих дефініцій має сприятливий вплив на правозастосовну діяльність у багатьох відношеннях лише за умови адекватності правової дійсності, що ними відображена, тому науковець пропонує власне бачення дефініції поняття державна таємниця, під яким, на його думку слід розуміти сукупність відомостей, засекречування яких продиктоване суспільною необхідністю безпечних умов існування особи, суспільства та держави; коло цих відомостей визначається правовими актами і змінюється в залежності від конкретної зовнішньополітичної та внутрішньополітичної ситуації [140, с.42-43]. Дослідник зауважує на тому, що в умовах демократії свобода інформації повинна бути нормою, проте, державні інтереси, а також інтереси суспільства й окремої особи потребують захисту, вимагають від держави накладати певні обмеження на свободу інформації. Іншими словами, у стратегічних інтересах безпеки особи, суспільства та держави необхідно створити не тільки розвинуту інформаційну сферу, але й вирішити питання її захисту. Адже саме через інформаційну сферу в основному реалізуються наміри щодо завдання шкоди безпеці України в різноманітних сферах її діяльності. У контексті державної інформаційної політики мова повинна йти не тільки про права громадян, юридичних осіб і держави на вільне одержання, поширення і використання інформації, але і про необхідність захисту та раціональне використання державних інформаційних ресурсів, захист конфіденціальної інформації та інтелектуальної власності [140, с.42-43]. Що стосується закону

«Про захист персональних даних», то він орієнтований перш за все на захист прав і свобод людини та громадянина у інформаційній сфері, а саме тих відомостей про фізичну особу, які становлять її персональні дані. Персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [99]. Однак, визначаючи підстави і порядок обробки персональних даних, а також гарантії їх захисту, закон разом із тим передбачає випадки, коли зазначені гарантії захисту персональних не діють, або діють обмежено. Такими випадками є ті, що стосуються питань національної безпеки, загального добробуту.

Важливим з точки зору забезпечення нормативно-правової основи інформаційної безпеки України є закон «Про доступ до публічної інформації» від 13.01.2011 р. № 2939-VI, який визначає порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом, та інформації, що становить суспільний інтерес [88]. Метою цього закону є забезпечення прозорості та відкритості суб'єктів владних повноважень і створення механізмів реалізації права кожного на доступ до публічної інформації [88]. У ньому закріплені: гарантії та принципи доступу до публічної інформації; основні процедурні аспекти реалізації права на такий доступ; суб’єктний склад відносин, що регулюються зазначеним законом, а також форми реалізації доступу. У законі прямо закріплені випадки, коли доступ до певної публічної інформації може бути обмежений, зокрема у статті 6 закону «Про доступ до публічної інформації» встановлено, що обмеження доступу до інформації здійснюється відповідно до закону при дотриманні сукупності таких вимог: 1) виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи кримінальним правопорушенням, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості

правосуддя; 2) розголошення інформації може завдати істотної шкоди цим інтересам; 3) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні[88].

Важливими законодавчими актами з питань інформації та інформаційної діяльності, які також стосуються інформаційної безпеки є: Закони України «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-комунікаційних системах» та «Про електронні комунікації», «Про медіа». Перший нормативно-правовий акт (тобто закон «Про основні засади забезпечення кібербезпеки України») визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [111]. Прийняття цього закону стало важливим кроком на шляху забезпечення інформаційної безпеки України, адже ми живемо в епоху інформаційного суспільства, коли інформаційні технології та телекомунікаційні системи охоплюють усі сфери життєдіяльності людини, держави. Сьогодні ми все більше й більше використовуємо їх у своїй діяльності. Але взявши на службу телекомунікації і глобальні комп'ютерні мережі, слід знати й розуміти, які можливості для зловживання створюють ці технології. Сьогодні жертвами хакерів можуть стати не лише люди, але й цілі держави [45]. Експерти в сфері кібербезпеки більшості провідних країн світу відзначають стійку тенденцію до значного зростання кількості та розширення спектру кібератак з метою порушення конфіденційності, цілісності та доступності державних інформаційних ресурсів, в тому числі на об'єктах критичної інформаційної інфраструктури [26]. За ефективністю та наслідками застосування кіберзброю, а саме такий термін все частіше використовують вчені, можна прирівняти до зброї масового ураження. Тому,

наголошують фахівці, кібербезпека – одна з основних проблем, що викликає занепокоєння. І чим швидше людство розвиває інформаційні технології, тим більшою є потреба в захисті інформаційно-телекомунікаційних систем. Оскільки критичні вразливості в програмному забезпеченні та автоматизованих системах викликають небезпідставні побоювання, то не дивно, що уряди та суспільство в усьому світі шукають кращих заходів і методів для захисту особистих даних Інтернет-ресурсів від кіберзагроз [45]. Звісно закон «Про основні засади забезпечення кібербезпеки України» не вирішує усіх актуальних питань забезпечення безпеки кібернетичного простору, однак він: по-перше, містить визначення ключових понятійно-термінологічних конструкцій (кібербезпека, кібератака, кіберпростір, кіберзахист, кібероборона, кіберзагроза, кібертероризм тощо) пов'язаних із кібербезпекою, що є дуже важливим для чіткого визначення сутності та змісту тих явищ, з якими працює держава у межах відповідної своєї безпекової політики. Так, наприклад, у цьому законі закріплено, що кіберпростір – це середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних; кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі; кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів; кіберзахист - сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту

інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем; кібероборона – сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії [111]; по-друге, в законі «Про основні засади забезпечення кібербезпеки України» нормотворець визначив ключові засадничі аспекти забезпечення кібербезпеки як то: її принципи, суб'єктно-об'єктний склад, основи взаємодії та контролю з питань кібербезпеки. Слід відмітити, що деякі фахівці досить скептично ставляться до практичної цінності зазначеного закону, через його загальність, правники підкреслюють, що за своїм змістом він більше нагадує загальну стратегію державної політики у сфері кібербезпеки, аніж нормативно-правовий акт, спрямований на врегулювання конкретних відносин В. Гудима з цього приводу зазначає, що досліджуваний закон є головним чином рамковим документом, він юридично визначає ключові поняття у сфері кібербезпеки і робить спробу, відверто кажучи, невдалу, розподілити сфери відповідальності державних органів у сфері захисту інформації. Частина закону просто переказує ключові положення Стратегії кібербезпеки і не містить чогось нового. Тому якихось швидких чи суттєвих змін від цього закону очікувати не варто [26]. Д. Снопченко також наголошує на тому, що означений закон досить узагальнений і до якихось безпосередніх дій не приведе. Однак, справедливо відмічає фахівець, цей закон має стати основою для прийняття наступних спеціальних законів та підзаконних актів з цього приводу. Крім того, підкреслює Д. Снопченко, важливими позитивними моментами цього вище згаданого закону є те, що: кіберзахисту залучили міністерство оборони, крім ДСТСЗІ і СБУ, які займалися цим раніше; передбачено відповідальність не тільки за кіберзлочини, а й за неякісний захист власників інформації цієї

самої інформації, яку вони зобов'язані будуть захищати. В основному це буде стосуватися держорганів, і сподіваюся, що вони будуть з більшою увагою ставитися до кіберзахисту і не тримати свої поштові скриньки на російських серверах – як мінімум; гадано в законі про освіту не тільки в вишах для фахівців, а й для суспільства, для підняття загальної освіченості населення в питаннях кіберзахисту, тому прості користувачі теж стануть більш захищеними. Загалом, підсумовує фахівець з інформаційної безпеки, закон можна вважати першим заставним каменем в загальній політиці України в напрямку кібербезпеки. Подальший її розвиток залежить тільки від кропіткої роботи фахівців, які впроваджують системи на місцях [26].

Наступний нормативно-правовий акт вищої юридичної сили, який слід відмітити у контексті досліджуваної проблематики є закон «Про захист інформації в інформаційно-комунікаційних системах», від 05.07.1994 р.№ 80/94-ВР, який регулює відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах [98]. Об'єктами захисту в зазначеній системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації [98]. Цей закон, а також вище згаданий закон з питань кібербезпеки логічно доповнює Закон України «Про електронні комунікації» від 16.12.2020 № 1089-IX визначає правові та організаційні основи державної політики у сферах електронних комунікацій та радіочастотного спектра, а також права, обов’язки та відповідальність фізичних і юридичних осіб, які беруть участь у відповідній діяльності або користуються електронними комунікаційними послугами [90]. Значна увага у цьому нормативно-правовому акті відведена питанням безпеки електронних комунікацій, яка визначена як 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 [90]. Очевидно, що забезпечення безпеки електронних комунікацій прямо пов’язане з інформаційною безпекою, оскільки електронна комунікація (телекомунікація, електрозв’язок) – це передавання та/або приймання інформації незалежно від її типу або виду у вигляді електромагнітних сигналів за допомогою технічних засобів електронних комунікацій [90]. Характеризуючи важливість законодавства з питань електронної комунікації та його значення для забезпечення інформаційної безпеки, слід відмітити думку М. В. Гайворонського, який відмічає, що можна було б припустити, що питання захисту цифрової інформації можна вирішувати тими самими методами, що застосовували для захисту традиційних (паперових) носіїв інформації. Певного мірою це дійсно так [25, с.18]. Але, наголошує дослідник, є й інший бік проблеми. Комп’ютерна технологія оброблення інформації несе в собі певні загрози, які можуть призвести до небажаних втрат або тимчасової недоступності важливих даних. Зрештою, будь-яка нова технологія приховує небезпеку, яка не завжди очевидна. У контексті інформаційно-комунікаційних систем слід згадати системи зберігання даних, надійність яких власники інформації інколи переоцінюють. Але є й менш очевидні проблеми. Зокрема, це можливість (на жаль, реалізована на практиці) існування шкідливого і навіть руйнівного програмного забезпечення. Передумовою його існування є унеможливлення або суттєве ускладнення перевірки всіх функцій програмного забезпечення. Це означає, що програми можуть містити так звані недокументовані функції — приховані функції, реалізовані програмістами та навмисно або через їхню недбалість долучені до програмного продукту і не описані в документації. Такі функції можуть бути активізовані випадково (за збігу обставин, внаслідок помилок чи збоїв) або навмисно (за певних умов). Одним із найпоширеніших і найнебезпечніших різновидів шкідливого програмного забезпечення є комп’ютерні віруси, здатні розмножуватись і розповсюджуватись [25, с.18 - 19]. З усього цього, підсумовує М. В. Гайворонський, що без застосування спеціальних заходів захисту існує дуже висока ймовірність пошкодження

інформації в інформаційно-комунікаційній системі, що може завдати збитків її власнику. Отже, задачі захисту інформації в інформаційно-комунікаційній системі є суперпозицією задач двох головних напрямів: захист важливої інформації, зокрема державної, військової або комерційної таємниці, від цілеспрямованих дій порушників; захист інформації від впливів, спричинених некоректним функціонуванням комп'ютерної системи через відмови обладнання, збої програмного забезпечення, помилки в реалізації апаратних або програмних засобів, або наявність програмних засобів з прихованими руйнуючими властивостями [25, с.19]. Важливо відмітити, що закон покладає відповідальність на забезпечення інформаційної безпеки не лише на постачальників електронних послуг, але й на споживачів (в тому числі кінцевих) цих послуг.

Що стосується Закону України «Про медіа», то цей Закон спрямований на забезпечення реалізації права на свободу вираження поглядів, права на отримання різнобічної, достовірної та оперативної інформації, на забезпечення плюралізму думок і вільного поширення інформації, на захист національних інтересів України та прав користувачів медіа-сервісів, регулювання діяльності у сфері медіа відповідно до принципів прозорості, справедливості та неупередженості, стимулювання конкурентного середовища, рівноправності і незалежності медіа та визначає правовий статус, порядок формування, діяльності та повноваження Національної ради України з питань телебачення і радіомовлення (Національна рада) [104]. Даний закон замінив цілий ряд вже застарілих законів, які регламентували діяльність засобів масової інформації в Україні. Є . Кравчук, обґрунтовуючи важливість і значення закону «Про медіа», відмічає, що чинні до цього моменту (тобто до прийняття закону «Про медіа») закони з питань діяльності ЗМІ суттєво застарілі та не враховували реалії сьогодення, зокрема те, що інформаційний простір суттєво розширився та набув нових форм, перш за все йдеться про всесвітню електронну мережу Інтернет [138]. Закон «Про медіа» містить цілу низку нововведень і удосконалень, однак ми звернемо увагу

лише на ті, що стосуються його безпекової частини. Перш за все слід відзначити що у зазначеному законі прямо закріплено, що одним із ключових принципів організації та функціонування сфери медіа в Україні є свобода, яка можу бути обмежена тільки за виключних обставин, зокрема в інтересах національної безпеки. Так, у статі 4 закону «Про медіа» встановлено, що діяльність у сфері медіа ґрунтується на принципах свободи вираження поглядів і переконань, свободи поширення, обміну та отримання інформації, свободи діяльності суб'єктів у сфері медіа, у тому числі вільного визначення змісту інформації, свободи господарської діяльності у сфері медіа, гарантованості права на інформацію, відкритості та доступності інформації, достовірності і повноти інформації, правомірності одержання, використання, поширення, зберігання та захисту інформації, захищеності особи від втручання в її особисте та сімейне життя. Будь-які обмеження зазначених свобод, у тому числі при прийнятті державними органами, органами місцевого самоврядування рішень, які забороняють або обмежують розповсюдження будь-якого медіа на території України, рішень про зупинення, анулювання або відмову у видачі ліцензій, про відмову у реєстрації суб'єкта у сфері медіа, можуть бути встановлені та застосовані лише на підставі закону, якщо це є необхідним у демократичному суспільстві, а відповідне обмеження є пропорційним (ненадмірним) щодо поставленої мети. Обмеження зазначених свобод може здійснюватися лише в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя. При впровадженні обмежень у сфері медіа державні органи, органи місцевого самоврядування, їх посадові особи застосовують практику Європейського суду з прав людини як джерело права [104]. Більш конкретно випадки обмеження щодо змісту інформації передбачені у статті 36 закону, зокрема на території України в медіа та на

платформах спільного доступу до відео забороняється поширювати: заклики до насильницької зміни, повалення конституційного ладу, розв'язування або ведення агресивної війни або воєнного конфлікту, порушення територіальної цілісності України, ліквідації незалежності України, інформацію, яка виправдовує чи пропагує такі дії; висловлювання, що розпалюють ненависть, ворожнечу чи жорстокість до окремих осіб чи груп осіб за ознакою етнічного чи соціального походження, громадянства, національності, раси, релігії та вірувань, віку, статі, сексуальної орієнтації, ґендерної ідентичності, інвалідності; висловлювання, що підбурюють до дискримінації чи утисків стосовно окремих осіб чи груп осіб за ознакою етнічного чи соціального походження, громадянства, національності, раси, релігії та вірувань, віку, статі, сексуальної орієнтації, ґендерної ідентичності, інвалідності або за іншими ознаками; 4) пропаганду або заклики до тероризму та терористичних актів, інформацію, що виправдовує чи схвалює такі дії; інформацію, що заперечує або виправдовує злочинний характер комуністичного тоталітарного режиму 1917-1991 років в Україні, злочинний характер націонал-соціалістичного (нацистського) тоталітарного режиму, створює позитивний образ осіб, які обіймали керівні посади у комуністичній партії (посаду секретаря районного комітету і вище), вищих органах влади та управління СРСР, УРСР (УСРР), інших союзних та автономних радянських республік (крім випадків, пов'язаних з розвитком української науки та культури), працівників радянських органів державної безпеки, виправдовує діяльність радянських органів державної безпеки, встановлення радянської влади на території України або в окремих адміністративно-територіальних одиницях, переслідування учасників боротьби за незалежність України у XX столітті. Особливості розповсюдження і демонстрування фільмів, що містять популяризацію радянських органів державної безпеки, регулюються Законом України "Про кінематографію та ін. [104]. Окремо слід відмітити розділ VIII закону «Про медіа», який присвячений питанням контролю та нагляду, а також відповідальності за порушення у сфері медіа. Важливо, що у цьому

підрозділі викладені не лише випадки дій (бездіяльності), які вважаються правопорушеннями, а також стягнення, які накладаються на суб'єкта за вчинення цих правопорушень, але й ряд інших важливих положень, що становлять нормативно-правову основу забезпечення режиму законності у сфері медіа, зокрема статтями зазначеного підрозділу врегульовано наступне: принципи здійснення нагляду та контролю за дотриманням законодавства у сфері медіа; суб'єкти цього контролю та нагляду; перелік і зміст, а також порядок застосування заходів реагування (окрім стягнень) тощо.

Окремо слід відмітити Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23.06.2006 р. № 3475-IV, який визначає організаційно-правові засади діяльності Державної служби спеціального зв'язку та захисту інформації України, яка є державним органом, що призначений для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, активної протидії агресії у кіберпросторі, а також інших завдань відповідно до закону [86]. У даному підрозділі ми не будемо детально розглядати правовий статус та діяльність даного суб'єкта, оскільки системі суб'єктів забезпечення реалізації інформаційної безпеки України присвячений окремий підрозділ представленого дослідження, втім відмітимо, що саме цей суб'єкт, згідно законодавства виконує цілу низку важливих завдань у сфері забезпечення інформаційної безпеки, наприклад, забезпечення впровадження системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлення вимог до аудиторів інформаційної безпеки, їх атестації (переатестації) [86]. Означена служба належить до категорії ключових суб'єктів забезпечення національної безпеки України. Разом із тим слід відмітити, що ця державна структура зараз перебуває на етапі реформування з метою її приведення у відповідність до потреб і реалій

сьогодення, а також до провідних міжнародних стандартів. У Концепції реформування Державної служби спеціального зв'язку та захисту інформації України, затвердженій Указом Президента України від 22.10.2021 р. № 544/202 зазначать, що метою цієї Концепції є реформування та розвиток Державної служби спеціального зв'язку та захисту інформації України як суб'єкта сектору безпеки і оборони із запровадженням уніфікованої системи планування та управління ресурсами на основі сучасних європейських та євроатлантичних підходів, що дасть змогу підвищити інституційну спроможність, а також оптимізувати організаційну структуру Державної служби спеціального зв'язку та захисту інформації України. Основним завданням Концепції є підвищення інституційної спроможності Державної служби спеціального зв'язку та захисту інформації України та подальший її розвиток як складової національної системи кібербезпеки держави та суб'єкта сектору безпеки і оборони з урахуванням: поточного стану та тенденцій розвитку безпекової ситуації навколо України; стратегічних та концептуальних документів з питань розвитку сектору безпеки і оборони; міжнародних стандартів у сфері спеціального зв'язку та захисту інформації [119]. При цьому у Концепції відмічається, що одним із важливих питань, які слід вирішити в ході зазначеної реформи, є удосконалення нормативно-правових та організаційно-управлінських засад діяльності Державної служби спеціального зв’язку та захисту інформації України.

Окрім вище наведених законів, які є спеціальними, тобто прямо орієнтованими на врегулювання відносин у сфері інформації та інформаційної діяльності, у контексті досліджуваної тематики слід також відмітити й деякі інші Закони України, які й тій чи іншій мірі стосуються забезпечення інформаційної безпеки, а саме: по-перше, закон «Про національну безпеку України» від 21.06.2018 р. № 2469-VIII, який визначає основи та принципи національної безпеки і оборони, цілі та основні засади державної політики, що гарантуватимуть суспільству і кожному громадянину захист від загроз. Цим Законом визначаються та розмежовуються

повноваження державних органів у сферах національної безпеки і оборони, створюється основа для інтеграції політики та процедур органів державної влади, інших державних органів, функції яких стосуються національної безпеки і оборони, сил безпеки і сил оборони, визначається система командування, контролю та координації операцій сил безпеки і сил оборони, запроваджується всеосяжний підхід до планування у сферах національної безпеки і оборони, забезпечуючи у такий спосіб демократичний цивільний контроль над органами та формуваннями сектору безпеки і оборони [108]. Значення цього закону у контексті досліджуваної проблематики полягає перш за все у тому, що у ньому прямо проголошено інформаційну безпеку як одну із основних складових національної безпеки, а також у загальному вигляді окреслено коло суб'єктів, які опікуються питаннями інформаційної безпеки; по-друге, закони, які регламентують правовий статус та організаційно-правові аспекти діяльності окремих органів публічної влади (окрім вже вищезгаданої Державної служби спеціального зв'язку та захисту інформації України), як то: Кабінет Міністрів України, Національна поліція України, Служба безпеки України, місцеві державні адміністрації, органи місцевого самоврядування та ін.. Більш детально роль суб'єктів загально, галузевої та спеціальної компетенції у питанні забезпечення інформаційної безпеки України ми розглянемо у окремому підрозділі, присвяченому система суб'єктів забезпечення реалізації інформаційної безпеки України.

Отже, з огляду на вище викладене, можемо констатувати, що сьогодні в Україні діє ціла низка нормативно-правових актів вищої юридичної сили, тобто Законів, які спрямовані на врегулювання відносин у сфері інформації та інформаційної діяльності. Можна з упевненістю говорити про те, що наразі законодавчим регулюванням охоплено більшість аспектів організації та функціонування інформаційної галузі в нашій державі, при цьому значна увага відведена саме забезпеченню інформаційної безпеки України. Однак, при цьому ми не можна не відмітити тієї обставини, що жоден із вище значених нормативно-правових актів не є комплексним документом з питань

реалізації державної політики саме у сфері інформаційної безпеки України. Кожен із вище згаданих законів регулюючи певні відносини у інформаційній сфері, питань інформаційної безпеки стосується лише у тій мірі, наскільки це необхідно для мети саме цього закону і предмету його регулювання. Натомість спеціального закону з питань інформаційної безпеки в нашій державі наразі немає. Переконані, що прийняття такого нормативно-правового акту є необхідним кроком, який забезпечить:

- по-перше, консолідацію усієї сукупності нормативно-правових актів з питань інформаційної безпеки у єдину структуровану систему із чітко визначеною ієрархією;

- по-друге, закріплення у системному вигляді на вищому юридичному рівні ключових засад реалізації інформаційної безпеки України, зокрема таких як: визначення основних термінів, принципи, гарантії, напрямки і форми, суб'єктне коло. Тобто цей закон має визначити цілісну та послідовну систему параметрів реалізації єдиної державної політики у сфері інформаційної безпеки.

Окрім Законів, значну частину нормативно-правового підґрунтя реалізації інформаційної безпеки України складають підзаконні нормативно-правові акти, які умовно можемо розподілити на декілька груп:

1) концептуальні. До цієї категорії підзаконних нормативно-правових актів належать ті, в яких викладені концептуальні та стратегічні засади державної політики у щодо забезпечення інформаційної безпеки, програмні цілі та завдання з її реалізації. Одним із ключових актів цієї групи на сьогодні є Стратегія Інформаційної безпеки, затверджена і введена в дію Указом Президента України від 28.12.2021 р. № 685/2021 [117]. У цьому правовому документі владою викладене офіційна позиція щодо бачення кола основних проблем і загроз, які стоять сьогодні перед українським суспільством і державою (як на національному, так і глобальному рівні), а також цілі і завдання, напрямки та механізми протидії цим небезпекам і викликам, зміцнення і розвитку механізму інформаційної безпеки в Україні. О.

Ткаченко, акцентуючи увагу на важливості прийняття цієї Стратегії, зазначає, що інформаційна безпека в 21-му сторіччі має надважливе значення. Телебачення, інтернет, соціальні мережі – увесь цей арсенал вже використовується проти України. І вражає мільйони людей. Іноді, навіть, непомітно для них самих. А оскільки соціальні мережі входять в життя наших дітей все раніше і раніше, ми повинні мати інструменти, як не допустити відвертої пропаганди, агресивної риторики, маніпуляції історичними фактами. Стратегія – один з перших кроків на шляху до таких дієвих інструментів [154]. Результатами реалізації державної політики у сфері забезпечення інформаційної безпеки згідно цієї стратегії має бути таке: захищений інформаційний простір України; ефективне функціонування системи стратегічних комунікацій; здійснення ефективної протидії поширенню незаконного контенту; забезпечення сталого процесу інформаційної реінтеграції громадян України, які проживають на тимчасово окупованих територіях України, та поширення українського телерадіомовлення на територіях України, прилеглих до тимчасово окупованих територій; суттєве підвищення рівня медіакультури та медіаграмотності населення; дотримання конституційних прав особи на вільне вираження своїх поглядів і переконань, захист приватного життя; забезпечення захисту прав журналістів; формування української громадянської ідентичності [117]. Окрім цієї стратегії, питань інформаційної безпеки України також стосуються такі стратегічні документи як: 1) Стратегія національної безпеки України від 14.09.2020 р. [115], в якій закріплено, що інформаційна безпека є однією із ключових складових інформаційної безпеки, і що забезпечення першої має бути орієнтоване як на забезпечення стійкості національної інформаційної сфери, так і її активний розвиток через запровадження нових технологій і підвищення інформаційної грамотності населення; 2) Стратегія забезпечення державної безпеки від 16.02.2022 р. № 56/2022, в якій окрім іншого акцентовано увагу на тому, що безпекове середовище в нашій країні потребує посилення протидії деструктивні

пропаганді як ззовні, так і всередині України, як використовуючи суспільні протиріччя, розпалює ворожнечу, провокує конфлікти та підриває суспільну єдність. Відсутність цілісної інформаційної політики держави, недостатня розвиненість національної інформаційної інфраструктури, слабкість системи стратегічних комунікацій ускладнюють нейтралізацію цієї загрози на тлі інформаційної експансії Російської Федерації, зокрема шляхом розширення власної інформаційної інфраструктури та контрольованих нею структур на тимчасово окупованих територіях Автономної Республіки Крим та міста Севастополь, а також в окремих районах Донецької та Луганської областей [124]; 3) Стратегія воєнної безпеки України від 25.03.2021 р. № 121/2021, в якій зазначається, що всеохоплююча оборона України передбачає превентивні дії та здійснення стійкому опору агресору не лише на суші, на морі та в повітряному просторі України, але й у кіберпросторі та передбачає нав’язуванні своєї волі в інформаційному просторі. А тому опанування та активне впровадження сучасних технологій є одним із пріоритетних завдань відповідних суб’єктів, що опікуються питаннями оборони держави [120]; 4) Стратегія кібербезпеки України від 26.08.2021 р. № 447/2021, спрямована на убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства; захист прав, свобод і законних інтересів громадян України у кіберпросторі; європейська і євроатлантична інтеграція у сфері кібербезпеки [116]; 5) Стратегія комунікації з питань євроатлантичної інтеграції України на період до 2025 року від 11.08.2021 р. № 348/2021, метою якої є підвищення рівня поінформованості та розуміння українським суспільством, міжнародною спільнотою змісту і практичної цінності змін в Україні, пов'язаних з реалізацією стратегічного курсу євроатлантичної інтеграції, створення у зв'язку з цим системної інформаційної взаємодії (комунікації) з питань євроатлантичної інтеграції [127]; 6) Стратегія інформаційної реінтеграції Автономної Республіки Крим та м. Севастополя від 27.12.2018 р. № 1100-р, спрямована на забезпечення інформаційної реінтеграції тимчасово окупованої території України (Автономної Республіки

Крим та м. Севастополя), створення інформаційними інструментами передумов для відновлення територіальної цілісності та суверенітету України [130]; 7) Стратегія інформаційної реінтеграції Донецької та Луганської областей від 26.07. 2018 р. № 539-р, цілі реалізації якої полягають у наступному: реалізація інформаційних прав і свобод людини і громадянина, підвищення рівня підтримки громадянами України державної політики у сфері інформаційної реінтеграції тимчасово окупованих територій у Донецькій та Луганській областях; впровадження ефективного механізму для забезпечення доступу громадян України, які проживають на тимчасово окупованих територіях у Донецькій та Луганській областях, а також прилеглих до них територіях, до загальноукраїнського інформаційного простору [127];

2) статусні – це підзаконні нормативно-правові акти, в яких визначається правовий статус (цілі, завдання, функції, права та обов'язки тощо) суб'єктів публічної влади, які у тій чи іншій мірі займаються питаннями забезпечення реалізації інформаційної безпеки, наприклад: Постанови КМУ «Питання діяльності Міністерства інформаційної політики України» від 14.01.2015 р. № 2 [80], «Про затвердження Положення про Міністерство оборони України» від 26.11.2014 р. № 671 [95], «Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України» від 03.09.2014 р. № 411 [93] та ін.;

3) функціональні – підзаконні нормативно-правові акти, положеннями яких визначаються безпосередні заходи з реалізації інформаційної безпеки, врегульовуються і конкретизуються форми та процедури її здійснення (наприклад, розпорядження КМУ «Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року» від 30.03.2023 р. N 272-р; постанова КМУ «Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури» від 24.03. 2023 р. № 257.

Отже, підсумовуючи даний підрозділ, можемо охарактеризувати

сучасний стан нормативно-правового регулювання забезпечення реалізації інформаційної безпеки України як задовільний, адже на сьогодні в нашій державі прийнято цілий ряд нормативно-правових актів різної юридичної сили, які визначають і концептуальні, і матеріально-правові, і процедурні аспекти реалізації зазначеної безпеки. Наразі інформаційна безпека на офіційному рівні визнана неодмінною і вкрай важливою складовою забезпечення національної, державної та воєнної безпеки держави, а нормативно-правові засади механізму забезпечення реалізації безпосередньо самої інформаційної безпеки розраховані не лише на боротьбу із конкретними нагальними загрозами і небезпеками, а на всебічне зміцнення і розвиток інформаційної сфери України з урахуванням як національних, так і міжнародних інтересів нашої держави. Разом із тим не можна не відмітити того, що відсутність закону «Про інформаційну безпеку України», який мав би стати стрижневим у системі нормативно-правових актів з питань інформаційної безпеки, не сприяє узгодженій та послідовній реалізації цієї безпеки [16].

Висновки до Розділу 1

Акцентовано увагу на тому, що аналіз положень Закону України «Про інформацію», що був прийнятий в нашій державі у жовтня 1992 року, переконливо свідчить про досить чітке усвідомлення владою того, що інформаційна сфера є вкрай важливою і необхідною умовою розвитку як окремої особи, так і суспільства і держави в цілому, а також того, що інформація та інформаційна діяльність можуть застосовуватися як із благими намірами, так і у злочинних цілях. А тому вкрай важливо не лише затвердити право осіб на інформацію (її вироблення, збирання, зберігання, використання, розповсюдження), але й закріпити гарантії та інструменти забезпечення безпеки інформаційної сфери. Однак, у той же час не можна говорити про те,

що приймаючи закон «Про інформацію» на початку 90-х років XX-го століття, українська влада приділяла суттєву увагу інформаційній безпеці українського суспільства і держави.

Наголошено, що період від проголошення державного суверенітету до прийняття Конституції України включно, тобто 1990 - 1996 роки 20-го століття, слід вважати першим етапом становлення та розвитку інформаційної безпеки України. Характерними властивостями того часу стало: по-перше, визнання офіційною владою інформаційної сфери як окремої, самостійної і вкрай важливої галузі суспільного життя; по-друге, закріплення того, що інформація та інформаційна діяльність не лише сприяють розвитку держави і суспільства, але можуть становити суттєву загрозу для їх інтересів; по-третє, встановленні організаційно-правових засад державної політики в інформаційній сфері, при цьому окрема увага приділена охороні і захисту інформації, яка має особливе значення для забезпечення безпеки українського суспільства і держави; по-четверте, окреслення владних інституцій, які опікуються питаннями державної інформаційної політики, і наділені відповідними повноваженнями.

Констатовано, що попре зазначені позитивні кроки у напрямку забезпечення інформаційної безпеки України, зроблені протягом 1990 - 1996 років, говорити про те, що саме у цей час почалося формування цілісного механізму забезпечення зазнаної безпеки, навряд чи доцільно, адже тоді ще не існувало чіткого розуміння сутності інформаційної безпеки як складової національної безпеки, не було закладено концептуальних і стратегічних засад організації, функціонування та розвитку механізму інформаційної безпеки. Тож, визначивши зазначений період деякі засади функціонування інформаційного простору в Україні та здійснення державної політики щодо цього простору, управління ним, влада заклала необхідні підвалини для формування механізму забезпечення інформаційної безпеки України.

З’ясовано, що другий період становлення і розвитку інформаційної безпеки України, який припадає на 1998 – 2006 роки, був не такий насичений

за кількістю прийнятих нових нормативно-правових актів з питань інформації та інформаційної діяльності, однак він ознаменувався перш за все тим, що саме на цьому етапі українська влада нарешті прямо позначила інформаційну безпеку як неодмінну і вкрай важливу складову національної безпеки. Також на даному етапі були вперше, з моменту проголошення незалежності України, сформульовані та закріплені на офіційному рівні деякі концептуальні засади та програмні цілі і завдання забезпечення інформаційної безпеки в нашій державі. Крім того, в якості позитивних моментів, що властиві даному етапу становлення і розвитку інформаційної безпеки України, слід відмітити те, що: по-перше, українська влада почала усвідомлювати загрози інформаційній безпеці держави, які несе в собі широке впровадження і активне використання інформаційно-комп'ютерних технологій; по-друге, Україна приєдналася до міжнародних документів з питань протидії злочинності в кіберпросторі та захисту інформації; по-третє, було створено спеціальний орган публічної влади з питань захисту інформації, що становить особливе значення для українського суспільства і держави; по-четверте, визнано інформацію та інформаційні технології потужнім засобом дестабілізації суспільно-політичної обстановки в країні, що застосовується для підвищення ефективного та ведення воєнних конфліктів. Відповідно ефективний механізм забезпечення інформаційної безпеки є одним із важливих інструментів протидії воєнним конфліктам.

Аргументовано, що третій етап становлення та розвитку інформаційної безпеки, який тривав протягом 2007 до 2014 років, характеризується тим що: було сформульоване і закріплене на законодавчому рівні поняття інформаційної безпеки; інформаційна безпека була віднесена до однієї із ключових і пріоритетних на даному етапі суспільного розвитку сфер державної політики; закріплений пріоритет національних інтересів у сфері інформаційної безпеки перед індивідуальними; визначені основні проблеми забезпечення інформаційної безпеки в Україні, а також засоби і шляхи їх усунення та подальшого удосконалення механізму інформаційної безпеки;

починають впроваджуватися міжнародні стандарти і норми протидії злочинній активності у інформаційному (зокрема кібернетичному) просторі. Однак, попри безумовно позитивні та такі важливі зміни у державній інформаційні й політиці, відмічено, що ті її завдання і аспекти, які стосуються саме забезпечення інформаційної безпеки все ще не склалися у комплексний підхід до врегулювання цього боку інформаційної сфери. Йдеться про те, що влада сфокусувалася на розвитку інформаційних технологій, їх активному впровадженні в усі ключові сфери суспільного життя, підвищенні інформаційної освіченості населення, а питанням інформаційної безпеки приділялася хоча і суттєва, втім вторинна увага, як необхідному кроку для протидії тим можливим ризикам і загрозам, що можуть нести у собі інформатизація та цифровізації суспільства.

Відмічено, що четвертий, етап становлення і розвитку інформаційної безпеки України розпочався у 2014 році після російської агресії проти нашої держави і триває до теперішнього часу. Саме ця подія досить чітко вказала на те: що війна може бути не лише у вигляді збройного протистояння, але й інформаційною, а фронт, відповідно може бути як військовий, так й інформаційний; що інформаційний суверенітет – це не якесь абстрактне, а цілком реальне явище, від забезпечення якого залежать і державність, і територіальна цілісність, і національна ідентичність; що для того, щоб захистити національні інтереси не достатньо запровадити заходи протидії лише окремим проявам злочинної активності в інформаційній сфері, натомість має бути сформований цілісний, комплексний, дієвий механізм, який би дозволяв вчасно виявляти та ефективно протистояти інформаційним загрозам будь-якого характеру і масштабу.

Констатовано, що тільки після початку агресії російської федерації проти України, яка в тому числі здійснюється в інформаційному просторі, українське суспільство та публічна влада почали по-справжньому уважно і відповідально ставитися до питання забезпечення інформаційної безпеки. Зокрема йдеться про те, що від визнання деяких окремих загроз і викликів,

що стоять перед Україною в інформаційній сфері, а також від визначення певних напрямків їх подолання, влада перейшла до: формулювання комплексу концептуальних засад, стратегічних пріоритетів, цілей і напрямків щодо забезпечення інформаційної безпеки України, як на глобальному, так і національному рівні; закріплення на законодавчому рівні основних засад організації та функціонування адміністративно-правового механізму забезпечення інформаційної безпеки із розподілом відповідних завдань і повноважень між суб'єктами публічної влади. Саме на цьому етапі інформаційної безпеки реально розкрилася як необхідна умова не просто протидії злочинності, а збереження української державності, територіальної цілісності та національної ідентичності.

Виокремлено наступні ключові напрямки забезпечення реалізації інформаційної безпеки України: 1) ідеологічний; 2) нормативно-правовий; 3) організаційно-управлінський; 4) культурно-освітній; 5) налагодження ефективної, системної та систематичної внутрішньодержавної взаємодії та міжнародної співпраці з питань інформації та інформаційної безпеки; 6) інноваційний.

Акцентовано увагу на тому, що ідеологія сучасної державної політики з реалізації інформаційної безпеки в Україні має враховувати цілу низку умов і факторів та, звичайно ж, не зводитися виключно до протистояння конкретному ворогу (у даний час це російська федерація, яка активно веде інформаційну війну проти України). В основі цієї ідеології мають бути як національні та громадянські, так і абсолютні (або всезагальні) цінності та принципи. Україна має прагнути сформувати і розвивати стійку і адаптивну інформаційну систему із широкими можливостями, яка здатна ефективно протистояти і національним, і глобальним загрозам. Ключовою ідеєю протидії зазначеним загрозам мають стати не стільки заборони і різного роду обмеження з метою відгородитися, закритися від усього, що є чи здається ворожим, небезпечним, незрозумілим, скільки високоефективна контрпропаганда та просвітницька робота, спрямована на виховання медійно

грамотних людей, з високим рівнем інформаційної та громадянської культури, правової та національної свідомості, здатних критично ставитися до отриманої інформації та ідентифікувати відповідні загрози. Тож по-справжньому ефективний механізм забезпечення інформаційної безпеки не може спиратися на ізоляціонізм.

Аргументовано, що нормативно-правовий напрямок розвитку державної політики у сфері забезпечення реалізації інформаційної безпеки України включає: а) забезпечення своєчасного оновлення нормативно-правове підґрунтя механізму забезпечення інформаційної безпеки в Україні, приводячи його у відповідність до перспектив подальшого розвитку та актуальних викликів і загроз; б) гармонійне поєднання прав і свобод людини та громадянина в інформаційній сфері з національними інтересами у ній; в) забезпечення нормативно-правових засад для ефективного просвітництва населення, підвищення їх медійної грамотності, правової культури та свідомості; г) створення сприятливих та нормативно-правових умов для розвитку економічної активності населення у інформаційній сфері; г) удосконалення матеріально-правових та процедурних засад контролю в інформаційній сфері, своєчасне виявлення та оцінювання ризиків; д) створення сприятливого нормативно-правого середовище для взаємодії публічної влади всіх рівні із громадськістю з питань інформації та інформаційної діяльності.

Підкреслено, що сутнісний зміст управлінської діяльності полягає у ефективній організації функціонування підпорядкованої або керованої системи задля належного виконання її завдань та функцій. У розрізі представленої проблематики організаційно управлінський напрямок розвитку досліджуваної політики повинен передбачати: удосконалення системи суб’єктів забезпечення інформаційної безпеки; поліпшення якості кадрового забезпечення суб’єктів, які займаються забезпеченням інформаційної безпеки; покращення механізмів контролю за інформаційною діяльністю;

удосконалення механізмів координації діяльності суб'єктів із забезпечення інформаційної безпеки.

Констатовано, що сьогодні в Україні діє ціла низка нормативно-правових актів вищої юридичної сили, тобто Законів, які спрямовані на врегулювання відносин у сфері інформації та інформаційної діяльності. Відмічено, що наразі законодавчим регулюванням охоплено більшість аспектів організації та функціонування інформаційної галузі в нашій державі, при цьому значна увага відведена саме забезпеченню інформаційної безпеки України. Однак, при цьому ми не можна не відмітити тієї обставини, що жоден із вище значених нормативно-правових актів не є комплексним документом з питань реалізації державної політики саме у сфері інформаційної безпеки України. Кожен із вище згаданих законів регулюючи певні відносини у інформаційній сфері, питань інформаційної безпеки стосується лише у тій мірі, наскільки це необхідно для мети саме цього закону і предмету його регулювання. Натомість спеціального закону з питань інформаційної безпеки в нашій державі наразі немає. Переконані, що прийняття такого нормативно-правового акту є необхідним кроком, який забезпечить: по-перше, консолідацію усієї сукупності нормативно-правових актів з питань інформаційної безпеки у єдину структуровану систему із чітко визначеною ієрархією; по-друге, закріплення у системному вигляді на вищому юридичному рівні ключових засад реалізації інформаційної безпеки України, зокрема таких як: визначення основних термінів, принципи, гарантії, напрямки і форми, суб'єктне коло. Тобто цей закон має визначити цілісну та послідовну систему параметрів реалізації єдиної державної політики у сфері інформаційної безпеки.

Доведено, що окрім Законів, значну частину нормативно-правового підґрунтя реалізації інформаційної безпеки України складають підзаконні нормативно-правові акти, які умовно можна розподілити на декілька груп: 1) концептуальні. До цієї категорії підзаконних нормативно-правових актів належать ті, в яких викладені концептуальні та стратегічні засади державної

політики у щодо забезпечення інформаційної безпеки, програмні цілі та завдання з її реалізації; 2) статусні – це підзаконні нормативно-правові акти, в яких визначається правовий статус (цілі, завдання, функції, права та обов'язки тощо) суб'єктів публічної влади, які у тій чи іншій мірі займаються питаннями забезпечення реалізації інформаційної безпеки; 3) функціональні – підзаконні нормативно-правові акти, положеннями яких визначаються безпосередні заходи з реалізації інформаційної безпеки, врегульовуються і конкретизуються форми та процедури її здійснення

Сучасний стан нормативно-правового регулювання забезпечення реалізації інформаційної безпеки України охарактеризовано як задовільний, адже на сьогодні в нашій державі прийнято цілий ряд нормативно-правових актів різної юридичної сили, які визначають і концептуальні, і матеріально-правові, і процедурні аспекти реалізації зазначеної безпеки. Наразі інформаційна безпека на офіційному рівні визнана неодмінною і вкрай важливою складовою забезпечення національної, державної та воєнної безпеки держави, а нормативно-правові засади механізму забезпечення реалізації безпосередньо самої інформаційної безпеки розраховані не лише на боротьбу із конкретними нагальними загрозами і небезпеками, а на всебічне зміцнення і розвиток інформаційної сфери України з урахуванням як національних, так і міжнародних інтересів нашої держави. Разом із тим, не можна не відмітити того, що відсутність закону «Про інформаційну безпеку України», який мав би стати стрижневим у системі нормативно-правових актів з питань інформаційної безпеки, не сприяє узгодженій та послідовній реалізації цієї безпеки.

РОЗДІЛ 2.
МЕХАНІЗМ ОРГАНІЗАЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

2.1. Розмежування галузей права у правовому регулюванні забезпечення реалізації інформаційної безпеки України.

Механізм забезпечення реалізації інформаційної безпеки України являє собою складне, багаторівневе і багатоаспектне утворення, в межах якого переплітається та поєднується велика кількість різного роду суспільних відносин, для належного впорядкування і гарантування яких потрібне залучення засобів регулювання різних галузей права, що обумовлено як специфікою суб'єктного складу цих відносин, так і їх предметною основою. Саме тому у межах представленого підрозділу ми маємо на меті дослідити межі регулятивного впливу окремих галузей права на забезпечення реалізації інформаційної безпеки України.

Перш за все поглянемо на зв'язок адміністративного та інформаційного права, засоби та методи якого є одними із ключових для врегулювання забезпечення реалізації інформаційної безпеки України. Задля цього слід звернути увагу на то що являють собою ці правові галузі, та які їх предмет і методи регулювання. Адміністративне право є однією з найбільш розгалужених та об'ємних галузей української системи права. В. В. Галунько та ін. цілком слушно відмічають, що аміністративне право наповнює всю правову матерію суспільства. Практично неможливо знайти важливі суспільні відносини, які б не врегульовувалися певною мірою нормами адміністративного права [3, с.18]. Для визначення ролі адміністративного права у правовій системі, В. В. Галунько звертається до розкриття змісту мети і завдань адміністративного права. Метою адміністративного права є врегулювання відносин між суб'єктами публічної адміністрації та приватними особами. Основними галузевими завданнями адміністративного

права є забезпечення того, щоб: публічна адміністрація якісно та своєчасно надавала адміністративні послуги; публічна адміністрація ефективно здійснювала виконавчо-розпорядчу діяльність; було мінімізовано корупційні та інші випадки зловживань у діяльності публічної адміністрації [3, с.18]. Предметом адміністративного права України, на думку зазначеного правника є суспільні відносини, які виникають між суб'єктами публічної адміністрації та приватними особами. За змістом предмет адміністративного права складається з надання адміністративних послуг і здійснення виконавчо-розпорядчої діяльності (публічного управління) адміністрацією [3, с.20]. Ю.П. Битяк, В. М. Гаращук, О. В. Дьяченко сстверджують, що предмет адміністративного права становлять суспільні відносини, які виникають з метою реалізації і захисту прав громадян, створення нормальних умов для функціонування громадянського суспільства й держави. Такі відносини пов'язані з: 1) діяльністю органів виконавчої влади; 2) внутрішньо-організаційною діяльністю інших державних органів, підприємств, установ, організацій; 3) управлінською діяльністю органів місцевого самоврядування; 4) здійсненням іншими недержавними суб'єктами делегованих повноважень органів виконавчої влади; 5) здійсненням правосуддя у формі адміністративного судочинства. Правознавці підкреслюють, що предмет адміністративного права охоплює широке коло відносин, зміст яких об'єктивно потребує правового врегулювання за допомогою специфічних методів, механізмів. Остання обставина дозволяє визначити адміністративне право як профілюючу галузь, яка разом із кримінальним і цивільним правом утворює юридичну основу, обов'язкову частину очолюваної конституційним правом системи [2, с.25-26]. С.М. Алфьоров, С.В. Ващенко, М.М. Долгополова, А. П. Купін у своїх тлумачать адміністративне право як галузь права, що регулює з метою реалізації завдань і функцій держави суспільні відносини управлінського характеру, які складаються у сфері виконавчої влади, внутрішньо-організаційній діяльності інших державних органів, а також у процесі здійснення громадськими організаціями, їх

органами зовнішніх юридично-владних повноважень. Інакше кажучи, зауважують дослідники, адміністративне право - це управлінське право, яке відрізняється від інших галузей права специфікою предмета, методу регулювання та структурними особливостями. Предмет адміністративного права, на їх думку, становить широкий комплекс суспільних відносин, що виникають у зв'язку з реалізацією функцій державної виконавчої влади, змістом якої є управління суспільством [5, с.8-9]. При цьому, підкреслюють С.М. Алфьоров та ін. адміністративному праву притаманні певні межі правового регулювання - це сфера діяльності виконавчих та розпорядчих органів і суспільні відносини управлінського характеру, що складаються у цій сфері. Вони виникають, розвиваються та припиняються між: вищими і нижчими органами виконавчої влади (між Кабінетом Міністрів України і обласною державною адміністрацією); органами виконавчої влади і підпорядкованими їм підприємствами, установами, організаціями (між Міністерством освіти і науки України і ректором вищого навчального закладу); органами виконавчої влади, які не пов'язані безпосередньо підпорядкованістю (між Міністерством охорони здоров'я України і Міністерством освіти і науки України); органами управління й органами громадських організацій (між обласною державною адміністрацією і президією обласної ради профспілок); органами виконавчої влади і громадянами (між районним відділом внутрішніх справ і громадянином, який притягається до адміністративної відповідальності за адміністративний проступок) [5, с.9]. Особливістю предмета адміністративного права, на думку науковців, виступає те, що ним є не саме державне управління, а суспільні відносини, які у зв'язку з управлінням виникають. Саме це дає змогу віднести до предмета адміністративного права й недержавні види управлінського впливу (наприклад, у сфері комерційної, підприємницької діяльності). Основне завдання адміністративного права - це правове регулювання організаційних, управлінських відносин у суспільстві (адміністративна діяльність) та правоохоронна діяльність держави [5]. З точки зору В. А.

Бортника Адміністративне право — сукупність правових норм, які регулюють суспільні відносини, що формуються в ході забезпечення органами виконавчої влади і органами місцевого самоврядування реалізації та захисту прав, свобод і законних інтересів фізичних і юридичних осіб, а також: у процесі державного і самоврядного управління в сферах соціально-економічного й адміністративно- політичного розвитку та охорони громадського порядку. Предмет адміністративного права — суспільні відносини, які виникають з метою реалізації і захисту прав громадян, створення нормальних умов для функціонування громадянського суспільства й держави. Суспільні відносини, що перебувають у сфері регулювання адміністративним правом (тобто є його предметом) – це: а) відносини, що формуються у ході державного управління економічною, соціально-культурною та адміністративно-політичною сферами, а також реалізації повноважень виконавчої влади, делегованих державою органам місцевого самоврядування, громадським організаціям і деяким іншим недержавним інституціям; б) відносини, що формуються у ході діяльності органів виконавчої влади та органів місцевого самоврядування, їх посадових осіб щодо забезпечення реалізації та захисту в адміністративному порядку прав і свобод громадян, надання їм, а також юридичним особам різноманітних адміністративних (управлінських) послуг; в) відносини, що формуються у процесі внутрішньої організації та діяльності апаратів усіх державних органів, адміністрацій державних підприємств, установ та організацій, а також у зв’язку з проходженням державної служби або служби в органах місцевого самоврядування; г) у зв’язку з реалізацією юрисдикції адміністративних судів і поновлення порушених прав громадян та інших суб’єктів адміністративного права; ґ) у ході застосування заходів адміністративного примусу, включаючи адміністративну відповідальність щодо фізичних і юридичних осіб [11, с.11-12]. З точки зору О. Ф. Андрійко адміністративне право — одна з галузей публічного права, яка регулює суспільні відносини, що виникають у сфері організації, а також діяльності

органів публічної адміністрації, спрямованої на забезпечення та захист прав і свобод громадян. Норми адміністративного права, зауважує дослідниця, регулюють значне коло суспільних відносин, особливістю яких є те, що вони виникають у результаті владної діяльності органів публічної адміністрації, які діють від імені держави, і однією зі сторін цих відносин є орган виконавчої влади або виконавчий орган місцевого самоврядування чи інший орган, наділений державою владними повноваженнями у відповідній сфері. Об'єктом адміністративного права, з позиції О.Ф. Андрійко, є адміністративно-правові відносини, що формуються під час: 1) державного регулювання економічною, соціально-культурною, адміністративно-політичною сферою, реалізації повноважень органів державної виконавчої влади та виконавчих органів місцевого самоврядування, громадськими організаціями та іншими недержавними інституціями; 2) внутрішньої організації та діяльності органів публічної адміністрації у зв'язку з проходженням державної служби та служби в органах місцевого самоврядування; діяльності органів публічної адміністрації та їхніх посадових осіб щодо забезпечення реалізації та захисту в адміністративному праві прав і свобод громадян; 3) застосування заходів адміністративного примусу, зокрема, адміністративна відповідальність фізичних і юридичних осіб; 4) у зв'язку з реалізацією юрисдикції адміністративних судів щодо поновлення порушених прав громадян та інших суб'єктів адміністративного права [6].

Що ж стосується інформаційного права, то визначення предмету цієї галузі права є більш складним в силу того, що інформація як така пов'язана із кожною галуззю права. Г. В. Виноградова вважає, що предмет інформаційного права становлять відносини, що виникають в усіх сферах життя і діяльності особи, суспільства та держави в процесі збирання, зберігання, використання та поширення інформації [21, с.13]. Безпосередньо інформаційне право вона визначила як галузь права, що становить систему спеціальних правових норм, що виникають в інформаційній сфері (тобто у

сфері збирання, зберігання, використання та поширення інформації). Інформаційне право є комплексною галуззю, що ґрунтується на методах публічного і приватного права та використовує при вирішенні завдань правового регулювання інформаційних відносин практично весь арсенал правових механізмів [21, с.14].

Б. А. Кормич, аналізуючи проблематику предмету інформаційного права зауважує на тому, що чітке виокремлення предмету інформаційного права є доволі не непростим завданням, адже інформаційні відносини у тій чи іншій мірі присутні усім галузям права, наприклад, процес збирання доказів по кримінальній справі можна розглядати як процес збирання інформації, який начебто має регулюватися нормами інформаційного права, хоча насправді цей процес регулюється нормами кримінально-процесуального права. Б. А. Кормич стверджує, що для чіткого обмеження предметної сфери інформаційного права недоцільно розглядати як предмет регулювання будь-які суспільні відносини, що виникають з приводу інформації чи інформаційних процесів, адже інформація як така є складовою будь-якого типу суспільних відносин. Для інформаційного права важливі лише суспільні відносини, що визначають параметри і характеристики інформаційних процесів, тобто насамперед їх види, форми, засоби, й вже потім змістовне наповнення, яке не завжди має значення для правового регулювання. З огляду на зазначене, правознавець пропонує розуміти під предметом інформаційного права суспільні відносини, що виникають з приводу встановлення режимів та форм обігу інформації, реалізації інформаційних прав і правового статусу суб'єктів інформаційних процесів і формування їх правомірної поведінки і зв'язків [52, с.37].

Отже, з огляду на вище викладені наукові позиції щодо визначення поняття та розуміння змісту предмета регулювання адміністративної та інформаційної галузі права, можемо зробити висновок про те, що засобами адміністративного права визначаються і регламентуються, перш за все загальні матеріальні і процедурні засади організації та функціонування

державної політики щодо забезпечення інформаційної безпеки. Саме за допомогою адміністративно-правових засобів і механізмів врегульовані такі питання як: правовий статус центральних та територіальних органів виконавчої влади, які у тій чи іншій мірі залучені до забезпечення реалізації інформаційної безпеки в Україні; концептуальні та стратегічні засади забезпечення й розвитку інформаційної безпеки; пріоритетні напрямки діяльності та взаємодії суб'єктів публічної влади з питань інформаційної безпеки, а також координація їх діяльності; процедури та заходи протидії загрозам і викликам інформаційній безпеці України як на внутрішньому, так і зовнішньому рівнях; адміністративна відповідальність за порушення інформаційного законодавства та порядок притягнення до нього. У свою чергу засобами регулювання інформаційного права врегульовані ті відносини, процеси, факти, які стосуються: форм і способів створення (виготовлення, виробництва) інформації, її накопичення, зберігання, режимів використання і розповсюдження; здійснення індивідуальними і колективними суб'єктами своїх інформаційних прав та обов'язків; здійснення спеціальними суб'єктами контролю за законністю в інформаційній сфері; формування інформаційної культури населення та проведення відповідної просвітницької діяльності [**Error! Reference source not found.**].

Поряд із адміністративним та інформаційним правом, засобами яких регулюється забезпечення реалізації інформаційної безпеки, слід відмітити і Конституційне право. Саме нормами останнього: визначається загальне правове поле, в межах якого відбувається реалізація зазначеної безпеки; встановлюються основоположні гарантії та пріоритети на яких ґрунтується суспільно-державне життя в цілому та його інформаційна сфера зокрема; врегульовується правове становище суб'єктів загальної компетенції, які визначають організаційно-правові, ідеологічні, управлінські та інші основи держаної політики щодо забезпечення інформаційної безпеки [**Error! Reference source not found.**].

Отже, правове регулювання забезпечення реалізації інформаційної

безпеки є явищем комплексним і його не можна звести до засобів та (або) методів якоїсь окремої правової галузі, оскільки у механізмі цього забезпечення задіяна ціла низка суб'єктів різного рівня і статусу, а інструменти реалізації інформаційної безпеки мають і юридичний, і управлінський, і технічний, і культурний й інший характер, використання яких опосередковується правовідносинами, що мають як управлінську, так й іншу природу [**Error! Reference source not found.**].

2.2. Система суб'єктів забезпечення реалізації інформаційної безпеки України та місце серед них Служби безпеки України.

Механізм забезпечення реалізації інформаційної безпеки України має кілька обов'язкових, тобто таких, без яких він не функціонуватиме взагалі, структурних ланок, однією з яких є суб'єктний склад, адже саме вони (індивідуальні та колективні суб'єкти), власне і приймають рішення та безпосередньо здійснюють відповідні заходи з питань реалізації зазначеної безпеки. Кількість суб'єктів, які на сьогодні в нашій державі залучені до забезпечення інформаційної безпеки є дуже великою, одні більшою мірою опікуються питаннями формування державної політики у сфері інформаційної безпеки та прийняттям відповідних нормативно-правових актів, а інші – здійсненням певного кола заходів. З метою більш детального усвідомлення структури та змісту активної (або дієвої) складової механізму реалізації інформаційної безпеки, розглянемо систему суб'єктів забезпечення реалізації інформаційної безпеки України.

Перш за все слід визначити, що ми ведемо мову саме про систему, а не про звичайну сукупність чи окремих суб'єктів реалізації інформаційної безпеки. Система – це сукупність елементів, що характеризується структурою, зв'язками та функціями, які забезпечують цілеспрямований розвиток. У сучасній науці існує кілька варіантів визначення поняття

«система» залежно від того, яке базове поняття покладено в його основу [34, с.641]. Найбільш поширеними визначеннями зазначеного поняття є такі: система — цілісна взаємозалежна безліч об’єктів; система — цілісна безліч об’єктів (елементів), пов’язаних між собою взаємними відносинами; система — порядок (план, класифікація), згідно з яким розташовується група понять для утворення єдиного цілого; система — сукупність взаємозалежних, певним чином організованих і взаємодіючих елементів; система — організована безліч структурних елементів, що взаємопов’язані і виконують певні функції; система — комплекс вибірково залучених компонентів, у яких взаємодія і взаємини набувають характеру взаємоспрямування компонентів на одержання фіксованого корисного результату; система — сукупність взаємозалежних елементів, відособлена від середовища і взаємодіюча з ним як ціле [33, с.15]. З огляду на зазначене, система може бути охарактеризована такими поняттями як «цілісність», «сукупність», «множина». Система, являє собою певне організоване ціле, це явище, яке протилежне хаосу, дезорганізації та безладу. В найбільш загальному вигляді система – це об’єднана сукупність закономірно пов’язаних один з одним елементів. Для системи характерні кілька важливих ознак. По-перше, система – це сукупність елементів. По-друге, елементи поєднані один з одним зв’язками, які значно більш міцні порівняно зі зв’язками цих елементів з об’єктами навколишнього середовища. По-третє, вона характеризується організацією, яка відрізняє її від навколишнього середовища з його високою ентропією. По-четверте, для системи характерні інтегровані властивості, які не збігаються з властивостями суми елементів, а також відрізняються від властивостей окремих елементів. Тому система є цілісним утворенням. Важливими властивостями системи є структурність, взаємозалежність із навколишнім середовищем, ієрархічність, множинність описів. У таблиці наведено характеристики її властивостей. [34, с.641; 33, с.16]. Тож загалом, як справедливо відмічає І. М. Дудник, систему можна визначити як цілісну відмежовану сукупність взаємозв’язаних елементів, якій притаманні нові

інтегративні властивості, що є якісно вищими від суми властивостей окремих частин [33, с.16].

Отже, система суб'єктів забезпечення реалізації інформаційної безпеки являє собою складний механізм, тобто сукупність активних, взаємопов'язаних і взаємодіючих суб'єктів, що перебувають у певній ієрархії та виконують відведене їм функціональне призначення. Обсяги і характер компетенції зазначених суб'єктів у досліджуваній сфері різняться, залежно від того, є для них забезпечення реалізації інформаційної безпеки основним (одним із декількох основних) чи супутнім напрямом діяльності. З огляду на зазначене, вважаємо, що до основних складових вище зазначеної системи суб'єктів належать такі:

І. Суб'єкти загальної компетенції, до яких належать Верховна Рада України, Президент України, Кабінет Міністрів України, місцеві державні адміністрації, органи місцевого самоврядування.

1) Верховна Рада України (парламент) – це єдиний орган законодавчої влади в Україні, до повноважень якого належить наступне: внесення змін до Конституції України в межах і порядку, передбачених розділом XIII цієї Конституції; прийняття законів; затвердження Державного бюджету України та внесення змін до нього, контроль за виконанням Державного бюджету України, прийняття рішення щодо звіту про його виконання; визначення засад внутрішньої і зовнішньої політики, реалізації стратегічного курсу держави на набуття повноправного членства України в Європейському Союзі та в Організації Північноатлантичного договору; затвердження загальнодержавних програм економічного, науково-технічного, соціального, національно-культурного розвитку, охорони довкілля; заслуховування щорічних та позачергових послань Президента України про внутрішнє і зовнішнє становище України; оголошення за поданням Президента України стану війни і укладення миру, схвалення рішення Президента України про використання Збройних Сил України та інших військових формувань у разі збройної агресії проти України; розгляд і прийняття рішення щодо схвалення

Програми діяльності Кабінету Міністрів України; призначення за поданням Президента України Прем'єр-міністра України, Міністра оборони України, Міністра закордонних справ України, призначення за поданням Прем'єр-міністра України інших членів Кабінету Міністрів України, Голови Антимонопольного комітету України, Голови Державного комітету телебачення і радіомовлення України, Голови Фонду державного майна України, звільнення зазначених осіб з посад, вирішення питання про відставку Прем'єр-міністра України, членів Кабінету Міністрів України; призначення на посаду та звільнення з посади за поданням Президента України Голови Служби безпеки України; здійснення контролю за діяльністю Кабінету Міністрів України відповідно до цієї Конституції та закону; призначення на посади та звільнення з посад Голови та інших членів Рахункової палати; призначення на посаду та звільнення з посади Уповноваженого Верховної Ради України з прав людини; заслуховування його щорічних доповідей про стан дотримання та захисту прав і свобод людини в Україні; призначення на посади та звільнення з посад половини складу Національної ради України з питань телебачення і радіомовлення; затвердження загальної структури, чисельності, визначення функцій Служби безпеки України, Збройних Сил України, інших утворених відповідно до законів України військових формувань, а також Міністерства внутрішніх справ України; надання згоди на призначення на посаду та звільнення з посади Президентом України Генерального прокурора; висловлення недовіри Генеральному прокуророві, що має наслідком його відставку з посади; надання законом згоди на обов'язковість міжнародних договорів України та денонсація міжнародних договорів України; здійснення парламентського контролю у межах, визначених цією Конституцією та законом. Верховна Рада України здійснює також інші повноваження, які відповідно до Конституції України віднесені до її відання[51]. З викладеного видно, що парламент виконує декілька важливих функцій у контексті забезпечення реалізації інформаційної політики:

а) законотворча функція. Тобто встановлення вищому офіційному рівні на основоположних юридичних засад (принципів та норм), у відповідності до яких має бути організована та здійснюватися державна політика щодо інформаційної безпеки в Україні;

б) організаційно-установча функція, яка полягає у тому, що парламент призначає (або звільняє) чи надає згоду на призначення посадових певних посадових осіб, які займаються питаннями забезпечення інформаційної безпеки (наприклад, голова СБУ, Міністр культури та інформаційної політики України; половина складу Національної ради України з питань телебачення і радіомовлення). Крім того саме парламент затверджує структуру, функціональне призначення та чисельність таких правоохоронних органів як СБУ та МВС, а також ЗСУ, які роблять значний внесок у вирішення питань забезпечення інформаційної безпеки нашої держави;

в) контрольна функція. Д. О. Разумков відмічає, що парламентський контроль – важливий інструмент, який допомагає єдиному органу законодавчої влади України – Верховній Раді – отримувати необхідну інформацію про виконання обов’язків та здійснення повноважень органами виконавчої влади. Таким чином, український Парламент як представник всього народу контролює використання бюджетних коштів, дотримання законів, ефективність роботи міністерств та інших відомств [134]. Парламентський контроль за діяльністю органів виконавчої влади, зазначає І.К. Залюбовська, можна визначити як врегульовану правовими нормами діяльність Верховної Ради України щодо виявлення відповідності змісту, форм, методів, результатів діяльності органів виконавчої влади, їх керівників та інших посадових осіб Конституції України, вимогам законів. Головне завдання парламентського контролю полягає, однак, не в тому, щоб фіксувати недоліки та порушення, а в тому, щоб на підставі виявлених недоліків вживати реальних та дійових заходів щодо їх усунення, з'ясовувати їх причини та вживати заходів щодо запобігання їх у майбутньому шляхом надання відповідних зауважень та, якщо це необхідно, внесення змін та

доповнень до діючого законодавства, розробки заходів щодо нейтралізації виявлених порушень [38, с.11]. Отже, завдяки контролю, парламент може оцінювати якість та ефективність здійснення органами виконавчої влади державної політики у сфері забезпечення інформаційної безпеки. Даний контроль можна умовно поділити на такі різновиди: фінансовий, інформаційний, юридичний і політичний. Перший (тобто фінансовий) різновид контролю дає змогу парламенту перевіряти законність, ефективність та доцільність використання бюджетних коштів у межах забезпечення реалізації протидії інформаційної безпеки. Даний контроль здійснюється від імені ВРУ рахунковою палатою України. До інформаційного контролю можна віднести: заслуховування доповідей і звітів Кабінету Міністрів України, Генерального прокурора України, міністра МВС інших вищих посадових осіб органів виконавчої влади, які обираються, або для призначення яких необхідна згода Верховної Ради України; проведення «Днів уряду», запити, проведення парламентських дебатів щодо певних визначених питань державного життя, парламентські слухання [38, с.13]. Юридичним контролем парламенту, справедливо відзначає І.К. Залюбовська, можна вважати депутатські запити (інтерпеляції); депутатські звернення; парламентські розслідування; проведення без скликання у дводенний термін спеціальних (надзвичайних) засідань у разі введення військового або надзвичайного стану; дострокове припинення повноважень Верховної Ради Автономної Республіки Крим. Політичним контролем, на її думку, слід вважати резолюції про недовіру Кабінету Міністрів України; усунення з посади Президента України при застосуванні процедури імпічменту; звільнення з посад інших посадових осіб органів виконавчої влади [38, с.13]. Дослідниця підкреслює, що ці форми можна кваліфікувати як політичні, оскільки вони не можуть застосовуватися так часто і регулярно, як дві попередні. Окрім цього, у результаті їхньої реалізації настають значні зміни у політичній системі держави [38, с.13]. Важливо відмітити, що український парламент, як видно із вище наведеного, здійснює свої функції як безпосередньо, так і через своїх

посадових осіб (народні депутати, уповноважений з прав людини) та відповідні парламентські органи (комітети, Рахункова палата);

2) Президент України є главою держави і виступає від її імені. Крім того він є гарантом державного суверенітету, територіальної цілісності України, додержання Конституції України, прав і свобод людини і громадянина [51]. Навіть із цієї коротенької конституційної норми слідує, що Президент України є одним із основних суб'єктів забезпечення національної безпеки, неодмінною складовою якої, як ми вже неодноразово відмічали, є інформаційна безпека, а отже Глава держави, окрім іншого опікується й питаннями інформаційної безпеки. Коло повноважень Президента України закріплені у Конституції України. Так, відповідно до статті 106 Основного закону, Глава нашої держави: забезпечує державну незалежність, національну безпеку і правонаступництво держави; звертається з посланнями до народу та із щорічними і позачерговими посланнями до Верховної Ради України про внутрішнє і зовнішнє становище України; представляє державу в міжнародних відносинах, здійснює керівництво зовнішньополітичною діяльністю держави, веде переговори та укладає міжнародні договори України; призначає та звільняє глав дипломатичних представництв України в інших державах і при міжнародних організаціях; приймає вірчі і відкличні грамоти дипломатичних представників іноземних держав; призначає позачергові вибори до Верховної Ради України у строки, встановлені цією Конституцією; 8) припиняє повноваження Верховної Ради України у випадках, передбачених цією Конституцією; 9) вносить за пропозицією коаліції депутатських фракцій у Верховній Раді України, сформованої відповідно до статті 83 Конституції України, подання про призначення Верховною Радою України Прем'єр-міністра України в строк не пізніше ніж на п'ятнадцятий день після одержання такої пропозиції; вносить до Верховної Ради України подання про призначення Міністра оборони України, Міністра закордонних справ України; призначає на посаду та звільняє з посади за згодою Верховної Ради України Генерального прокурора;

призначає на посади та звільняє з посад половину складу Національної ради України з питань телебачення і радіомовлення; вносить до Верховної Ради України подання про призначення на посаду та звільнення з посади Голови Служби безпеки України; зупиняє дію актів Кабінету Міністрів України з мотивів невідповідності цій Конституції з одночасним зверненням до Конституційного Суду України щодо їх конституційності; є Верховним Головнокомандувачем Збройних Сил України; призначає на посади та звільняє з посад вище командування Збройних Сил України, інших військових формувань; здійснює керівництво у сферах національної безпеки та оборони держави; очолює Раду національної безпеки і оборони України; вносить до Верховної Ради України подання про оголошення стану війни та у разі збройної агресії проти України приймає рішення про використання Збройних Сил України та інших утворених відповідно до законів України військових формувань; приймає відповідно до закону рішення про загальну або часткову мобілізацію та введення воєнного стану в Україні або в окремих її місцевостях у разі загрози нападу, небезпеки державній незалежності України; створює у межах коштів, передбачених у Державному бюджеті України, для здійснення своїх повноважень консультативні, дорадчі та інші допоміжні органи і служби; підписує закони, прийняті Верховною Радою України; має право вето щодо прийнятих Верховною Радою України законів (крім законів про внесення змін до Конституції України) з наступним поверненням їх на повторний розгляд Верховної Ради України; здійснює інші повноваження, визначені Конституцією України [51]. Із наведеного переліку повноважень Президента можемо говорити, що він має нормотворчі, організаційно-установчі, контрольні та координаційні функції, які дозволяють йому: визначати нормативно-правові засади забезпечення реалізації інформаційної безпеки. Зокрема існуючі на сьогодні концептуальні і стратегічні засади інформаційної безпеки затверджені та введені в дію саме Главою держави; контролювати якість та ефективність функціонування національного механізму безпеки і оборони, однією із складових якого є й

інформаційна безпека; узгоджувати та спрямовувати діяльність інститутів публічної влади щодо забезпечення як національної безпеки в цілому, так й інформаційної зокрема; формувати за потреби спеціальні консультативно-дорадчі органи.

Особливе місце у системі президентських органів посідає Рада національної безпеки і оборони України (РНБО України), яка є координаційним органом з питань національної безпеки і оборони. Рада національної безпеки і оборони України координує і контролює діяльність органів виконавчої влади у сфері національної безпеки і оборони. Головою Ради національної безпеки і оборони України є Президент України, який формує і персональний склад цієї Ради національної безпеки і оборони України формує Президент України. До складу Ради національної безпеки і оборони України за посадою входять Прем'єр-міністр України, Міністр оборони України, Голова Служби безпеки України, Міністр внутрішніх справ України, Міністр закордонних справ України[51]. Функціями Ради національної безпеки і оборони України є: 1) внесення пропозицій Президентові України щодо реалізації засад внутрішньої і зовнішньої політики у сфері національної безпеки і оборони; 2) координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони у мирний час; 3) координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони в умовах воєнного або надзвичайного стану та при виникненні кризових ситуацій, що загрожують національній безпеці України [114]. Виконуючи ці функції РНБО України: розробляє та розглядає на своїх засіданнях питання, які відповідно до Конституції та законів України, Стратегії національної безпеки України, Воєнної доктрини України належать до сфери національної безпеки і оборони, та подає пропозиції Президентові України, приймає рішення щодо: визначення стратегічних національних інтересів України, концептуальних підходів та напрямів забезпечення національної безпеки і оборони у політичній,

економічній, соціальній, воєнній, науково-технологічній, екологічній, інформаційній та інших сферах; проектів державних програм, доктрин, законів України, указів Президента України, директив Верховного Головнокомандувача Збройних Сил України, міжнародних договорів, інших нормативних актів та документів з питань національної безпеки і оборони; удосконалення системи забезпечення національної безпеки та організації оборони, утворення, реорганізації та ліквідації органів виконавчої влади у цій сфері; проекту Закону України про Державний бюджет України та пропозицій до Бюджетної декларації по статтях, пов'язаних із забезпеченням національної безпеки і оборони України; матеріального, фінансового, кадрового, організаційного та іншого забезпечення виконання заходів з питань національної безпеки і оборони; заходів політичного, економічного, соціального, воєнного, науково-технологічного, екологічного, інформаційного та іншого характеру відповідно до масштабу потенційних та реальних загроз національним інтересам України; доручень, пов'язаних з вивченням конкретних питань та здійсненням відповідних досліджень у сфері національної безпеки і оборони, органам виконавчої влади та науковим закладам України; залучення контрольних, інспекційних та наглядових органів, що функціонують у системі виконавчої влади, до здійснення контролю за своєчасністю та якістю виконання прийнятих Радою національної безпеки і оборони України рішень, введених в дію указами Президента України; забезпечення і контролю надходження та опрацювання необхідної інформації, її збереження, конфіденційності та використання в інтересах національної безпеки України, аналізу на її основі стану і тенденції розвитку подій, що відбуваються в Україні і в світі, визначення потенційних та реальних загроз національним інтересам України та ін. [114];

3) Кабінет Міністрів України (уряд) є вищим органом у системі органів виконавчої влади. Уряд здійснює виконавчу владу безпосередньо та через міністерства, інші центральні органи виконавчої влади, Раду міністрів Автономної Республіки Крим та місцеві державні адміністрації, спрямовує,

координує та контролює діяльність цих органів. Кабінет Міністрів України відповідальний перед Президентом України і Верховною Радою України, підконтрольний і підзвітний Верховній Раді України у межах, передбачених Конституцією України. До основних завдань Кабінету Міністрів України належать: забезпечення державного суверенітету та економічної самостійності України, здійснення внутрішньої та зовнішньої політики держави, виконання Конституції та законів України, актів Президента України; вжиття заходів щодо забезпечення прав і свобод людини та громадянина, створення сприятливих умов для вільного і всебічного розвитку особистості; забезпечення проведення бюджетної, фінансової, цінової, інвестиційної, у тому числі амортизаційної, податкової, структурно-галузевої політики; політики у сферах праці та зайнятості населення, соціального захисту, охорони здоров'я, освіти, науки і культури, охорони природи, екологічної безпеки і природокористування; розроблення і виконання загальнодержавних програм економічного, науково-технічного, соціального, культурного розвитку, охорони довкілля, а також розроблення, затвердження і виконання інших державних цільових програм; забезпечення розвитку і державної підтримки науково-технічного та інноваційного потенціалу держави; здійснення заходів щодо забезпечення обороноздатності та національної безпеки України, громадського порядку, боротьби із злочинністю, ліквідації наслідків надзвичайних ситуацій; спрямування та координація роботи міністерств, інших органів виконавчої влади, здійснення контролю за їх діяльністю [102]. Діяльність Кабінету Міністрів України спрямовується на забезпечення інтересів Українського народу шляхом виконання Конституції та законів України, актів Президента України, а також Програми діяльності Кабінету Міністрів України, схваленої Верховною Радою України, вирішення питань державного управління у сфері економіки та фінансів, соціальної політики, праці та зайнятості, охорони здоров'я, освіти, науки, культури, спорту, туризму, охорони навколишнього природного середовища, екологічної безпеки, природокористування, правової політики,

законності, забезпечення прав і свобод людини та громадянина, запобігання і протидії корупції, розв'язання інших завдань внутрішньої і зовнішньої політики, цивільного захисту, національної безпеки та обороноздатності. Зокрема, реалізуючи свої завдання та функції уряд України, окрім іншого, проводить державну політику у сфері інформатизації, сприяє становленню єдиного інформаційного простору на території України [102].

Отже, уряд, як вищий орган виконавчої гілки влади, здійснює значний обсяг роботи щодо забезпечення реалізації інформаційної безпеки. Основними напрямками цієї роботи є такі:

а) нормовстановчий. Уряд наділений повноваженнями, які дають йому змогу, як готувати відповідні законопроекти для ВРУ, так і приймати власні підзаконні акти матеріально-правового і процедурного характеру;

б) організаційно-установчий, який проявляється у повноваженнях КМУ щодо призначення (звільнення) певних посадових осіб (наприклад Голова Державної служби спеціального зв'язку та захисту інформації України), а також щодо утворення і ліквідації органів виконавчої гілки влади (для прикладу, територіальні органи поліції утворює, ліквідовує та реорганізовує Кабінет Міністрів України за поданням Міністра внутрішніх справ України на підставі пропозицій керівника поліції [109]; територіальний орган Адміністрації Державної служби спеціального зв'язку та захисту інформації України утворюється, ліквідується та реорганізовується за погодженням з Віце-прем'єр-міністром України - Міністром цифрової трансформації України, Кабінетом Міністрів України [97]);

в) управлінський, в межах якого уряд: визначає цілі та пріоритети реалізації державної політики щодо забезпечення інформаційної безпеки, розробляє відповідні програми дій і плани заходів; розподіляє роботу між виконавцями зазначених програм і планів заходів, координує та контролює їх роботу; визначає обсяги та джерела необхідних ресурсі;

г) фінансовий. Уряд забезпечує проведення державної фінансової та податкової політики, сприяє стабільності грошової одиниці України. КМУ

розробляє та схвалює Бюджетну декларацію, розробляє проекти законів про Державний бюджет України та про внесення змін до Державного бюджету України, забезпечує виконання затвердженого Верховною Радою України Державного бюджету України, подає Верховній Раді України звіт про його виконання; приймає рішення про використання коштів резервного фонду Державного бюджету України [102].

4) місцеві державні адміністрації, які здійснюють виконавчу владу в областях і районах, містах Києві та Севастополі. Також вони реалізую повноваження, делеговані їй відповідною місцевою радою (тобто органом муніципальної влади). Місцеві державні адміністрації в межах відповідної адміністративно-територіальної одиниці забезпечують: виконання Конституції, законів України, актів Президента України, Кабінету Міністрів України, інших органів виконавчої влади вищого рівня; законність і правопорядок, додержання прав і свобод громадян; виконання державних і регіональних програм соціально-економічного та культурного розвитку, програм охорони довкілля, програм утвердження української національної та громадянської ідентичності, а в місцях компактного проживання корінних народів і національних меншин – також програм їх національно-культурного розвитку; підготовку та схвалення прогнозів відповідних бюджетів, підготовку та виконання відповідних бюджетів; звіт про виконання відповідних бюджетів та програм; взаємодію з органами місцевого самоврядування; реалізацію інших наданих державою, а також делегованих відповідними радами повноважень [105]. Здійснюючи ці завдання та функції, адміністрації вирішують такі питання: забезпечення законності, охорони прав, свобод і законних інтересів громадян; соціально-економічного розвитку відповідних територій; бюджету, фінансів та обліку; розвиток науки, освіти, культури, охорони здоров’я, фізкультури і спорту, сім’ї, жінок, молоді та дітей, утвердження української національної та громадянської ідентичності; проведення оборонної роботи та мобілізаційної підготовки [105]. Окрім цього місцеві адміністрації реалізують контрольні повноваження у ряді сфер,

зокрема це контроль за: станом фінансової дисципліни, обліку та звітності, виконання державних контрактів і зобов'язань перед бюджетом, належним і своєчасним відшкодуванням шкоди, заподіяної державі; додержанням законодавства з питань науки, мови, реклами, освіти, культури, охорони здоров'я, материнства та дитинства, сім'ї, молоді та дітей, соціального захисту населення, фізичної культури і спорту, охороною праці та своєчасною і не нижче визначеного державою мінімального розміру оплатою праці, додержанням громадської безпеки і порядку, правил технічної експлуатації транспорту та дорожнього руху, додержанням законодавства про державну таємницю та інформацію, станом захисних споруд цивільного захисту (цивільної оборони) [105];

5) органи місцевого самоврядування, які здійснюють муніципальну владу на відповідних територіях і вирішують наступні питання: утворення і ліквідація постійних та інших комісій ради, затвердження та зміна їх складу, обрання голів комісій; затвердження за пропозицією сільського, селищного, міського голови структури виконавчих органів ради, загальної чисельності апарату ради та її виконавчих органів відповідно до типових штатів, затверджених Кабінетом Міністрів України, витрат на їх утримання; затвердження програм соціально-економічного та культурного розвитку відповідних адміністративно-територіальних одиниць, цільових програм з інших питань місцевого самоврядування; розгляд прогнозу місцевого бюджету, затвердження місцевого бюджету, внесення змін до нього; затвердження звіту про виконання відповідного бюджету та ін. [106]. Загалом у законодавстві, що визначає основні засади організації та функціонування органів місцевого самоврядування в Україні практично немає положень, які б стосувалися безпосередньо забезпечення реалізації інформаційної безпеки, окрім хіба що норми, яка зобов'язує виконавчі органи місцевих рад сприяти діяльності Державної служби спеціального зв'язку та захисту інформації України [106].

Отже, враховуючи вище викладене, можемо дійти висновку, що

суб'єкти загальної компетенції, здійснюють свій внесок у забезпечення реалізації інформаційної безпеки України наступним чином:

а) формують загально правове поле, в якому відбувається реалізації інформаційної безпеки. Тобто саме суб'єкти загальної компетенції визначають ті основоположні матеріально-правові та процедурні засади, на яких ґрунтується державна інформаційна політика та забезпечення інформаційної безпеки, як у державі в цілому, так і в окремих її регіонах.;

б) визначають концептуальні та стратегічні засади здійснення інформаційної безпеки на певний період з урахуванням чинних правових норм та принципів, а також реалій і потреб суспільного розвитку та забезпечення національної безпеки держави;

в) визначають загальну програму дій та заходів, які необхідно реалізувати задля виконання відповідних концепцій і стратегій, та забезпечення інформаційної безпеки;

г) здійснюють загальне управління механізмом забезпечення реалізації інформаційної безпеки, що передбачає: координацію діяльності підзвітних та (або) підпорядкованих органів і посадових осіб, уповноважених на реалізацію державної політики у сфері інформаційної безпеки; контроль за законністю та ефективністю їх роботи; розподіл завдань між зазначеними органами і посадовими особами та забезпечення їх необхідними матеріально-фінансовими ресурсами; визначення структури суб'єктів, які відповідальні за безпосереднє здійснення заходів із забезпечення інформаційної безпеки, а також призначення їх вищого керівництва.

ІІ. Суб'єкти забезпечення реалізації інформаційної безпеки України міжгалузевої компетенції. Основними представниками цієї групи суб'єктів є органи прокуратури та суди України. Прокуратура України становить єдину систему, яка в порядку, передбаченому цим Законом, здійснює встановлені Конституцією України функції з метою захисту прав і свобод людини, загальних інтересів суспільства та держави. На прокуратуру покладаються такі функції: 1) підтримання державного обвинувачення в суді;

2) представництво інтересів громадянина або держави в суді у випадках, визначених цим Законом та главою 12 розділу III Цивільного процесуального кодексу України; 3) нагляд за додержанням законів органами, що провадять оперативно-розшукову діяльність, дізнання, досудове слідство; 4) нагляд за додержанням законів при виконанні судових рішень у кримінальних справах, а також при застосуванні інших заходів примусового характеру, пов'язаних з обмеженням особистої свободи громадян [113].

Що ж стосується судів, то це єдині органи державної влади в Україні, які уповноваженні на здійснення правосуддя, тобто розгляд і вирішення в судових засіданнях цивільних справ, господарських, адміністративних та кримінальних справ, а також справ про адміністративні правопорушення. Суд, здійснюючи правосуддя на засадах верховенства права, забезпечує кожному право на справедливий суд та повагу до інших прав і свобод, гарантованих Конституцією і законами України, а також міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України [129].

Ми не будемо детально зупинятися на характеристиці цих суб'єктів, оскільки їх роль у забезпеченні реалізації інформаційної безпеки не має яскраво вираженого адміністративно-правового характеру. Втім відмітимо, що прокуратура і суди забезпечують досліджувану безпеку завдяки здійсненню правосуддя, а також через реалізацію судового контролю та прокурорського нагляду. У межах цих функцій зазначені суб'єкти забезпечують захист режиму законності та відновлення правового порядку у сфері інформації й інформаційної діяльності.

III. Суб'єкти галузевої компетенції. До цієї групи суб'єктів належить досить просторе коло суб'єктів, адже органи галузевої компетенції реалізують державну політику у відповідній галузі. Галузь — це поєднання об'єктів управління під керівництвом відповідного органу виконавчої влади за ознаками виробничої єдності незалежно від їх географічного розташування. Органами галузевої компетенції є: міністерства, інші

центральні органи виконавчої влади, що мають у своєму підпорядкуванні підприємства, установи, інші структури й тим самим керують певною галуззю (Міністерство оборони, Міністерство освіти і науки, Державний комітет України по водному господарству тощо), а також місцеві органи цих міністерств, інших центральних органів виконавчої влади [2, с.74]. Основними представниками галузевої компетенції в Україні є міністерства. Міністерство є центральним органом виконавчої влади, який забезпечує формування та реалізує державну політику в одній чи декількох визначених Кабінетом Міністрів України сферах, проведення якої покладено на Кабінет Міністрів України Конституцією та законами України. Міністерство очолює міністр України (далі - міністр), який є членом Кабінету Міністрів України. Основними завданнями міністерства як органу, що забезпечує формування та реалізує державну політику в одній чи декількох сферах, є: 1) забезпечення нормативно-правового регулювання; 2) визначення пріоритетних напрямів розвитку; 3) інформування та надання роз'яснень щодо здійснення державної політики; 4) узагальнення практики застосування законодавства, розроблення пропозицій щодо його вдосконалення та внесення в установленому порядку проектів законодавчих актів, актів Президента України, Кабінету Міністрів України на розгляд Президентові України та Кабінету Міністрів України; 4^{-1}) забезпечення здійснення соціального діалогу на галузевому рівні; 5) здійснення інших завдань, визначених законами України [133]. На сьогодні в нашій державі існує 19 міністерства, кожне з яких у тій чи іншій мірі у своїй діяльності займаються питаннями реалізації інформаційної безпеки, однак ступінь залучення деяких із цих галузевих органів публічної влади до вирішення проблем забезпечення реалізації інформаційної безпеки значно вищий, зокрема такими міністерствами є:

а) Міністерства культури та інформаційної політики (МКІП), яке є головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику у сферах культури, державної мовної політики, популяризації України у світі, державного

іномовлення, інформаційного суверенітету України (у частині повноважень з управління цілісними майновими комплексами державного підприємства “Мультимедійна платформа іномовлення України” та Українського національного інформаційного агентства “Укрінформ”) та інформаційної безпеки, а також забезпечує формування та реалізацію державної політики у сферах відновлення та збереження національної пам’яті, мистецтв, охорони культурної спадщини, музейної справи, вивезення, ввезення і повернення культурних цінностей. Про те, що МКІП є одним із ключових суб’єктів галузевої компетенції з питань інформаційної безпеки досить яскраво свідчить коло завдань і повноважень цього міністерства. Так основними завданнями МКІП є забезпечення формування та реалізація: державної політики у сферах культури та державної мовної політики; державної політики у сферах інформаційного суверенітету (у частині повноважень з управління цілісними майновими комплексами державного підприємства “Мультимедійна платформа іномовлення України” та Українського національного інформаційного агентства “Укрінформ”), інформаційної безпеки України; державної політики у сфері державного іномовлення; державної політики у сферах популяризації України в світі, стратегічних комунікацій, зокрема з питань поширення суспільно важливої інформації в Україні та за її межами. Відповідно до покладених на нього завдань зазначене міністерство виконує такі повноваження: узагальнює практику застосування законодавства з питань, що належать до його компетенції, розробляє пропозиції щодо вдосконалення законодавчих актів, актів Президента України, Кабінету Міністрів України та в установленому порядку вносить їх на розгляд Кабінету Міністрів України; розробляє проекти законів та інших нормативно-правових актів з питань, що належать до його компетенції; здійснює підготовку та подання Кабінетові Міністрів України пропозицій щодо застосування, скасування та внесення змін до спеціальних економічних та інших обмежувальних заходів (санкцій), що вносяться Кабінетом Міністрів України на розгляд Ради національної безпеки і оборони України

відповідно до Закону України “Про санкції”, та бере участь у формуванні, реалізації та моніторингу ефективності державної санкційної політики з питань, що належать до його компетенції; погоджує проекти законів, інших актів законодавства, які надходять на погодження від інших міністерств та інших центральних органів виконавчої влади, готує в межах повноважень, передбачених законом, висновки і пропозиції до проектів законів, інших актів законодавства, які подаються на розгляд Кабінету Міністрів України, та проектів законів, внесених на розгляд Верховної Ради України іншими суб’єктами права законодавчої ініціативи, нормативно-правових актів Верховної Ради Автономної Республіки Крим; готує в межах повноважень, передбачених законом, зауваження і пропозиції до прийнятих Верховною Радою України законів, що надійшли на підпис Президентові України; здійснює нормативно-правове регулювання у сферах культури та мистецтв, інформаційного суверенітету (у частині повноважень з управління цілісними майновими комплексами державного підприємства “Мультимедійна платформа іномовлення України” та Українського національного інформаційного агентства “Укрінформ”), інформаційної безпеки України, державної мовної політики, охорони культурної спадщини, популяризації України в світі, державного іномовлення, вивезення, ввезення і повернення культурних цінностей, музейної справи, відновлення та збереження національної пам’яті; здійснює нормативно-правове регулювання в інформаційній та видавничій сферах, у сфері медіа; бере участь у здійсненні нормативно-правового регулювання з питань тимчасово окупованих територій України у Донецькій та Луганській областях, Автономній Республіці Крим і м. Севастополі та населення, що на них проживає, з метою їх реінтеграції в єдиний культурний та інформаційний простір України; визначає перспективи та пріоритетні напрями розвитку у сферах культури та мистецтв, інформаційного суверенітету (у частині повноважень з управління цілісними майновими комплексами державного підприємства “Мультимедійна платформа іномовлення України” та Українського

національного інформаційного агентства “Укрінформ”), інформаційної безпеки України, державної мовної політики, охорони культурної спадщини, популяризації України в світі, державного іномовлення, вивезення, ввезення і повернення культурних цінностей, музейної справи, відновлення та збереження національної пам’яті; визначає перспективи та пріоритетні напрями розвитку в інформаційній та видавничій сферах, у сфері медіа; визначає перспективи та пріоритетні напрями реінтеграції населення, що проживає на тимчасово окупованих територіях України у Донецькій та Луганській областях, Автономній Республіці Крим і м. Севастополі, в єдиний культурний та інформаційний простір України, забезпечує їх реалізацію та ін. [31];

б) Міністерство цифрової трансформації України, яке є головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики: у сферах цифровізації, цифрового розвитку, цифрової економіки, цифрових інновацій та технологій, робототехніки та роботизації, електронного урядування та електронної демократії, розвитку інформаційного суспільства, інформатизації; у сфері впровадження електронного документообігу; у сфері розвитку цифрових навичок та цифрових прав громадян; у сферах відкритих даних, публічних електронних реєстрів, розвитку національних електронних інформаційних ресурсів та інтероперабельності, електронних комунікацій та радіочастотного спектра, розвитку інфраструктури широкосмугового доступу до Інтернету, електронної комерції та бізнесу; у сфері надання електронних та адміністративних послуг; у сферах електронних довірчих послуг та електронної ідентифікації; у сфері розвитку ІТ-індустрії; у сфері розвитку та функціонування правового режиму Дія Сіті. Основними завданнями Мінцифри є формування та реалізація державної політики: у сферах цифровізації, цифрового розвитку, цифрової економіки, цифрових інновацій та технологій, робототехніки та роботизації, електронного урядування та електронної демократії, розвитку інформаційного суспільства; у сфері

впровадження електронного документообігу; у сфері розвитку цифрових навичок та цифрових прав громадян; у сферах відкритих даних, публічних електронних реєстрів, розвитку національних електронних інформаційних ресурсів та інтероперабельності, електронних комунікацій та радіочастотного спектра, розвитку інфраструктури широкосмугового доступу до Інтернету, електронної комерції та бізнесу; у сфері надання електронних та адміністративних послуг; у сферах електронних довірчих послуг та електронної ідентифікації та інвестицій в ІТ-індустрію; у сфері розвитку ІТ-індустрії; у сфері розвитку та функціонування правового режиму Дія Сіті [81].

в) Міністерство внутрішніх справ, місія якого полягає у забезпеченні формування державної політики у сферах: 1) охорони прав і свобод людини, інтересів суспільства і держави, протидії злочинності, забезпечення публічної безпеки і порядку, а також надання поліцейських послуг; 2) захисту державного кордону та охорони суверенних прав України в її виключній (морській) економічній зоні; 3) цивільного захисту, захисту населення і територій від надзвичайних ситуацій та запобігання їх виникненню, ліквідації надзвичайних ситуацій, рятувальної справи, гасіння пожеж, пожежної та техногенної безпеки, діяльності аварійно-рятувальних служб, а також гідрометеорологічної діяльності; 4) міграції (імміграції та еміграції), у тому числі протидії нелегальній (незаконній) міграції, громадянства, реєстрації фізичних осіб, біженців та інших визначених законодавством категорій мігрантів [94]. МВС України є одним із ключових правоохоронних відомств у складі уряду України, в силу чого воно опікується цілою низкою управлінських питань з питань національної безпеки, зокрема тих, які стосуються інформаційної сфери та діяльності. Окремо слід відмітити, що саме МВС координує роботу Національної поліції України, у складі якої утворені та функціонують підрозділи кіберполіції, що опікується питаннями безпеки і підтримки порядку у електронних мережах;

г) Міністерство оборони України, основними завданнями якого є: 1)

забезпечення формування та реалізація державної політики з питань національної безпеки у воєнній сфері, сферах оборони і військового будівництва у мирний час та особливий період щодо: організації в силах оборони заходів оборонного планування; визначення засад воєнної, військової кадрової та військово-технічної політики у сфері оборони; 2) здійснення військово-політичного та адміністративного керівництва Збройними Силами; 2-1) забезпечення формування та реалізація державної політики з питань національного спротиву; 3) здійснення в установленому порядку координації діяльності державних органів та органів місцевого самоврядування щодо підготовки держави до оборони; 4) забезпечення в межах повноважень, передбачених законом, реалізації державної політики з оборонних питань, що пов'язані з використанням повітряного простору України та захистом суверенітету держави; 5) координація діяльності Держспецтрансслужби для забезпечення стійкого функціонування транспорту в мирний час та в особливий період [95]. Виконуючи покладені на нього завдання, МО України реалізує цілий ряд повноважень, які стосуються інформаційної безпеки нашої держави, зокрема: готує в межах повноважень, передбачених законом, зауваження і пропозиції до прийнятих Верховною Радою України законів, що надійшли на підпис Президентові України; провадить розвідувальну та інформаційно-аналітичну діяльність в інтересах національної безпеки та оборони держави; бере участь у виконанні завдань державної інформаційної політики у сфері оборони, інформаційних заходах, спрямованих на підвищення рівня обороноздатності держави та на протидію інформаційним операціям агресора (противника); проводить постійний моніторинг інформаційного середовища, виявляє потенційні та реальні інформаційні загрози в сфері оборони, здійснює відповідні заходи; засновує телерадіоорганізації, засоби масової інформації, офіційні друковані видання та бере участь у їх діяльності; забезпечує впровадження та розвиток новітніх інформаційних технологій у сфері оборони; відповідно до компетенції забезпечує електронну інформаційну взаємодію з органами державної влади

під час обміну інформацією для здійснення повноважень, визначених законодавством; забезпечує в межах повноважень, передбачених законом, демократичний цивільний контроль за діяльністю Збройних Сил та Держспецтрансслужби; створює необхідні умови для здійснення іншими суб'єктами демократичного цивільного контролю передбачених законом повноважень та інформує із зазначених питань громадськість та засоби масової інформації [95];

ґ) Міністерство освіти і науки, ключовими завданнями якого є 1) забезпечення формування та реалізація державної політики у сферах освіти і науки, наукової, науково-технічної діяльності та інноваційної діяльності в зазначених сферах, трансферу (передачі) технологій; 2) забезпечення формування та реалізації державної політики у сфері здійснення державного нагляду (контролю) за діяльністю закладів освіти, підприємств, установ та організацій, які надають послуги у сфері освіти або провадять іншу діяльність, пов'язану з наданням таких послуг, незалежно від їх підпорядкування і форми власності [96]. Здійснюючи свої завдання та функції, МОН України, окрім іншого, забезпечує реалізацію державної політики стосовно державної таємниці, захист інформації з обмеженим доступом, а також технічний захист інформації, контроль за їх збереженням в апараті МОН [96].

Отже, вище наведені завдання, функції та повноваження міністерств свідчать про те, що суб'єкти галузевої компетенції здійснюють величезний внесок у забезпечення реалізації інформаційної безпеки в Україні, зокрема саме вони:

- забезпечують реалізацію законів та підзаконних актів, що видаються такими органами загальної компетенції як Верховна Рада України, Президент України та Кабінет Міністрів України, з питань інформаційної безпеки;

- здійснюють управління підпорядкованими їм відповідними територіальними органами виконавчої влади, а також координують діяльність інших центральних органів влади, що перебувають у віданні відповідних

міністерств;

- контролюють ефективність та законність здійснення підпорядкованими і підвідомчими суб'єктами заходів інформаційної безпеки;

- аналізують стан практичної реалізації законодавчих положень з питань інформаційної безпеки та формулюють на підставі цього відповідні пропозиції і рекомендації вищим органам державної влади щодо удосконалення чинного законодавства з питань інформації та інформаційної безпеки;

- визначають стратегічні засади реалізації та розвитку інформаційної безпеки у межах їх галузі, планують заходи щодо забезпечення реалізації інформаційної безпеки, визначають їх виконавців та необхідні для цього ресурси.

IV. Суб'єкти спеціальної компетенції. Ці суб'єкти забезпечують реалізацію державної політики в певній сфері, здійснюють керівництво з питань, які мають загальний характер для всіх чи багатьох галузей господарства, соціально-культурного будівництва [2, с.75\]. Найбільш яскравими представниками цієї категорії суб'єктів, у контексті досліджуваної проблематики, є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України та Служба безпеки України.

1) Державна служба спеціального зв'язку та захисту інформації України виконує цілу низку завдань, що забезпечення інформаційного захисту, зокрема це: формування та реалізація державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах (далі - інформаційно-комунікаційні системи) і на об'єктах інформаційної діяльності, а також у сферах використання державних інформаційних ресурсів в частині захисту інформації, протидії технічним розвідкам, функціонування, безпеки

та розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, активної протидії агресії у кіберпросторі; участь у формуванні та реалізації державної політики у сферах електронного документообігу (в частині захисту інформації державних органів та органів місцевого самоврядування), електронної ідентифікації (з використанням електронних довірчих послуг, захисту критичної інформаційної інфраструктури), електронних довірчих послуг, захисту критичної інформаційної інфраструктури (у частині встановлення вимог з безпеки та захисту інформації під час надання та використання електронних довірчих послуг, захисту критичної інформаційної інфраструктури, контролю за дотриманням вимог законодавства у сфері електронних довірчих послуг, захисту критичної інформаційної інфраструктури); забезпечення в установленому порядку та в межах компетенції діяльності суб'єктів, які безпосередньо здійснюють боротьбу з тероризмом; реалізація державної політики щодо захисту критичної технологічної інформації, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснення державного контролю в цих сферах; визначення вимог до захисту критичної технологічної інформації, формування загальних вимог до кіберзахисту об'єктів критичної інфраструктури, ведення переліку об'єктів критичної інформаційної інфраструктури, здійснення заходів щодо його оновлення та актуалізації; створення та забезпечення функціонування системи активної протидії агресії у кіберпросторі; створення та забезпечення функціонування Центру активної протидії агресії у кіберпросторі; виконання інших завдань, передбачених законодавством у сфері забезпечення кібербезпеки та кіберзахисту [86]. Як видно із приведеного кола завдань Держспецзв'язку України вирішує цілий спектр важливих питань щодо забезпечення інформаційної безпеки України, які мають як технічний, так і організаційно-управлінський характер. Для вирішення цих питань Держспецзв'язку наділяється значним колом повноважень, які з одного боку зобов'язують даний суб'єкт до: створення та забезпечення належного функціонування

Національної телекомунікаційної мережі; впровадження організаційно-технічної моделі кіберзахисту та здійснює організаційно-технічні заходи із запобігання; виявлення та реагування на кіберінциденти та кібератаки та усунення їх наслідків, інформує про кіберзагрози та відповідні методи захисту від них; впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури; встановлення вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації); організації й проводення аудиту захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість; забезпечення функціонування Державного центру кіберзахисту, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA та ін. [148]; а з іншого боку, ці повноваження надають Держспецзв'язку ряд можливостей як то: одержувати в установленому порядку від органів державної влади, органів місцевого самоврядування, військових формувань, утворених відповідно до законів України, підприємств, установ і організацій незалежно від форми власності інформацію, документи і матеріали, необхідні для виконання покладених на Державну службу спеціального зв'язку та захисту інформації України завдань; залучати фахівців державних органів, органів місцевого самоврядування, військових формувань, утворених відповідно до законів України, підприємств, установ і організацій незалежно від форми власності за погодженням з їх керівниками до розгляду питань, що належать до повноважень Державної служби спеціального зв'язку та захисту інформації України, а також до проведення спільних інспекційних перевірок; отримувати доступ в установленому порядку своїх уповноважених представників на об'єкти (території, приміщення, будівлі, споруди тощо) державних органів, органів місцевого самоврядування, військових формувань, утворених відповідно до законів України, підприємств, установ і організацій незалежно від форми власності, на яких знаходяться засоби спеціального зв'язку Державної служби спеціального зв'язку та захисту інформації України, на об'єкти (території, приміщення, будівлі, споруди

тощо), державний контроль щодо яких покладено на Державну службу спеціального зв'язку та захисту інформації України; проводити планові та позапланові перевірки як стану технічного захисту інформаційних ресурсів, так і дотримання законодавчих вимог підконтрольними суб'єктами щодо ліцензійних та інших вимог, яким має відповідати діяльність суб'єктів в інформаційній сфері тощо [86];

2) Національна поліція України нами віднесена до кола суб'єктів спеціальної компетенції з питань забезпечення реалізації інформаційної безпеки переважно через те, що у її складі організовані та функціонують підрозділи кіберполіції. Департамент кіберполіції Національної поліції України є міжрегіональним територіальним органом Національної поліції України, який входить до структури кримінальної поліції Національної поліції та відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність. Основними завданнями Департаменту кіберполіції Національної поліції України є такі: а) участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; б) сприяння у порядку, передбаченому чинним законодавством, іншим підрозділам Національної поліції у попередженні, виявленні та припиненні кримінальних правопорушень [46]. Головні напрямки діяльності кіберполіції України – це: здійснення превентивної роботи у кіберпросторі; реагування на факти правопорушень у зазначеному просторі, їх припинення, виявлення та притягнення винних осіб до відповідальності; відновлення порушеного стану законності; аналіз практики застосування законодавства з питань кібербезпеки та надання вищестоящим органам публічної влади пропозицій і рекомендації щодо удосконалення цього законодавства.

3) Служба безпеки України (СБУ), яка підпорядкована Главі держави. СБУ – це державний орган спеціального призначення з правоохоронними функціями, який забезпечує державну безпеку України. Основними завданнями цього суб'єкта є: захист державного суверенітету, конституційного ладу, територіальної цілісності, науково-технічного і оборонного потенціалу України, законних інтересів держави та прав громадян від розвідувально-підривної діяльності іноземних спеціальних служб, посягань з боку окремих організацій, груп та осіб, а також забезпечення охорони державної таємниці. До завдань Служби безпеки України також входить попередження, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, тероризму та інших протиправних дій, які безпосередньо створюють загрозу життєво важливим інтересам України [126]. Із кола наведених завдань чітко видно, що забезпечення інформаційної безпеки України, яка складової національної безпеки нашої держави, є одним із основних напрямків роботи СБУ, яка СБУ комплексно забезпечує контррозвідувальний захист інформаційної та кібернетичної безпеки держави. Пріоритетними завданнями на цьому напрямі діяльності спецслужби є: боротьба з кібертероризмом і кібершпигунством; розслідування кіберінцидентів і кібератак на державні електронні інформаційні ресурси; протидія проведенню ворожих спеціальних інформаційних операцій [39]. Значення забезпечення інформаційної безпеки саме у кіберпросторі особливо актуалізувалося в умовах російської агресії проти України, яка має гібридний характер і відбувається не лише у вигляді військового вторгнення, але шляхом проведення різного роду інформаційних операцій, зокрема у кіберпросторі. Про збільшення активності російських кібератак красномовно свідчить офіційна статистика. Так, якщо у 2020 році СБУ зафіксувала майже 800 кібератак, у 2021 – 1400, то у 2022 їхня кількість зросла більш ніж утричі – до 4500. Пріоритетні цілі російських спецслужб в українському кіберпросторі – енергетика, інфраструктура, логістика, військові об'єкти, центри прийняття рішень, бази даних органів влади,

державні реєстри та медіа. Також для ворога є привабливою сфера цифрової трансформації України. Тож кіберпідрозділи СБУ забезпечують контррозвідувальний захист електронних комунікацій, ІТ-галузі та афілійованого з ними середовища [39]. Слід відзначити, що участь СБУ у забезпеченні реалізації інформаційної безпеки не обмежується відбиттям кібератак, вона також активно протидіють різного роду інформаційно-психологічним операціям, до яких активно вдається ворог, особливо із початком повномасштабного вторгнення на територію нашої країни [39].. Застосування зазначених операцій має на меті дискредитувати зовнішню і внутрішню політику, зменшити міжнародну підтримку України, розколоти наше суспільство, поширювати панічні настрої. Задля цього згенеровані кремлівським режимом фейки масово тиражують підконтрольні йому медіа, політики, блогери. Захищаючи інформаційний простір держави кіберфахівці СБУ блокували десятки ботоферм, численні антиукраїнські ютуб-канали. Викрили та притягнули до відповідальності сотні інтернет-агітаторів, які поширювали ворожі фейки та наративи. Наявні на сьогодні ресурси дають Україні змогу не тільки відбивати кібератаки та блокувати деструктивну діяльність в інформаційному просторі, а й атакувати ворога [39]. Задля забезпечення реалізації інформаційної безпеки у системі СБУ утворений та функціонує Ситуаційний центр забезпечення кібербезпеки, фахівці якого цілодобово дбають про інформаційну безпеку країни, а саме: протидіють кіберрозвідкам іноземних держав; займаються боротьбою з кібертероризмом і кібершпигунством; здійснюють контррозвідувальні та оперативно-розшукові заход; протидіють спробам розхитати ситуацію в країні через різноманітні інформаційні «вкиди» [142].

Слід відмітити, що СБУ, забезпечуючи інформаційну безпеку покладається як на власні ресурси, так й активно співпрацює з іншими суб’єктами на міжнародній арені та в середині держави. Так, для посилення колективної кібербезпеки СБУ тісно співпрацює з колегами з країн ЄС і НАТО, координує свою діяльність з ІТ-фахівцями з усього світу. У той же час

СБУ докладає значних зусиль для налагодження активної співпраці із громадськістю для забезпечення ефективної протидії ворожому впливу і агресії. Так, наприклад, Департамент кібербезпеки СБУ з перших днів війни створив один з важливих інструментів протидії ворогу – телеграм-бот @stop_russian_war_bot. На нього громадяни відправляли та відправляють оперативну інформацію про переміщення військ ворога. Завдяки таким повідомленням було знищено сотні одиниць ворожої техніки і ліквідовано декількох російських генералів. Також на нього можна повідомляти дані про колаборантів. Протягом року українці направили у чат-бот понад 100 000 повідомлень [39].

З огляду на вище викладене, можемо констатувати, що саме суб'єкти спеціальної компетенції роблять найбільший внесок у питання безпосередньої реалізації державної політики у сфері інформаційної безпеки України, адже саме вони: займаються безпосереднім практичним втіленням тих рішень і заходів, які спрямовані на зміцнення стійкості національної інформаційної сфери; протидіють конкретним загрозам і викликам; мають найбільш повну та детальну інформацію про проблеми і недоліки правозастосовного, управлінського, матеріально-технічного, кадрового та іншого характеру, що виникають під час реалізації інформаційної безпеки.

Отже, за результатами проведеного у даному підрозділі дослідження, можемо стверджувати, що на сьогодні в Україні створена та функціонує розгалужена і багаторівнева система суб'єктів забезпечення реалізації інформаційної безпеки. У середині цієї системи існує доволі чітке розмежування компетенцій між зазначеними суб'єктами, кожен з яких виконує певний обсяг роботи орієнтованої на забезпечення зазначеної безпеки: одні визначать загальні правові засади і принципи її забезпечення, другі – концептуальні засади, стратегічні напрямки та пріоритети зміцнення і розвитку інформаційної безпеки; треті – розробляють програми реалізації зазначених концептуальних і стратегічних засад, визначають матеріальні і процедурні аспекти виконання закріплених правових засад і принципів з

огляду на реалії і потреби сьогодення; четверті – контролюють та координують практичну реалізацію заходів інформаційної безпеки у відповідності до вимог законності та ключових засад державної політики у цій сфері, а також опікуються питаннями ресурсного забезпечення діяльності спрямованої на забезпечення інформаційної безпеки; п’яті – безпосередньо на практиці виконують конкретні заходи правового, організаційного, технічного та іншого характеру, спрямовані на протидію загрозам інформаційній безпеці України, зміцнення стійкості національного інформаційного простору, захист прав і законних інтересів його індивідуальних та колективних учасників, зокрема держави і суспільства в цілому. Особлива роль у цьому аспекті забезпечення реалізації інформаційної безпеки відводиться Службі безпеки України, яка має здійснювати комплекс заходів, що передбачають протидію ворожому впливу і агресії в інформаційному середовищі як шляхом відбиття атак, так і через здійснення активних атакуючих дій, спрямованих на ліквідацію чи пригнічення ворожих інформаційних ресурсів та інфраструктури, що забезпечує їх функціонування [165].

2.3. Форми та методи реалізації інформаційної безпеки України.

Реалізація інформаційної безпеки є складною за своєю сутністю та змістом діяльністю, яка знаходить зовнішній прояв у відповідних формах. Взагалі, форма – це термін, що використовується для опису зовнішнього вигляду, в якому виражається певна сутність або зміст, будь то матеріальний чи нематеріальний. Форма відображає, як система, об'єкт, предмет, дія, думка і т. д. організовані. У зв'язку з цим, поняття форми також включає в себе такі поняття, як структура, порядок і організація. Термін «форма», підкреслює О.Б. Німко, означає вид, будь-який зовнішній прояв певного змісту. Це шлях здійснення цілеспрямованого впливу, що вказує як практично здійснюється

управлінська діяльність [72].

Форми права, пише Н. Чубоха, – це зовнішній вираз правових норм, що покликані регулювати суспільні відносини, які ухвалюються законодавчими та виконавчими органами держави, а також іншими уповноваженими на це органами. Форми права включають в себе як національні нормативно-правові акти, так і міжнародно-правові акти, згода на обов'язковість яких надана Верховною Радою України, а разом вони утворюють замкнуту систему національних форм права. Лише офіційно визнані види форм права можуть служити формою матеріалізації норми права [159, с.109]. Науковець слушно відмічає, що дослідження форм права має велике значення для подальшого вдосконалення правотворчості і правозастосувальної діяльності, зокрема, у сфері підготовки та видання нормативно-правових актів, врахування різних форм права для вираження змісту правової норми, їх систематизації тощо. Завдання законодавця полягає не в тому, щоб придумувати ті чи інші форми права, а в тому, щоб розвиваючи зміст права, вчасно виявити необхідність заміни застарілої форми новою і зі всієї багатоманітності об'єктивно можливих форм знайти ту, яка найбільше підходить до змісту права, найкращим способом виражає мету законодавства в даних умовах [159, с.109].

Таким чином, форми реалізації інформаційної безпеки України представляють собою зовнішній прояв практичної діяльності спеціально уповноважених суб'єктів, яка спрямована на створення правових та організаційних умов для забезпечення конфіденційності, цілісності та доступності інформації, а також на захист інформаційних ресурсів від несанкціонованого доступу, втрати, зміни, руйнування або розголошення. Варто зауважити, що в юридичній літературі сформовано не так багато підходів щодо переліку відповідних форм. Тож ми, спираючись на аналіз наукових поглядів вчених та норм чинного законодавства, переконані, що вказані форми найбільш доцільно поділити на три великі групи: 1) нормативно-правові; 2) організаційно-управлінські; та 3) спеціальні

форми, що властиві саме для реалізації інформаційної безпеки.

Так, в першу чергу приділимо увагу формам правовим. С.М. Мельничук пропонує розглядати правову форму як зумовлений правом і змістом діяльності держави нормативно визначений процес здійснення функцій держави органами державної влади та недержавними організаціями певними способами у межах, що регламентовані Конституцією та законами України [68, с.60]. А.Т. Комзюк відзначає, що правова форма – це специфічна організаційна форма діяльності органів держави та посадових осіб, яка, з одного боку, здійснюється на засаді суворого дотримання вимог законів та інших нормативно-правових актів, а з іншого, її результати завжди пов’язані з появою певних юридичних наслідків [49, с. 12]. До характерних ознак правової форми вчені відносять наступні: а) правова форма діяльності завжди пов'язана з розглядом юридичних питань, таких як правопорушення, правові спори, скарги. Це стосується життєвих обставин, які прямо визначені законом (або іншими нормативними актами) і вимагають певного підтвердження та юридичного регулювання; б) правова діяльність здійснюється виключно уповноваженими органами держави, посадовими особами та іншими суб'єктами; в) правова форма діяльності завжди включає в себе операції з нормами права і використовує їх як основний інструмент; г) результати правової діяльності завжди документуються у відповідних офіційних процесуальних документах, визначених законом; ґ) правова діяльність потребує встановлення ряду гарантій, і відносини, що виникають під час розгляду справ, регулюються системою норм процесуального права; д) правова діяльність включає в себе використання різних методів та засобів юридичної техніки [153]. Н.М. Пархоменко стверджує, що правові форми – це наукова комплексна категорія, що відображає різні суспільні явища, які потребують регламентації, а також слугує каркасом усередині права, впорядковує і поєднує всі правові явища і право як таке. Коли йдеться про правові форми, то мають на увазі право як певне соціальне явище, що відрізняється від інших явищ (політика, релігія, мораль), які разом із правом

визначаються матеріальними й економічними умовами життя суспільства. Іншими словами, поняття «правова форма» є загальним, відображенням об’єктивного зв’язку права і явищ, на які воно впливає, визначення його місця серед інших форм» [78, с.54-55].

Тож, саме через правові форми виражається сутність та практичний нормативного регулювання реалізації інформаційної безпеки в Україні. Серед правових форм, перш за все, варто виділити нормотворчість. Т.В. Курусь вказує, що нормотворчість - це особлива форма діяльності компетентних суб’єктів нормотворчості з підготовки, розробки, прийняття та офіційного оприлюднення норм права, яка заснована на пізнанні об’єктивних соціальних потреб та інтересів суспільства [60, с. 9]. До ключових ознак нормотворчості вчені відносить такі: здійснюється уповноваженими суб’єктами: а) державою, її органами (парламентом, урядом, міністерствами, місцевими адміністраціями тощо); б) громадянським суспільством (народом), його організаціями; є формою владної вольової діяльності уповноважених суб’єктів, яка включає в себе вивчення, узагальнення і систематизацію типових конкретних правовідносин, що виникають у суспільстві; є не диктатом волі уповноважених суб’єктів, а процедурою формулювання норм, котрі властиві соціальним відносинам, стали типовими діями їх учасників; виражається у санкціонуванні існуючих чи встановленні нових, зміні чи призупиненні чинних і скасуванні застарілих правових норм на підставах, передбачених законом; набуває завершення в письмовому акті-документі, що називається нормативно-правовим актом (законом) [60, с. 10].

О.В. Петришин вказує, що нормотворчість - це процес діяльності уповноважених суб'єктів, спрямований на створення, розгляд, прийняття та офіційне опублікування нормативно-правових актів відповідно до визначеної процедури. Основними рисами цього процесу є: 1) нормотворчість є складовою частиною процесу створення правових актів. Під час нормотворчості в нормативно-правових актах формалізуються норми права, які виникають з узагальнення найважливіших та повторювальних суспільних

відносин. Вона також слугує засобом усунення негативних суспільних практик; 2) нормотворчість є однією з форм діяльності публічної влади, поряд із іншими, такими як правозастосування, тлумачення права, контроль та нагляд; 3) основним результатом нормотворчості є прийняття нормативно-правових актів, які фіксують формальні норми права; 4) нормотворчість здійснюється компетентними суб'єктами - органами та представниками публічної влади; 5) нормотворчість підпорядкована певній процедурі, яка регулюється законодавством. Узагальнюючи О.В. Петришин вказує, що нормотворчість - це важливий етап у процесі створення правових актів, де визначені суб'єкти уповноважені для розробки та прийняття норм, і вона підкоряється конкретній правовій процедурі [151].

Специфічним випадком нормотворчості є законотворчість або законодавча діяльність, яка полягає у розробленні, прийнятті та введенні в дію компетентними нормативних актів вищої юридичної сили законів. Значення нормотворчості як форми протидії правопорушенням у фінансовій сфері обумовлене такими обставинами: по-перше, сама по собі зазначена протидія є видом правової діяльності, тобто її організації та здійснення повинні відбуватися на підставі, у порядку і межах визначених законодавством. Звісно різні заходи протидії вимагають різного ступеня їх правової регламентації: одні із них регулюються лише у загальному вигляді, інші – мають жорсткі законодавчі рамки, втім функціонування усього адміністративно-правового механізму досліджуваної протидії в цілому відбувається на відповідних організаційно-правових засадах; по-друге, неякісне, недосконале законодавство досить часто є тим фактором, який сприяє вчиненню особами правопорушень, оскільки вони знають як можна скористатися законодавчими недоліками у своїх корисних цілях і уникнути при цьому покарання. Головними заходами, які становлять зміст цієї форми є: аналіз діючого законодавства на предмет його відповідності наявному рівню розвитку фінансової сфери та відносин, що у ній відбуваються; виявлення у ньому (законодавстві) недоліків і прогалин; оновлення та

доповнення діючого законодавства, що здійснення внаслідок проходження складної процедури нормотворчості: ініціатива і підготовка проекту нормативного акту; внесення проекту нормативного акту суб'єкту нормотворення; розгляд та обговорення проекту нормативного акту; прийняття нормативного акту; введення нормативного акту в дію [34, с.486]

Таким чином, нормотворчість є надважливою формою реалізації інформаційної безпеки в Україні, адже саме за її допомогою вбачається можливим створити нормативно-правове підґрунтя для здійснення відповідної діяльності. А відтак, значення нормотворчості в розрізі представленої проблематики полягає у тому, що: по-перше, за її допомогою вбачається можливим виявити застарілі норми, які не відповідають викликам сучасності та, відповідно, вдосконалити їх зміст; по-друге, систематизувати законодавство у сфері інформаційної безпеки, що робить його більш простішим та зрозумілішим; по-третє, адаптувати відповідне нормативно-правове забезпечення до вимог та стандартів Європейського Союзу.

Із вказаною вище формою тісно пов'язана установча та правозастосовна форми. Установча діяльність, пише О.Ф. Скакун, - це правова форма діяльності держави, яка виражається в реалізації на основі норм матеріального права повноважень на формування, перетворення або скасування органів держави, їх структурних підрозділів, посад [145]. На нашу думку, установча форма забезпечення інформаційної безпеки спрямована на визначення найбільш важливих аспектів, необхідних для успішної організації функціонування досліджуваної системи, зокрема: 1) визначення кола суб'єктів, діяльність яких спрямована на забезпечення інформаційної безпеки, їх правового статусу, мети завдань та засад взаємодії; 2) перерозподіл відповідальності, створення відповідних підрозділів, визначення ролей та функцій управління інформаційною безпекою; 3) встановлення стандартів та процедур для забезпечення інформаційної безпеки, включаючи методи та технології для захисту інформації та процедури реагування на інциденти; 4) розкриття вимог до фахівців, які

відповідають за забезпечення інформаційної безпеки (рівень освіти, практичні уміння, навички тощо; 5) визначення фінансових та матеріальних ресурсів, які виділяються для реалізації заходів інформаційної безпеки.

І остання правова форма, якій ми приділимо увагу – правозастосовна. О.Ф. Скакун зазначає, що правозастосування - це владно-організуюча діяльність компетентних державних органів і посадових осіб, що здійснюється в процедурно-процесуальному порядку, яка полягає в індивідуалізації юридичних норм стосовно конкретних суб'єктів і конкретних життєвих випадків в акті застосування норм права [145, с.388–389]. Ознаками правозастосування, пише вчена, є: 1) має владний характер, тому що це діяльність компетентного органу або посадової особи, і лише в рамках наданих йому (їй) повноважень; 2) має індивідуалізований, персоніфікований характер, тому що являє собою вирішення конкретної справи, життєвого випадку, певної правової ситуації на основі норм права; 3) має процедурно-процесуальний характер, тому що являє собою офіційний порядок дій, складається з низки стадій; 4) має творчий, інтелектуальний характер, тому що це завжди інтелектуальна діяльність. Для застосування норм права необхідно свідомо проводити низку дій; 5) здійснюється на основі норм права; 6) має юридична оформлений характер — завершується ухваленням спеціального акта (у більшості випадків письмового), який називається актом застосування норм права або правозастосовним актом; 7) у своїй результативній частині (правозастосовний акт) завжди відіграє роль юридичного факту, який породжує, змінює або припиняє конкретні правовідносини (наприклад, вступ до шлюбу, розлучення подружжя, усиновлення дитини) [145, с.390]. В. Г. Лихолоб відмічає, що застосування норм права – це по суті діяльність державних органів, а також деяких уповноважених державою громадських організацій, що здійснюють у межах наданих їм повноважень державно-владну діяльність з індивідуального регулювання поведінки учасників соціального життя через наділення їх правами та обов'язками або вирішення їхніх спорів з іншими особами та

організаціями [63, с. 167].

Отже, правозастосування представляє собою найбільш гнучку та дієву складову у системі забезпечення реалізації прав. Ця складова не лише надає можливість оперативно вивчати потреби суспільства, але й формувати їх в формі, яка прийнятна для законодавців. У процесі правозастосування спостерігається вплив соціально-політичних факторів, що дозволяє суб'єктам правозастосування відчувати, сприймати, оцінювати та узагальнювати їх для інших учасників суспільства. Особливість правозастосування полягає в тому, що воно є конкретним видом соціальної діяльності, що відбувається в межах правових норм і впливає на суспільні відносини, регулюючи їх. Соціальні фактори, як рушійні сили та джерело правозастосування, також мають соціальний характер за своєю природою [43].

Тож, правозастосування, як форма забезпечення інформаційної безпеки, представляє собою процес забезпечення та виконання нормативно-правових приписів, шляхом надання спеціально уповноваженим суб’єктам повноважень (набору суб'єктивних прав та юридичних обов’язків), діяльність яких спрямована на вирішення питань, пов’язаних із створенням умов конфіденційності, цілісності та доступності інформації, а також на захистом інформаційних ресурсів та персональних даних фізичних та юридичних осіб, органів державної влади, тощо.

Наступну групу форм реалізації інформаційної безпеки складують організаційно-управлінські. Організація як діяльність має два аспекти: це, по-перше, діяльність щодо побудови та вдосконалення структури будь-якої соціальної системи (наприклад, органів внутрішніх справ) і, по-друге, діяльність щодо втілення в життя управлінських рішень. Другий аспект може бути охарактеризований як складова частина процесу управління (управлінського циклу). Крім того, поняття «організація» часто застосовується як рівнозначне поняттю «управління». Це обумовлено не тільки тим, що організація виконання управлінського рішення є центральним робочим елементом управлінського циклу, але й тим, що організаційні

моменти буквально пронизують усю діяльність щодо управління. Навіть висунення управлінських гіпотез підчас необхідно організовувати, не кажучи вже про збирання інформації, контроль та облік. Тому прийнято вважати, що управління саме по собі потребує організації. Але при цьому слід розрізняти ці поняття, маючи на увазі, що перше, тобто управління, є ширшим за друге і включає його до свого складу [152, с.247–248; 75, с.737]. В свою чергу в узагальненому вигляді управління – це діяльність суб'єкта, що виявляється у цілеспрямованому, організуючому впливі на об'єкт управління, здійснюваному з метою приведення його у бажаний для суб'єкта стан. Управлінська система – це єдине ціле, що існує і розвивається внаслідок взаємодії його компонентів [48].

Тож, організаційно-управлінські форми забезпечення інформаційної безпеки представляють собою сукупність послідовних дій організаційного та управлінського характеру, які спрямовані на створення необхідних умов для протидії та запобіганню правопорушенням у сфері використання інформації. До відповідних форм, як вбачається, найбільш доцільно віднести наступні:

- проведення зборів (нарад). У найбільш загальному розумінні нарада – це форма організації спільної діяльності працівників одного або декількох підприємств, установ, організацій, підрозділів, груп, яких збирає керівник для обговорення того чи іншого питання, вироблення або прийняття рішення [27]. Тож, проведення нарад і зборів в контексті інформаційної безпеки в державі має велике значення для забезпечення надійного захисту конфіденційної інформації та безпеки державних інформаційних ресурсів. Ці зустрічі є ключовим інструментом для обговорення проблемних питань, пов'язаних з безпекою держави, та прийняття рішень, спрямованих на запобігання можливим загрозам та реагування на інциденти. Ці зустрічі дозволяють опрацювати перспективні напрямки покращення державної політики у відповідній сфері, норм чинного законодавства та необхідної інфраструктури.

- науково-практичні конференції. Наукова конференція – форма

організації наукової діяльності, при якій дослідники (не обов'язково вчені чи студенти) представляють і обговорюють свої роботи. Зазвичай заздалегідь (в інформаційному листі або стендовому оголошенні) повідомляється про тему, час і місце проведення конференції. Потім починається збір тез доповідей і іноді оргвнесків. За своїм статусом конференція займає проміжне положення між семінаром і конгресом. Науково-методична конференція – це ефективна форма залучення широких кіл керівників і фахівців органів державної влади, місцевого самоврядування, підприємств, установ і організацій, науковців до аналізу практики, узагальнення й поширення кращого досвіду державного управління й самоврядування, господарювання й економічної діяльності, створення теоретичних і методичних передумов для його впровадження [69]. Науково-практичні конференції є досить важливою формою забезпечення інформаційної безпеки. Сутність цих заходів полягає в об'єднанні фахівців, дослідників, представників державних органів та підприємств для обговорення актуальних питань інформаційної безпеки та обміну досвідом. Проведення відповідних заходів сприяє обміну знаннями та дослідницькими результатами, що сприяє підвищенню рівня освіченості учасників та підвищенню їхньої компетентності в галузі інформаційної безпеки. В процесі проведення конференцій науковці та практичні працівники мають можливість виявити та обговорити актуальні проблеми та виклики у сфері забезпечення інформаційної безпеки. В рамках таких заходів проводяться дискусії та аналізується практичний досвід, що сприяє знаходженню ефективних рішень для вирішення цих проблем.

- розробка прогнозів, програм у сфері забезпечення інформаційної безпеки. Взагалі, планування — це цілеспрямована інтелектуальна діяльність людей, що має на меті визначення цілей і завдань функціонування певних систем (підприємство, район, держава…) та шляхів і методів досягнення цих цілей і завдань. Тобто планування передбачає прийняття заздалегідь рішення про те, що робити, коли робити, хто і як буде робити, проектування бажаного майбутнього та ефективних шляхів його досягнення. Образно кажучи,

планування — це міст між нашим нинішнім становищем і тим, якого ми прагнемо [82]. Тож, розробка прогнозів і програм у сфері забезпечення інформаційної безпеки є фундаментальною діяльністю в контексті захисту інформації в сучасному світі. Її сутність полягає в тому, щоб систематично підходити до питань інформаційної безпеки, а саме: визначати потенційні загрози, аналізувати ризики та розробляти стратегії та програми, спрямовані на запобігання цим загрозам та забезпечення інформаційної безпеки. Прогнозування в цьому контексті дає можливість передбачити можливі ризики та загрози для інформаційної інфраструктури, а також визначити майбутні тенденції в інформаційних технологіях та загрозах, які можуть виникнути в результаті цих тенденцій. Цей аналіз допомагає розробити адекватні стратегії та програми забезпечення інформаційної безпеки. Саме за допомогою останніх вбачається можливим визначити місію та цілі в галузі інформаційної безпеки, а також способи досягнення цих цілей.

- матеріально-технічне забезпечення. Ця форма забезпечення охоплює надання необхідних ресурсів, обладнання та технологій для забезпечення надійності та безпеки інформації та інформаційних систем на національному рівні. Спеціалізоване обладнання та програмне забезпечення, яке використовується для захисту інформації, грає критичну роль у запобіганні, виявленні та вирішенні інформаційних загроз. Це включає в себе засоби шифрування, системи виявлення вторгнень, антивірусне програмне забезпечення, засоби аутентифікації та багато інших технологій. Матеріальне забезпечення також охоплює фізичні заходи безпеки, такі як контроль доступу до інформаційних об'єктів та захист фізичних приміщень, де зберігається важлива інформація.

- розробка та прийняття управлінських рішень. Управлінське рішення є вихідним і ключовим аспектом в організаційній діяльності кожного керівника. Ця точка зору дозволяє розглядати управлінське рішення як основний зміст процесу управління та важливий інструмент системного підходу до функціонування підприємства. Кожне підприємство відіграє

важливу роль в суспільстві, що означає, що приймаючи управлінське рішення, слід враховувати не лише економічні аспекти, але і комплекс соціальних, ідеологічних, моральних і інших відносин. Прийняття рішення є коренем управління. Своєчасне і обґрунтоване рішення сприяє збільшенню продуктивності, тоді як недоцільне або незадовільне рішення може знизити результативність діяльності. Відповідальність керівника за процес прийняття рішень є вкрай високою, особливо для державних посадовців. Керівник не повинен приймати поспішні або необґрунтовані рішення [9].

І останню групу форм реалізації інформаційної безпеки в Україні складають спеціальні, які включають інформаційний патронат; інформаційну кооперацію та інформаційне протиборство. Так, інформаційним патронатом називається форма забезпечення інформаційної безпеки з боку держави фізичних та юридичних осіб. Інформаційне забезпечення безпеки включає добування різноманітних відомостей про дестабілізуючі фактори та інформаційні загрози, обмін інформацією між органами управління та засобами системи інформаційної безпеки. Інформаційний захист здійснюється різними шляхами, а саме від прийняття законопроектів до вжиття оперативних заходів силами інформаційної безпеки в процесі розвідувальної, контррозвідувальної, оперативно-розшукової та оперативно-інформаційної діяльності [64].

Інформаційна кооперація - це форма співпраці, при якій різні особи, організації або держави об'єднують свої зусилля для обміну, надання або спільного використання інформації з метою досягнення спільних цілей або завдань. Ця співпраця може стосуватися різних аспектів, таких як обробка даних, обмін інформацією, спільні дослідження, розробка спільних проектів, вирішення проблем або забезпечення інформаційної підтримки в певних галузях або сферах діяльності. Інформаційна кооперація може мати місце на різних рівнях, включаючи міжнародний, національний, регіональний або місцевий рівні. Вона є важливим інструментом для обміну знаннями, досвідом та ресурсами, що допомагає вирішувати складні завдання та сприяє

розвитку спільних ініціатив у різних сферах, включаючи освіту, науку, технології, бізнес, культуру, медіа та багато інших. Інформаційна кооперація сприяє обміну інноваціями та спільному розвитку, що робить її важливим аспектом в сучасному світі, де доступ до інформації має вирішальне значення.

Інформаційне протиборство - це конфлікт або суперництво між різними сторонами, яке відбувається через використання інформаційних ресурсів та засобів з метою досягнення певних цілей або переваг. Ця форма протиборства може включати в себе розповсюдження дезінформації, кібератаки, маніпуляцію громадською думкою, шпигунство, психологічну війну та інші методи та техніки, спрямовані на здійснення впливу на інших у сфері використання інформації. Інформаційне протиборство може виникати як на міжнародному рівні, так і в межах держави, включаючи політичні, економічні, військові та соціокультурні аспекти. Ця форма протиборства стає все більш актуальною в епоху цифрових технологій та інтернету, оскільки інформаційний простір надає нові можливості для впливу на суспільство та держави. У цьому контексті, захист від інформаційного протиборства і кіберзагроз стає важливим аспектом національної та міжнародної безпеки.

Реалізація окреслених вище форм передбачає використання спеціального набору інструментів та засобів, які прийнято називати методами. З точки зору етимології «метод — це прийом чи система прийомів, що застосовуються в якій-небудь галузі діяльності» [18, с. 522]. У праві метод – це сукупністю прийомів та засобів, за допомогою яких упорядковуються суспільні відносини певного виду; специфічний спосіб владного впливу держави на суспільні відносини, здійснюваний за допомогою юридичних законів [47, с34]. Метод, доводить О.Ф. Скакун, – це шлях до визначеної мети. Вибір методу диктує об’єкт і предмет дослідження. Синонімом терміну «науковий метод» (у широкому його розумінні) є термін «науковий підхід», що означає принципову методологічну орієнтацію наукового дослідження [144, с. 28].

Таким чином, під методами реалізації інформаційної безпеки України найбільш доцільно розуміти сукупність визначених у нормах чинного законодавства механізмів, інструментів та засобів, які використовують в своїй діяльності спеціально-уповноважені суб’єкти задля досягнення кінцевої мети у відповідній сфері. До відповідних методів, як вбачається, найбільш доцільно віднести наступні:

- метод переконання. Переконання – це такий спосіб цілеспрямованого впливу на свідомість і поведінку учасників управлінських відносин, який проявляється в комплексі роз’яснювальних, рекомендаційних, виховних та заохочувальних заходів, що застосовуються з метою забезпечення правомірності їх поведінки, підвищення їх правосвідомості та законослухняності, зміцненню дисципліни та соціальної організованості, а також із метою профілактики правопорушень [23, с. 82].

- метод примусу. Примус – це застосування до певних осіб спеціальних заходів впливу з метою спонукати, змусити їх виконувати вимоги правових норм. Він може виступати у двох формах – як судовий та адміністративний (позасудовий) примус. Крім того, примус врегульовано нормами різних галузей права, тому він одночасно є правовим примусом (цивільно-правовим, дисциплінарним, адміністративним, кримінально-правовим) [1, с. 412].

Примус та переконання є загальними, базовими методами реалізації інформаційної безпеки в Україні. Втім, існують також методи спеціальні, до яких вбачається необхідним віднести наступні:

- шифрування даних - використання сучасних технологій шифрування для захисту конфіденційної інформації в державних і корпоративних мережах;

- аудит інформаційної безпеки. Це систематичний та об'єктивний процес оцінки інформаційних систем, процедур та політик, що впроваджуються в організації для забезпечення конфіденційності, цілісності та доступності інформації, а також ідентифікації потенційних загроз і ризиків

інформаційній безпеці. Аудит інформаційної безпеки включає в себе аналіз структури інформаційних систем, перевірку відповідності стандартам і нормативам, оцінку процесів управління ризиками та заходів забезпечення безпеки, а також розробку рекомендацій для поліпшення рівня інформаційної безпеки в організації. Аудит інформаційної безпеки допомагає ідентифікувати слабкі місця, визначити ризики та запропонувати заходи для зміцнення захисту інформації та запобігання можливим загрозам;

- кіберзахист, який передбачає розвиток і впровадження заходів з кіберзахисту для захисту державних і корпоративних інформаційних ресурсів від кібератак та загроз;
- управління доступом, що передбачає контроль доступу до інформації шляхом встановлення правил і обмежень щодо користувачів та працівників;
- інформаційна гігієна, яка включає навчання персоналу правилам безпеки в інтернеті, захисту паролів, уникнення соціальної інженерії тощо;
- моніторинг і виявлення загроз. Використання спеціалізованого програмного забезпечення для моніторингу та виявлення можливих загроз і кібератак;
- метод кризисного управління, що передбачає розробку та впровадження планів кризисного управління для реагування на інциденти і відновлення інформаційної інфраструктури.

Таким чином, саме наведені вище форми та методи відображають найбільш важливі практичні аспекти реалізації інформаційної безпеки в Україні. Так, якщо форми є зовнішнім проявом практичної діяльності спеціально уповноважених органів у відповідній сфері, то методи вказують які при цьому були використані інструменти. Втім, як суттєвий недолік варто відзначити, що окреслені нами форми та методи не віднайшли своє законодавче закріплення, а відтак, дана прогалина потребує усунення шляхом внесення змін та доповнень до чинного законодавства, норми якого регулюють питання забезпечення та реалізації інформаційної безпеки в

Україні.

Висновки до Розділу 2

Акцентовано увагу на тому, що засобами адміністративного права визначаються і регламентуються, перш за все, загальні матеріальні і процедурні засади організації та функціонування державної політики щодо забезпечення інформаційної безпеки. Саме за допомогою адміністративно-правових засобів і механізмів врегульовані такі питання як: правовий статус центральних та територіальних органів виконавчої влади, які у тій чи іншій мірі залучені до забезпечення реалізації інформаційної безпеки в Україні; концептуальні та стратегічні засади забезпечення й розвитку інформаційної безпеки; пріоритетні напрямки діяльності та взаємодії суб'єктів публічної влади з питань інформаційної безпеки, а також координація їх діяльності; процедури та заходи протидії загрозам і викликам інформаційній безпеці України як на внутрішньому, так і зовнішньому рівнях; адміністративна відповідальність за порушення інформаційного законодавства та порядок притягнення до нього. У свою чергу засобами регулювання інформаційного права врегульовані ті відносини, процеси, факти, які стосуються: форм і способів створення (виготовлення, виробництва) інформації, її накопичення, зберігання, режимів використання і розповсюдження; здійснення індивідуальними і колективними суб'єктами своїх інформаційних прав та обов'язків; здійснення спеціальними суб'єктами контролю за законністю в інформаційній сфері; формування інформаційної культури населення та проведення відповідної просвітницької діяльності. Поряд із адміністративним та інформаційним правом, засобами яких регулюється забезпечення реалізації інформаційної безпеки, слід відмітити і Конституційне право. Саме нормами останнього: визначається загальне правове поле, в межах якого відбувається реалізація зазначеної безпеки; встановлюються основоположні гарантії та пріоритети на яких ґрунтується суспільно-державне життя в цілому та його інформаційна сфера зокрема;

врегульовується правове становище суб'єктів загальної компетенції, які визначають організаційно-правові, ідеологічні, управлінські та інші основи держаної політики щодо забезпечення інформаційної безпеки.

Узагальнено, що правове регулювання забезпечення реалізації інформаційної безпеки є явищем комплексним і його не можна звести до засобів та (або) методів якоїсь окремої правової галузі, оскільки у механізмі цього забезпечення задіяна ціла низка суб'єктів різного рівня і статусу, а інструменти реалізації інформаційної безпеки мають і юридичний, і управлінський, і технічний, і культурний й інший характер, використання яких опосередковується правовідносинами, що мають як управлінську, так й іншу природу.

З'ясовано, що система суб'єктів забезпечення реалізації інформаційної безпеки являє собою складний механізм, тобто сукупність активних, взаємопов'язаних і взаємодіючих суб'єктів, що перебувають у певній ієрархії та виконують відведене їм функціональне призначення. Обсяги і характер компетенції зазначених суб'єктів у досліджуваній сфері різняться, залежно від того, є для них забезпечення реалізації інформаційної безпеки основним (одним із декількох основних) чи супутнім напрямом діяльності. До основних складових вище зазначеної системи суб'єктів належать такі: 1) суб'єкти загальної компетенції, до яких належать Верховна Рада України, Президент України, Кабінет Міністрів України, місцеві державні адміністрації, органи місцевого самоврядування; 2) суб'єкти забезпечення реалізації інформаційної безпеки України міжгалузевої компетенції (суди та органи прокуратури); 3) суб'єкти галузевої компетенції; 4) суб'єкти спеціальної компетенції (Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України та Служба безпеки України).

Відмічено, що суб'єкти загальної компетенції, здійснюють свій внесок у забезпечення реалізації інформаційної безпеки України наступним чином: а) формують загально правове поле, в якому відбувається реалізації інформаційної безпеки. Тобто саме суб'єкти загальної компетенції

визначають ті основоположні матеріально-правові та процедурні засади, на яких ґрунтується державна інформаційна політика та забезпечення інформаційної безпеки, як у державі в цілому, так і в окремих її регіонах; б) визначають концептуальні та стратегічні засади здійснення інформаційної безпеки на певний період з урахуванням чинних правових норм та принципів, а також реалій і потреб суспільного розвитку та забезпечення національної безпеки держави; в) визначають загальну програму дій та заходів, які необхідно реалізувати задля виконання відповідних концепцій і стратегій, та забезпечення інформаційної безпеки; г) здійснюють загальне управління механізмом забезпечення реалізації інформаційної безпеки, що передбачає: координацію діяльності підзвітних та (або) підпорядкованих органів і посадових осіб, уповноважених на реалізацію державної політики у сфері інформаційної безпеки; контроль за законністю та ефективністю їх роботи; розподіл завдань між зазначеними органами і посадовими особами та забезпечення їх необхідними матеріально-фінансовими ресурсами; визначення структури суб'єктів, які відповідальні за безпосереднє здійснення заходів із забезпечення інформаційної безпеки, а також призначення їх вищого керівництва.

Обґрунтовано, що суб'єкти спеціальної компетенції роблять найбільший внесок у питання безпосередньої реалізації державної політики у сфері інформаційної безпеки України, адже саме вони: займаються безпосереднім практичним втіленням тих рішень і заходів, які спрямовані на зміцнення стійкості національної інформаційної сфери; протидіють конкретним загрозам і викликам; мають найбільш повну та детальну інформацію про проблеми і недоліки правозастосовного, управлінського, матеріально-технічного, кадрового та іншого характеру, що виникають під час реалізації інформаційної безпеки.

Узагальнено, що на сьогодні в Україні створена та функціонує розгалужена і багаторівнева система суб'єктів забезпечення реалізації інформаційної безпеки. У середині цієї системи існує доволі чітке

розмежування компетенцій між зазначеними суб'єктами, кожен з яких виконує певний обсяг роботи орієнтованої на забезпечення зазначеної безпеки: одні визначать загальні правові засади і принципи її забезпечення, другі – концептуальні засади, стратегічні напрямки та пріоритети зміцнення і розвитку інформаційної безпеки; треті – розробляють програми реалізації зазначених концептуальних і стратегічних засад, визначають матеріальні і процедурні аспекти виконання закріплених правових засад і принципів з огляду на реалії і потреби сьогодення; четверті – контролюють та координують практичну реалізацію заходів інформаційної безпеки у відповідності до вимог законності та ключових засад державної політики у цій сфері, а також опікуються питаннями ресурсного забезпечення діяльності спрямованої на забезпечення інформаційної безпеки; п'яті – безпосередньо на практиці виконують конкретні заходи правового, організаційного, технічного та іншого характеру, спрямовані на протидію загрозам інформаційній безпеці України, зміцнення стійкості національного інформаційного простору, захист прав і законних інтересів його індивідуальних та колективних учасників, зокрема держави і суспільства в цілому. Особлива роль у цьому аспекті забезпечення реалізації інформаційної безпеки відводиться Службі безпеки України, яка має здійснювати комплекс заходів, що передбачають протидію ворожому впливу і агресії в інформаційному середовищі як шляхом відбиття атак, так і через здійснення активних атакуючих дій, спрямованих на ліквідацію чи пригнічення ворожих інформаційних ресурсів та інфраструктури, що забезпечує їх функціонування.

Доведено, що форми реалізації інформаційної безпеки України представляють собою зовнішній прояв практичної діяльності спеціально уповноважених суб'єктів, яка спрямована на створення правових та організаційних умов для забезпечення конфіденційності, цілісності та доступності інформації, а також на захист інформаційних ресурсів від несанкціонованого доступу, втрати, зміни, руйнування або розголошення.

Зауважено, що в юридичній літературі сформовано не так багато підходів щодо переліку відповідних форм. Тож, вказані форми запропоновано поділити на три великі групи: 1) нормативно-правові; 2) організаційно-управлінські; та 3) спеціальні форми, що властиві саме для реалізації інформаційної безпеки.

Аргументовано, що нормотворчість є надважливою формою реалізації інформаційної безпеки в Україні, адже саме за її допомогою вбачається можливим створити нормативно-правове підґрунтя для здійснення відповідної діяльності. А відтак, значення нормотворчості в розрізі представленої проблематики полягає у тому, що: по-перше, за її допомогою вбачається можливим виявити застарілі норми, які не відповідають викликам сучасності та, відповідно, вдосконалити їх зміст; по-друге, систематизувати законодавство у сфері інформаційної безпеки, що робить його більш простішим та зрозумілішим; по-третє, адаптувати відповідне нормативно-правове забезпечення до вимог та стандартів Європейського Союзу.

Встановлено, що установча форма забезпечення інформаційної безпеки спрямована на визначення найбільш важливих аспектів, необхідних для успішної організації функціонування досліджуваної системи, зокрема: 1) визначення кола суб’єктів, діяльність яких спрямована на забезпечення інформаційної безпеки, їх правового статусу, мети завдань та засад взаємодії; 2) перерозподіл відповідальності, створення відповідних підрозділів, визначення ролей та функцій управління інформаційною безпекою; 3) встановлення стандартів та процедур для забезпечення інформаційної безпеки, включаючи методи та технології для захисту інформації та процедури реагування на інциденти; 4) розкриття вимог до фахівців, які відповідають за забезпечення інформаційної безпеки (рівень освіти, практичні уміння, навички тощо; 5) визначення фінансових та матеріальних ресурсів, які виділяються для реалізації заходів інформаційної безпеки.

Констатовано, що правозастосування, як форма забезпечення інформаційної безпеки, представляє собою процес забезпечення та виконання

нормативно-правових приписів, шляхом надання спеціально уповноваженим суб’єктам повноважень (набору суб'єктивних прав та юридичних обов’язків), діяльність яких спрямована на вирішення питань, пов’язаних із створенням умов конфіденційності, цілісності та доступності інформації, а також на захистом інформаційних ресурсів та персональних даних фізичних та юридичних осіб, органів державної влади

Підкреслено, що науково-практичні конференції є досить важливою формою забезпечення інформаційної безпеки. Сутність цих заходів полягає в об'єднанні фахівців, дослідників, представників державних органів та підприємств для обговорення актуальних питань інформаційної безпеки та обміну досвідом. Проведення відповідних заходів сприяє обміну знаннями та дослідницькими результатами, що сприяє підвищенню рівня освіченості учасників та підвищенню їхньої компетентності в галузі інформаційної безпеки. В процесі проведення конференцій науковці та практичні працівники мають можливість виявити та обговорити актуальні проблеми та виклики у сфері забезпечення інформаційної безпеки. В рамках таких заходів проводяться дискусії та аналізується практичний досвід, що сприяє знаходженню ефективних рішень для вирішення цих проблем.

Наголошено, що розробка прогнозів і програм у сфері забезпечення інформаційної безпеки є фундаментальною діяльністю в контексті захисту інформації в сучасному світі. Її сутність полягає в тому, щоб систематично підходити до питань інформаційної безпеки, а саме: визначати потенційні загрози, аналізувати ризики та розробляти стратегії та програми, спрямовані на запобігання цим загрозам та забезпечення інформаційної безпеки. Прогнозування в цьому контексті дає можливість передбачити можливі ризики та загрози для інформаційної інфраструктури, а також визначити майбутні тенденції в інформаційних технологіях та загрозах, які можуть виникнути в результаті цих тенденцій. Цей аналіз допомагає розробити адекватні стратегії та програми забезпечення інформаційної безпеки. Саме за

допомогою останніх вбачається можливим визначити місію та цілі в галузі інформаційної безпеки, а також способи досягнення цих цілей.

З’ясовано, що матеріально-технічне забезпечення охоплює надання необхідних ресурсів, обладнання та технологій для забезпечення надійності та безпеки інформації та інформаційних систем на національному рівні. Спеціалізоване обладнання та програмне забезпечення, яке використовується для захисту інформації, грає критичну роль у запобіганні, виявленні та вирішенні інформаційних загроз. Це включає в себе засоби шифрування, системи виявлення вторгнень, антивірусне програмне забезпечення, засоби аутентифікації та багато інших технологій. Матеріальне забезпечення також охоплює фізичні заходи безпеки, такі як контроль доступу до інформаційних об'єктів та захист фізичних приміщень, де зберігається важлива інформація.

Встановлено, що інформаційна кооперація - це форма співпраці, при якій різні особи, організації або держави об'єднують свої зусилля для обміну, надання або спільного використання інформації з метою досягнення спільних цілей або завдань. Ця співпраця може стосуватися різних аспектів, таких як: обробка даних, обмін інформацією, спільні дослідження, розробка спільних проектів, вирішення проблем або забезпечення інформаційної підтримки в певних галузях або сферах діяльності. Інформаційна кооперація може мати місце на різних рівнях, включаючи міжнародний, національний, регіональний або місцевий рівні. Вона є важливим інструментом для обміну знаннями, досвідом та ресурсами, що допомагає вирішувати складні завдання та сприяє розвитку спільних ініціатив у різних сферах, включаючи освіту, науку, технології, бізнес, культуру, медіа та багато інших. Інформаційна кооперація сприяє обміну інноваціями та спільному розвитку, що робить її важливим аспектом в сучасному світі, де доступ до інформації має вирішальне значення.

Узагальнено, що інформаційне протиборство - це конфлікт або суперництво між різними сторонами, яке відбувається через використання інформаційних ресурсів та засобів з метою досягнення певних цілей або

переваг. Ця форма протиборства може включати в себе розповсюдження дезінформації, кібератаки, маніпуляцію громадською думкою, шпигунство, психологічну війну та інші методи та техніки, спрямовані на здійснення впливу на інших у сфері використання інформації. Інформаційне протиборство може виникати як на міжнародному рівні, так і в межах держави, включаючи політичні, економічні, військові та соціокультурні аспекти. Ця форма протиборства стає все більш актуальною в епоху цифрових технологій та інтернету, оскільки інформаційний простір надає нові можливості для впливу на суспільство та держави. У цьому контексті, захист від інформаційного протиборства і кіберзагроз стає важливим аспектом національної та міжнародної безпеки.

Доведено, що під методами реалізації інформаційної безпеки України найбільш доцільно розуміти сукупність визначених у нормах чинного законодавства механізмів, інструментів та засобів, які використовують в своїй діяльності спеціально-уповноважені суб’єкти задля досягнення кінцевої мети у відповідній сфері.

Відмічено, що примус та переконання є загальними, базовими методами реалізації інформаційної безпеки в Україні. Втім, існують також методи спеціальні, до яких вбачається необхідним віднести наступні: шифрування даних - використання сучасних технологій шифрування для захисту конфіденційної інформації в державних і корпоративних мережах; аудит інформаційної безпеки. Це систематичний та об'єктивний процес оцінки інформаційних систем, процедур та політик, що впроваджуються в організації для забезпечення конфіденційності, цілісності та доступності інформації, а також ідентифікації потенційних загроз і ризиків інформаційній безпеці. Аудит інформаційної безпеки включає в себе аналіз структури інформаційних систем, перевірку відповідності стандартам і нормативам, оцінку процесів управління ризиками та заходів забезпечення безпеки, а також розробку рекомендацій для поліпшення рівня інформаційної безпеки в організації. Аудит інформаційної безпеки допомагає ідентифікувати слабкі

місця, визначити ризики та запропонувати заходи для зміцнення захисту інформації та запобігання можливим загрозам; кіберзахист, який передбачає розвиток і впровадження заходів з кіберзахисту для захисту державних і корпоративних інформаційних ресурсів від кібератак та загроз; управління доступом, що передбачає контроль доступу до інформації шляхом встановлення правил і обмежень щодо користувачів та працівників; інформаційна гігієна, яка включає навчання персоналу правилам безпеки в інтернеті, захисту паролів, уникнення соціальної інженерії тощо; моніторинг і виявлення загроз. Використання спеціалізованого програмного забезпечення для моніторингу та виявлення можливих загроз і кібератак; метод кризисного управління, що передбачає розробку та впровадження планів кризисного управління для реагування на інциденти і відновлення інформаційної інфраструктури.

Узагальнено, саме наведені вище форми та методи відображають найбільш важливі практичні аспекти реалізації інформаційної безпеки в Україні. Так, якщо форми є зовнішнім проявом практичної діяльності спеціально уповноважених органів у відповідній сфері, то методи вказують які при цьому були використані інструменти. Втім, як суттєвий недолік варто відзначити, що окреслені нами форми та методи не віднайшли своє законодавче закріплення, а відтак, дана прогалина потребує усунення шляхом внесення змін та доповнень до чинного законодавства, норми якого регулюють питання забезпечення та реалізації інформаційної безпеки в Україні.

РОЗДІЛ 3.
ШЛЯХИ ВДОСКОНАЛЕННЯ ОРГАНІЗАЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

3.1 Міжнародний досвід правового регулювання забезпечення реалізації інформаційної безпеки та можливості його використання в Україні.

Забезпечення інформаційної безпеки у всіх сферах суспільного життя, особливо в умовах сьогодення, є важливим та надскладним викликом для будь-якої сучасної держави, і Україна у даному контексті не є виключенням. Втім, технологічний прогрес по-різному торкнувся різних держав, а відтак і механізми забезпечення реалізації інформаційної безпеки також відрізняються одне від одного. З огляду на це, для українського законодавця важливим є вивчення позитивного зарубіжного досвіду, запровадження якого дозволить якісно покращити правові та організаційні засади забезпечення реалізації інформаційної безпеки в реаліях, яких опинилась наша країна сьогодні.

В даному контексті в першу чергу слід приділити увагу Сполученим Штатам Америки, адже ця країна є однією із найбільш могутніх політичних, економічних, технологічних і військових акторів сучасних міжнародних відносин. Внаслідок активного використання інформаційних технологій США раніше за інші країни зіткнулися із негативними наслідками інформаційних загроз. Виявилися потенційно вразливі місця інформаційної сфери, а саме: небезпечний когнітивний вплив у негативній конотації з боку певних засобів масової інформації та соціальних мереж на суспільну думку всередині країни, а також прогалини у сфері захисту персональних даних, державних та приватних комп’ютерних мереж. Сполученим Штатам бракує наявності єдиної візії в контексті протиборства інформаційним атакам та

рішучості у реалізації політики інформаційної безпеки, а сучасні загрози та виклики, такі як постійні міжпартійні суперечки, російське втручання та вплив коронавірусної інфекції COVID-19, не наближають американців до цього [158]. Як результат, у США була створена система державного регулювання в сфері інформаційної діяльності, яка сприяє ефективному використанню сучасних інформаційних технологій для прискорення розвитку американської економіки [22].

За останні десятиліття у США сформувалася чітка й доволі ефективна система забезпечення інформаційної безпеки, що вибудовувалася в декілька етапів. Дослідники сходяться на думці, що пороговими серед них можна вважати декілька. У 1981 р. інформаційна безпека стає пріоритетом урядової політики США. У 1987 р. встановлено нову категорію інформації – «несекретна, але важлива з погляду національної безпеки». У 1992 р. інформаційна безпека зводиться в ранг національної інформаційної політики, особливу увагу звернено на глобальну інформаційну політику, а в обігу уряду США з'являється поняття «інформаційна війна». У 2001 р. формується поняття «міжнародна інформаційна безпека» і визнається, що незахищеність інформаційних ресурсів становить загрозу всьому світу. Поняття «інформаційна війна» в адміністрації президента за пріоритетністю – на другому місці (після тероризму). У 2009 р. цифрову інфраструктуру США оголошують стратегічною національною цінністю, а її захист – національним пріоритетом. У 2011 р. хакерські атаки прирівнюють до оголошення війни. З 2015 р. законодавче регулювання кіберпростору виходить на перший план політики США. Хоча подекуди й надалі мають місце факти недооцінки зовнішніх ризиків і загроз у сфері інформаційної безпеки (особливо при президенстві Д. Трампа, американське суспільство на них активно реагує і відносно швидко усуває. Саме тому ця система постійно розвивається та еволюціонує, а США продовжує залишатися світовим лідером у розбудові ефективної системи забезпечення інформаційної безпеки держави [79].

Тож, законодавство США про інформаційну безпеку є досить широким та складається із низки нормативно-правових актів. Серед останніх найбільш доцільно виділити наступні: 1) Закон «Про кіберзахист інфраструктури критичної важливості» (Cybersecurity Information Sharing Act - CISA), норми якого спрямовані на забезпечення обміну інформацією про кіберзагрози між публічним та приватним секторами з метою покращення кіберзахисту критично важливих інфраструктурних об'єктів; 2) Закон «Про кіберзахист критичних інфраструктур інформаційних технологій» (Cybersecurity and Infrastructure Security Agency Act - CISA Act), що визначає функції та повноваження Агентства з кіберзахисту і інфраструктурної безпеки (CISA); 3) Закон «Про кіберзахист інформації» (Cybersecurity Act of 2015), норм якого спрямовані на регулювання діяльності Федеральних агентств і CISA додаткові повноваження щодо захисту інформації та інфраструктури в урядовому секторі; 4) Закон «Про захист особистих даних» (Privacy Act). Регулює збір, збереження та використання особистої інформації громадян США федеральними агентствами; 5) Закон «Про кіберзахист стандартів» (Federal Information Security Modernization Act - FISMA); 6) Закон «Про використання інформаційних технологій у федеральних агентствах» (Federal Information Technology Acquisition Reform Act - FITARA). Закон призначений для покращення управління та нагляду за проектами інформатизації в урядовому секторі. 7) Закон «Про захист електронної комунікації» (Electronic Communications Privacy Act - ECPA): Регулює урядовий доступ до електронних комунікацій та електронних даних.

Варто звернути увагу на те, що чинним законодавством США досить багато уваги приділяється встановленню вимог щодо федеральних IT-систем. Так, до прикладу:

- Закон про електронний уряд 2002 року (публічний закон 107-347) спрямований на забезпечення конфіденційності під час здійснення федеральної інформаційної діяльності. Розділ 208 закону конкретно вимагає

від агентств проводити оцінку впливу на конфіденційність електронних інформаційних систем;

- Федеральний закон про управління інформаційною безпекою 2002 року (розділ III публічного права 107-347) встановлює методи безпеки для федеральних комп'ютерних систем і, серед інших положень щодо системної безпеки, вимагає від агенцій проводити періодичну оцінку ризику та масштабів шкоди, яка може бути завдана, що є результатом несанкціонованого доступу, використання, розголошення, порушення, модифікації або знищення інформації та інформаційних систем, які підтримують операції та активи агентства та стосуються безпеки інформації протягом життєвого циклу кожної інформаційної системи агентства;

- Циркуляр OMB A-130 Додаток III «Безпека федеральних автоматизованих інформаційних ресурсів», який вимагає від федеральних агенцій впровадження та підтримки програми для забезпечення належного захисту всієї інформації агенцій, яку збирають, обробляють, передають, зберігають або поширюють у загальних системах підтримки та основні додатки та переглядайте засоби безпеки в кожній системі, коли в систему вносяться значні зміни, але принаймні кожні три роки [164].

В розрізі представленої проблематики слід звернути увагу на те, що у березні 2023 року Білий дім опублікував нову Національну стратегію кібербезпеки США. Ця стратегія визнає міцну співпрацю, особливо між державним і приватним секторами секторах, що має важливе значення для безпеки кіберпростору. Відповідальність за кібербезпеку лягла на окремих користувачів і невеликі організації [70]. У Стратегії висвітлюються дії Міністерства оборони щодо інвестування та забезпечення захисту, доступності, надійності та стійкості кібермереж та інфраструктури для підтримки агентств, які не належать до Міністерства оборони, зокрема у виконанні їхніх пов'язаних функцій і захисту оборонної промислової бази. На відміну від попередніх ітерацій, Стратегія зобов'язується підвищити колективну кіберстійкість США шляхом розбудови кіберспроможності

союзників і партнерів. Це також відображає підхід департаменту до захисту батьківщини через кібердомен, а також пріоритетність інтеграції кіберможливостей у наші традиційні бойові можливості [70].

Таким чином, забезпечення інформаційної безпеки в США має глибокі коріння. У XX столітті, ця держава відіграли ключову роль у розвитку інформаційних технологій, що дозволило їм бути «першопрохідниками» у боротьбі з інформаційними загрозами. А відтак, саме США була однією із перших країн, яка розробила державну політику і систему державного регулювання в інформаційній сфері. На сьогоднішній день ця система забезпечує ефективне використання інформаційних технологій для прискорення розвитку американської економіки, а також забезпечує національну безпеку через контроль і захист важливих інформаційних інфраструктур. США також здійснюють великі інвестиції у дослідження та розвиток нових технологій для захисту від кібератак та інших загроз. Проте, в умовах постійного розвитку технологій і появи нових загроз і викликів, завдання щодо забезпечення інформаційної безпеки ніколи не закінчується. США продовжують працювати над посиленням своєї інформаційної безпеки та адаптувати свою стратегію до сучасних реалій, звертаючи увагу на нові виклики, такі як кіберзлочини та дезінформація. У цілому, Сполучені Штати Америки мають значний досвід і великі ресурси для забезпечення інформаційної безпеки, проте вони залишаються у відкритому стані для подальшого розвитку та удосконалення у цій важливій сфері.

Ще одна країна Північної Америки, якій ми приділимо увагу, - Канада. Канадська економіка значною мірою розраховує на Інтернет: у 2007 році обсяги продажів через мережу склали 62,7 мільярди доларів, і 87% канадських компаній використовували Інтернет для здійснення своєї комерційної діяльності. Канадські підприємства швидко інтегрували в свою роботу сучасні цифрові технології, включаючи нове покоління мобільних пристроїв. Уряд Канади також стає більш відомий залежним від Інтернет-послуг і надає громадянам понад 130 різних послуг у цифровій формі, таких

як подання податкових декларацій, страхових заявок на зайнятість, кредитних заявок і багато інших. Успішне виступ Канади в кіберпросторі розглядається як один із найбільших національних активів, і захист цієї кіберсистеми від шкідливих атак та інших руйнівних дій є завданням великої складності [163; 24].

У Канаді з 1946 року існує Центр безпеки комунікацій (Communications Security Establishment, CSEC), який є однією з 12 спецслужб країни та функціонує під егідою Міністерства національної оборони і має свою штаб-квартиру в Оттаві. Ця організація відповідає за здійснення зовнішньої радіоелектронної розвідки, забезпечення захисту електронних інформаційних мереж уряду та проведення криптографічних досліджень. У початку 2008 року відповідно до федеральної програми ідентичності урядових органів Канади, федеральні агентства включили слово «Канада» у свою назву, і таким чином Центр безпеки комунікацій отримав назву Центр безпеки комунікацій Канади (Communications Security Establishment Canada). CSEC відіграє унікальну роль у канадському розвідувальному співтоваристві, зосереджуючи свою роботу на сферах шифрування та криптоаналізу, а також на забезпеченні інформаційної безпеки урядових структур Канади. Крім цього, він виконує функції радіоелектронної розвідки. Організація також надає технічну та оперативну підтримку Королівській канадській кінній поліції та іншим федеральним правоохоронним органам та силовим структурам, включаючи Канадську берегову охорону та Канадську адміністрацію безпеки повітряного транспорту [65].

На сьогодні ключовими нормативно-правовими актами, які спрямовані на регулювання забезпечення інформаційної безпеки у Канаді є наступними:

1. Закон «Про кіберзахист» (Cybersecurity Act). Цей закон був прийнятий в 2020 році і створює рамку для регулювання кібербезпеки в Канаді. Він надає владі більше повноважень для захисту кіберінфраструктури та боротьби з кіберзагрозами.

2. Закон «Про захист інформації особистості» (Personal Information Protection and Electronic Documents Act - PIPEDA). Вказаний нормативно-правовий акт спрямовано на регулювання збору, збереження та обробку особистих даних в комерційних організаціях і федеральних установах.

3. Закон «Про захист інформації в сфері охорони здоров'я» (Personal Health Information Protection Act), який регулює збереження і обробку медичних даних та інформації про здоров'я пацієнтів.

4. Закон «Про електронний підпис» (Electronic Commerce Act). Цей закон регулює використання електронних підписів та цифрових ідентифікаторів в електронних транзакціях.

5. Закон «Про кіберзлочини» (Computer Crime Act), що визначає види кіберзлочинів та відповідальність за них.

6. Закон «Про національний кіберзахист» (National Cybersecurity Act). Цей закон надає федеральному уряду повноваження щодо кіберзахисту критичних інфраструктур та реагування на кіберзагрози.

Ці закони створюють правову базу для захисту інформаційної безпеки та кібербезпеки в Канаді. Вони визначають вимоги до кіберзахисту, захисту особистих даних і заходи для боротьби з кіберзлочинами. Важливе місце в системі відповідних нормативних джерел займає Стратегія кібербезпеки Канади. Остання є лише одним з елементів в серії ініціатив, спрямованих на захист національних інтересів. Уряд створив канадський «КІБЕРЦЕНТР» реагування на інциденти, який здатний контролювати і забезпечувати пом'якшення кіберзагроз, надавати консультації та координувати національні заходи у відповідь на будь-які загрози кібербезпеки. Влада Канади вносять зміни в законодавство, модернізують повноваження правоохоронних органів і забезпечують порядок, при якому технологічні інновації не зможуть застосовуватися з метою ухилення від законодавчого контролю над діями злочинної спрямованості в мережі [24].

Таким чином, забезпечення інформаційної безпеки в Канаді визначається як один із найважливіших аспектів національної безпеки та

економічного розвитку. Ця країна відзначається високим рівнем залученості до використання сучасних інформаційних технологій у різних сферах, включаючи бізнес, урядову діяльність та громадянські послуги. Центр безпеки комунікацій Канади (CSEC) відіграє ключову роль у забезпеченні країни важливими функціями, включаючи зовнішню радіоелектронну розвідку, захист урядових інформаційних мереж, криптографію та радіоелектронну розвідку. Організація також надає підтримку федеральним правоохоронним структурам та агентствам, що важливо для забезпечення національної безпеки. Втім, зростаючий обсяг послуг та інформації, які надаються електронним шляхом, вказує на необхідність постійного розвитку та підвищення рівня інформаційної безпеки. Канада постійно адаптує свою стратегію та інфраструктуру до зростаючих загроз, включаючи кіберзлочини та кібератаки. Важливим чинником успіху в цій сфері є забезпечення захисту не лише урядових органів, але й громадянського сектору, оскільки ефективний захист інформації має вирішальне значення для усіх аспектів суспільного та економічного життя. Отже, Канада постійно вдосконалює свої механізми забезпечення інформаційної безпеки, розпізнаючи її важливість для суверенітету, національної безпеки та стабільності суспільства. Захист інформації та інформаційних ресурсів є пріоритетом і здійснюється через співпрацю урядових та неурядових структур, а також за участі громадськості та бізнесу.

Переходячи до аналізу досвіду країн Європи в першу чергу слід приділити увагу Великобританії. Великобританія (потенціал якої у сфері кіберзахисту вважається одним з найпотужніших) все ще розбудовує власні сили безпеки у кіберпросторі. З 2010 року у повноцінному режимі функціонує Оперативний центр з кібербезпеки (20 співробітників) з метою координації вже існуючих різноманітних центрів із кібербезпеки різних відомств та створення майданчика для співпраці між урядом та приватним сектором із проблем кібербезпеки. Крім того, у Великобританії ефективно функціонує Командування урядових комунікацій (Government

Communications Headquarters), що забезпечує як захист критично важливої урядової інформації, так і отримання розвідувальних даних за допомогою новітніх комунікативних засобів [56].

До ключових законодавчих актів Великобританії у сфері забезпечення інформаційної безпеки найбільш доцільно віднести наступні:

1) Закон «Про мережу та інформаційну безпеку» 2016 року (Network and Information Systems (NIS) Regulations 2018). Вказаний нормативний акт спрямований на виконання Європейської директиви NIS і встановлює вимоги до кібербезпеки для операторів критичних інфраструктур та постачальників цифрових послуг.

2) Закон «Про кіберзлочинність» 2015 року (Computer Misuse Act 1990, amended in 2015): Цей закон криміналізує незаконний доступ до комп'ютерних систем, комп'ютерне шахрайство та інші кіберзлочини.

3) Закон «Про даних та захист особистої інформації» (Data Protection Act). Цей закон регулює збір та обробку особистих даних і впроваджує загальний регламент з захисту даних ЄС (GDPR).

4) Закон «Про засоби ведення розслідувань і кримінальні провадження» 2000 року (Regulation of Investigatory Powers Act - RIPA), який визначає повноваження урядових агентств щодо ведення розслідувань та нагляду за електронними комунікаціями.

5) Закон «Про кіберзахист» 2013 року (Cyber Security Act 2013), що спрямований на посилення заходів з кібербезпеки та забезпечення кіберзахисту інформаційних систем та мереж.

6) Закон «Про інформаційну безпеку» 2019 року (Information Security Act 2019), котрий регулює кібербезпеку в урядовому секторі та встановлює вимоги до захисту інформації.

Ці закони і нормативні акти створюють основу для захисту інформаційної безпеки та кібербезпеки в Великобританії, регулюють діяльність у сфері кіберзахисту, та надають інструменти для боротьби з

кіберзлочинами та забезпечення захисту особистих даних та інформаційних ресурсів.

Основним документом Великої Британії, який регулює питання національної безпеки, є Стратегія національної безпеки 2010 року, яка відома як «Сильна Британія в епоху невизначеності». Цей стратегічний документ визначає 16 найсерйозніших загроз для країни. Згідно цієї стратегії, основними пріоритетами визнані заходи в галузі інформаційної безпеки та боротьба з тероризмом, яким виділено «перший рівень» важливості. Документ виділяє кібератаки, які можуть бути здійснені державами, злочинцями та екстремістськими групами, як одну з найактуальніших загроз. Кібершпигунство, терористичні атаки на енергетичні, газові та водопостачальні системи, а також злочини в інтернеті розглядаються як найсерйозніші загрози. Уряд Великої Британії виділив додаткові фінансові ресурси для забезпечення відповідного рівня кібербезпеки, особливо для інфраструктури та військових об'єктів. Доктрина національної безпеки країни ґрунтується на новій концепції, яка поєднує готовність спеціальних служб у надзвичайних ситуаціях з активною участю звичайних громадян. Згідно з цією стратегією, громадяни повинні бути готові ефективно реагувати на широкий спектр потенційних загроз, включаючи природні катастрофи та терористичні акти [36].

Новітньою тенденцією у сфері кібербезпеки Великої Британії вважається державно-приватне партнерство як один з провідних механізмів попередження та мінімізації кіберзагроз для національної безпеки. Діяльність уряду щодо державно-приватного партнерства у сфері кібербезпеки, підкреслюється в експертному середовищі, полягає у залученні «приватного сектора до співпраці, просуванні інноваційних стартапів, координації інструментів забезпечення кібербезпеки, підтримці мереж фахівців з питань кібербезпеки». Можна стверджувати, що Велика Британія наразі характеризується високим рівнем розвитку національної системи кібербезпеки, що «забезпечується потужною стратегічною та законодавчою

базою, а також низкою практичних заходів, спрямованих на розбудову широкого партнерства між державними структурами, приватним сектором, науковими установами та громадянським суспільством» [83].

Уряд Великої Британії оприлюднив нову Рамкову програму для забезпечення національної стійкості, що відбулося 19 грудня 2022 року. Цей документ був розроблений у відповідності до зобов'язань уряду, визначених у звіті про Комплексний огляд безпеки, оборони, розвитку та зовнішньої політики, який був опублікований 16 березня 2021 року. Рамкова програма враховує зростаючу невизначеність в глобальному безпековому середовищі та спрямована на впровадження заходів до 2030 року. Документ включає в себе оновлені концепції та методику управління ризиками та плануванням на різних рівнях і передбачає посилення всебічної співпраці. Рамкова програма доповнює існуючі стратегічні документи Великої Британії в таких сферах, як енергетична безпека, кібербезпека, адаптація до зміни клімату, перехід до екологічно чистої енергії, безперебійність постачання критичних ресурсів та інші. У документі висвітлені покращені підходи до оцінки ризиків, розподілу обов'язків і відповідальності, підвищення звітності, розвитку партнерства, формування місцевих форумів стійкості, захисту вразливих груп населення, поширення необхідних знань і навичок, а також інвестування у зміцнення стійкості [73].

Отже, Велика Британія активно реагує на зростаючі загрози в кіберпросторі, враховуючи їх значущість для національної безпеки. Визнаючи актуальність кібератак як з боку інших країн, так і з боку злочинців і екстремістських груп, Велика Британія внесла значні зміни у свою стратегію забезпечення інформаційної безпеки. Основні аспекти цієї стратегії включають в себе покращені підходи до оцінки ризиків, розподілу обов'язків та відповідальності, а також поліпшення звітування. Велика Британія розглядає кібербезпеку як пріоритет і виділяє додаткові ресурси для захисту інфраструктури і важливих об'єктів, включаючи військові об'єкти. Поза питанням інформаційної безпеки Велика Британія також активно працює над

розвитком нових підходів до національної безпеки. Їхні заходи орієнтовані на співпрацю між спеціальними службами та звичайними громадянами, роблячи акцент на готовності реагувати на різні загрози, включаючи природні біди та терористичні події. У цілому, Велика Британія демонструє досить прогресивний підхід до забезпечення інформаційної безпеки, активно адаптуючи свої стратегії та заходи до змін в глобальному середовищі.

Далі в рамках представленої проблематики слід звернути увагу на досвід Німеччини. Німецьке розуміння інформаційної безпеки та інформаційної війни об'єднує дві сторони - наступальну і оборонну, з метою захисту національних інтересів. При визначенні небезпек, ризиків, викликів та загроз, німецьке уявлення розглядає окремо можливі дії з боку іноземних держав, відокремлюючи їх від неурядових об'єднань, злочинних співтовариств та фізичних осіб, таких як релігійні фанатики. За останніми подіями інтерес до проблеми військової електронної розвідки (ВЕРБ) зріс значно. Німецькі експерти вважають, що найближчими роками збільшиться вразливість економічної та політичної інфраструктури розвинутих країн внаслідок порушень у роботі інформаційних систем, спричинених застосуванням інформаційної зброї [36].

Німеччина має ряд законів, пов'язаних з інформаційною безпекою та кібербезпекою. До основних із них слід віднести:

1) Закон «Про кіберзахист» (Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, IT-Sicherheitsgesetz). Цей закон був прийнятий у 2015 році та поступово розширювався у наступні роки. Він встановлює вимоги щодо кіберзахисту критичних інфраструктур та постачальників цифрових послуг.

2) Закон «Про захист даних» (Bundesdatenschutzgesetz, BDSG). Цей закон регулює збір, обробку та збереження особистих даних і відповідає загальному регламенту щодо захисту даних ЄС (GDPR).

3) Закон «Про захист від кіберзлочинів» (Gesetz zur Verbesserung der Bekämpfung des Cybergroomings), який спрямований на боротьбу з кіберзлочинами, особливо в контексті кібершантажу та кібергрумінгу.

4) Закон «Про конфіденційність інформації» (Gesetz über die Verschlusssachen). Цей закон регулює захист класифікованої інформації та забезпечує конфіденційність урядових даних.

5) Закон «Про розширення повноважень Федерального офісу захисту конституції» (Gesetz zur Erweiterung der Befugnisse des Bundesamtes für Verfassungsschutz), норм якого спрямовані на врегулювання діяльності Федерального офісу захисту конституції і включає заходи щодо боротьби з екстремізмом і тероризмом в онлайн-середовищі.

Провідну роль у забезпеченні інформаційної безпеки Німеччини відіграє Федеральна служба інформаційної безпеки (BSI), адже Законом ФРН «Про посилення безпеки інформаційних систем» завдання щодо попередження й реагування на інциденти, викликані кібернетичними загрозами, управління й координація сил та засобів із захисту критичної інформаційної інфраструктури, зокрема, у взаємодії із приватним сектором, покладається саме на це відомство. BSI входить до Федерального міністерства внутрішніх справ, яке, серед інших функцій, забезпечує внутрішню безпеку і захист конституційного ладу Німеччини, здійснює боротьбу з тероризмом, екстремізмом, шпигунством і саботажем. Відповідно до Закону «Про Федеральне відомство безпеки інформаційних систем» BSI збирає та оцінює інформацію стосовно загроз кібербезпеці держави, виявляє нові типи кібератак, аналізує відповідні контрзаходи. Також на BSI у взаємодії з НАТО і ЄС покладається виконання наступних функцій: оцінка ризику впровадження інформаційних технологій; розробка критеріїв, методів і іспитових засобів для оцінки ступеня захищеності національних комунікаційних систем; перевірка ступеня захищеності інформаційних систем і видача відповідних сертифікатів; видача дозволів на впровадження інформаційних систем у важливі державні об’єкти; здійснення спеціальних

заходів безпеки інформаційного обміну в державних органах, поліції тощо; консультування представників промисловості з питань інформаційної безпеки. Крім того, відомство займається пропагандою необхідності забезпечення інформаційної безпеки [162].

В додаток до наведених моментів, необхідно відмітити, що Німеччина є однією з держав яка активно використовує переваги приватного сектору в процесі забезпечення державних відомств. Так, програма «Геркулес» є найбільшим в Європі спільним проектом державного і приватного секторів («Public-Private Partnerships»). Виконання програми в рамках відповідного договору між федеральним відомством з розробки та закупівлі озброєнь бундесверу і спільним підприємством «Information-stechnik GmbH». Ціллю останньої виступає впровадженням новітніх технологій, зокрема в сфері забезпечення інформаційної безпеки, у діяльність Міноборони Німеччини та Збройних Сил. Загалом, інноваційному забезпеченню діяльності Міноборони ФРН та ЗС цієї держави приділяється велика увага. В даний сектор постійно здійснюється впровадження нових інформаційних систем та технологій зв’язку, а також формується програмне забезпечення щодо їх захисту [55].

Таким чином, німецьке уявлення про інформаційну безпеку орієнтується на спільну наступальну та оборонну стратегію для захисту своїх національних інтересів. Це включає в себе ретельне вивчення можливих загроз і визначення відповідних дій щодо захисту інформації та критичних інфраструктур. Зокрема з позитивного боку варто відзначити той факт, що Німеччина активно реагує на зростаючі загрози в кіберпросторі. Держава визнає кібератаки, які можуть бути здійснені як державами, так і злочинцями, як одну з найбільших загроз для своєї національної безпеки. Ця увага до кібербезпеки виявляється в виділенні значних ресурсів на захист інфраструктури та важливих об'єктів. Крім того, важливим аспектом є розвиток нових стратегій національної безпеки, які покликані забезпечити співпрацю між спеціальними службами та громадянами, підкреслюючи

необхідність готовності відповідати на різноманітні загрози, включаючи природні катастрофи та терористичні акти.

І остання країна, досвіду якої ми приділимо увагу – Франція. В цій країні система державного регулювання забезпечення інформаційної безпеки є дещо схожою на німецьку. Фактично, захист інформаційної безпеки у Франції, здебільшого, звівся до забезпечення кібернетичної безпеки і безпеки даних Інтернет. В цілому, у правовій системі Франції сьогодні немає спеціальних правових актів, що регулюють роботу спеціалістів з різними видами інформації. Безпека державної таємниці гарантується кримінальним, а персональної інформації та комерційних таємниць - кримінальним, трудовим і цивільними кодексами [161].

Франція також має ряд законів, пов'язаних з інформаційною безпекою та кібербезпекою. Серед останніх слід виділити наступні:

1) Закон «Про кіберзахист» (Loi relative à la lutte contre le crime organisé, le terrorisme et leur financement, et comportant diverses dispositions relatives à la sécurité et aux libertés). Цей закон прийнято у 2016 році, він має на меті зміцнити заходи з кіберзахисту та боротьби з кіберзлочинністю.

2) Закон «Про захист персональних даних» (Loi Informatique et Libertés). Цей закон визначає правила збору, зберігання та обробки особистих даних та відповідні права громадян у цій сфері. Він був важливою частиною приведення французького законодавства у відповідність із загальним регламентом щодо захисту даних ЄС (GDPR).

3) Закон «Про інформаційну безпеку» (Loi sur la sécurité de l'information) - Цей закон спрямований на захист критичних інформаційних інфраструктур та діяльності, які можуть вплинути на національну безпеку Франції.

4) Закон «Про кіберзахист критичних інфраструктур» (Loi relative à la programmation militaire) - Цей закон визначає стратегію і заходи для кіберзахисту критичних інфраструктур, включаючи енергетичні, транспортні та інші об'єкти.

5) Закон «Про кіберзахист урядових систем» (Loi sur la sécurité des systèmes d'information).

Законом № 2005-493 від 19 травня 2005 року у Франції ратифіковано Конвенцію Ради Європи "Про кіберзлочинність", відповідно до якої комп'ютерні злочини класифікуються за двома напрямками: 1) інформаційні технології як засоби виконання незаконних дій (продажу контрафактних товарів, заборонених ліків, сутенерства, дитячої порнографії, незаконних фінансових махінацій тощо); 2) інформація як об'єкт злочину (несанкціонований доступ, порушення цілісності даних, махінації в платіжних системах та ін.) [36].

Інформаційна політика Франції є складовою державної стратегії розвитку країни, стратегії франкофонії та збереження національної самобутності й ідентичності, 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. Мета національної інформаційної політики Франції – становлення інформаційного суспільства, розвиток інформаційних супермагістралей (із забезпеченням франкомовності мереж), електронного ринку й банківської сфери, лібералізація комунікацій, оновлення інформаційного законодавства, стимулювання наукових досліджень у галузі інформаційного бізнесу, створення систем безпеки інформації та запобігання комп’ютерним злочинам. Проте спектр інформаційних послуг і політика обмежень для зарубіжних інформаційних ТНК (8 % присутності у французькому інформаційному просторі, обов’язковий переклад аудіо-, відео- та кінопродукції або титрування французькою мовою), державний контроль інформаційної діяльності й монополія держави в застосуванні високих технологій не сприяють лідерству країни у європейському регіоні [136].

Підбиваючи підсумок представленого підрозділу дисертаційного дослідження слід узагальнити, що на сьогоднішній день всі провідні держави

Європи та Світу прагнуть створити належні правові та організаційні умови для забезпечення інформаційної безпеки. А відтак, з позитивного боку слід виділити наступний зарубіжний досвід, який варто використати вітчизняному законодавцю в рамках вдосконалення правового регулювання забезпечення реалізації інформаційної безпеки в українських реаліях:

- по-перше, вбачається необхідним значно розширити нормативно-правовому базу шляхом прийняття ряду законодавчих актів, наприклад, законів, спрямованих на регулювання кіберзахисту урядових систем, критичних інфраструктур, тощо;
- по-друге, в окремих країнах, зокрема США, суттєва увага приділяється підготовці фахівців, що будуть здійснювати діяльність у сфері забезпечення інформаційної безпеки;
- по-третє, значний рівень фінансового забезпечення урядових програм, спрямованих на якісне покращення інформаційної безпеки в державі;
- по-четверте, розширення співпраці не тільки між різними органами державної влади, а й іншими недержавними суб'єктами, зокрема фахівцями з ІТ-сфери, а також іншими підприємствами, організаціями, які здійснюють свою діяльність у галузі інформаційних технологій;
- по-п'яте, в переважній більшості країн існують просунуті Стратегії кібербезпеки, які постійно оновлюються та враховують виклики сучасності.

3.2. Напрямки вдосконалення організаційно-правового забезпечення реалізації інформаційної безпеки України.

Проведений у попередніх підрозділах дисертаційного дослідження аналіз, а також узагальнення позитивного зарубіжного досвіду, дає змогу констатувати, що на сьогоднішній день в Україні наявною є низка проблем

правового та організаційного характеру у сфері забезпечення реалізації інформаційної безпеки. А відтак, важливим напрямком діяльності законодавця та вітчизняних науковців, є вдосконалення: по-перше, чинного законодавство, норми якого спрямовані на регулювання суспільних відносин у відповідній сфері; по-друге, організаційних засад реалізації діяльності у галузі забезпечення інформаційної безпеки.

Так, в першу чергу приділимо увагу покращенню системи чинного законодавства у даній сфері. Взагалі, законодавство є способом визначення та організації правових норм через правові акти. Проте, система законодавства це не просто набір таких актів. Це впорядкована система, побудована на принципах підпорядкування та узгодження її структурних компонентів. Якщо у системі права основним елементом є правило, то в системі законодавства основним елементом є нормативно-правовий акт. Система законодавства є упорядкованою залежно від різних об'єктивних критеріїв і виникає у відповідь на потреби соціального регулювання суспільства. Це включає в себе різні нормативні акти, що формуються з метою максимально ефективного використання правових норм [74]. Варто навести точку зору О.Ф. Скакун, яка вказує, що система законодавства представляє собою комплекс правових норм із законів, розподілених за галузями та інститутами права відповідно до предмета і методу правового регулювання. Вказана вище авторка виділяє декілька основних ознак системи законодавства: включає в себе основну частину правової системи і має зовнішню форму вираження; надає юридичну силу нормам права, які сформувалися в суспільстві; виражає норми права через первинні елементи, які розташовані у статтях законів; має ієрархічну (вертикальну) та рівнозначну (горизонтальну) будову; має суб'єктивний характер, оскільки включає в себе права та обов'язки суб'єктів права; має структуру, яка охоплює галузі та інститути законодавства. У підсумку О.Ф. Скакун зазначає, що основну роль у системі законодавства відіграють нормативні акти та їх структурні компоненти. Вони дозволяють групувати окремі розділи, статті та пункти нормативних актів за вмістом

правових норм, які вони містять, у більш стійкі форми, такі як інститути законодавства. Стаття закону виступає зовнішньою формою вираження правового змісту, який сконцентрований у правовому приписі [143].

Таким чином, законодавство у сфері забезпечення реалізації інформаційної безпеки України представляє собою системну сукупність нормативно-правових актів різної юридичної сили, норми яких спрямовані на врегулювання суспільних відносин у відповідній сфері. З огляду на запропоноване визначення, а також наведені вище наукові позиції, цілком справедливим буде говорити про те, що недосконаліть законодавства у досліджуваній галузі обумовлена наявністю прогалин у ньому, тобто відсутністю необхідних норм та/або їх недосконалим змістом. О.Ф. Скакун стверджує, що прогалини у законодавстві виникають, коли в чинних законодавчих актах повністю або частково відсутні необхідні юридичні норми, які, відповідно до принципів права, мають регулювати конкретні суспільні відносини. Окрім того, вчена зазначає, що причинами виникнення таких прогалин в законодавстві можуть бути: необдуманість включення всієї різноманітності сучасних життєвих ситуацій у нормативні акти, які потребують правового регулювання та можуть бути врегульовані правом; відставання нормотворчості від розвитку суспільних відносин, оскільки не завжди можливо передбачити появу нових життєвих ситуацій; наявність деформацій у процесі нормотворчості, що може бути наслідком лобіювання голосування в парламенті в інтересах певних бізнесових груп; технічні помилки законодавця, які можуть бути допущені при розробці нормативних актів та використанні прийомів юридичної техніки [143]. М.В. Цвік вказує на те, що прогалина в законодавстві представляє собою відсутність правового регулювання певних суспільних відносин, які повинні бути врегульовані відповідно до принципів права. Важливо розуміти, що прогалина може існувати навіть у тих випадках, коли відносини належать до сфери правового регулювання, але їх не було враховано в законодавчих актах, хоча вони мали б бути врегульовані. Науковець дійшов висновку, що існують різні причини

виникнення прогалин. Це стосується як первинних прогалин, які виникають через недоврахування багатоманітності життєвих ситуацій при формулюванні нормативних актів, так і наступних прогалин, які виникають через постійний розвиток суспільних відносин і виникнення нових життєвих ситуацій, які було неможливо передбачити заздалегідь. Оскільки повністю уникнути прогалин у законодавстві неможливо, то важливо знайти способи їх оперативного усунення чи заповнення, щоб забезпечити правову консистентність та дослідити засоби для їх подолання [37; 58].

Отже, наявність прогалин в законодавстві, норми якого спрямовані на регулювання забезпечення інформаційної безпеки не є явищем критичним та невирішуваним. Окрім того, в умовах сьогодення, коли інформаційні технології активно розвиваються, наявність вказаних прогалин є явищем об'єктивним та цілком зрозумілим. Варто зауважити, що на законодавчому рівні досить багато уваги приділяється проблемі інформаційної безпеки, підтвердженням чому є низка прийнятих стратегічних та концептуальних документів, яким ми приділяли увагу раніше. Втім незважаючи на це, прийняті документи не дали можливість вирішити всіх наявних проблем у відповідній сфері, підтвердженням чого є низки наукових поглядів на цю проблематику.

Так, до прикладу, А.І. Марущак цілком обґрунтовано зазначає, що інформаційна безпека є актуальним об'єктом дослідження юридичної науки. Сучасний стан відносин, що виникають з приводу реалізації законних прав та інтересів особи, суспільства, держави в інформаційній сфері, потребує оновлення і відповідного закріплення напрямів дослідження теоретико-правових питань забезпечення інформаційної безпеки. Перспективами подальших досліджень у цьому напрямі є розкриття основних понять та категорій для їх використання при розробці прикладних проблем інформаційної безпеки. Адже саме розмежування основних понять у цій сфері, їх уніфіковане застосування у процесі нормотворчої діяльності сприятиме однозначному розумінню основних завдань забезпечення

інформаційної безпеки особи, суспільства, держави. А це, в свою чергу, підвищуватиме ефективність практичної діяльності суб’єктів забезпечення інформаційної безпеки [66].

О. А. Панченко акцентує увагу на проблемах теоретичного характеру, які заважають нормальному функціонуванню сфери забезпечення інформаційної безпеки. Зокрема, на слушну думку вченого, проблемою є те, що чинне законодавство України не містить відповідного розгорнутого тлумачення поняття «інформаційна безпека держави», проте нормативні акти, які торкаються питань інформаційної безпеки, закономірно розглядають її в контексті більш загального поняття національної безпеки. Такий підхід значно обмежує та звужує зміст категорії «інформаційна безпека держави», позаяк виключно інформаційний простір слугує каналом реалізації загроз національній безпеці в усіх сферах діяльності держави [77]. Окрім того, важливим аспектом є те, що автором було здійснено комплексний підхід до визначення стратегії розвитку системи інформаційної безпеки в умовах глобалізації. Цей підхід об'єднує декілька ключових складових, таких як джерела захисту інформації, високий технічний та нормативно-правовий рівень забезпечення, а також професійну компетенцію державних службовців. Важливим аспектом цього підходу є стратегічне управління, спрямоване на аналіз імовірних успіхів і загроз, здатність вчасно виявляти потребу в змінах, які відповідають викликам з навколишнього середовища, а також сприяють інноваційним перевагам і їх гнучкому впровадженню. Це дозволяє створити довгострокові перспективи розвитку. Отже, цей підхід спрямований на створення захищеного середовища для особистості та функціонування інформаційного простору, яке об'єднує різні засоби захисту інформації у єдину інтегровану систему. Важливою перевагою такого підходу є можливість гарантувати певний рівень безпеки та надійності захисту інформації [76]. Далі О.А. Панченко відмічає, що основою ефективної організації та реалізації державної інформаційної політики є створення єдиного інформаційного простору України та її інтеграція у світовий

інформаційний простір. Важливі аспекти включають забезпечення інформаційної безпеки для особистості, суспільства та держави, формування демократично орієнтованої масової свідомості, розвиток галузі інформаційних послуг та розширення правового регулювання суспільних відносин, зокрема пов'язаних із отриманням, розповсюдженням та використанням інформації. Це сприятиме зміцненню зв'язків між центром і регіонами та збільшить цілісність країни [76].

У своєму науковому дослідженні Я.І. Чмирь дійшов до висновку, що Однією з ключових проблем, пов'язаних із забезпеченням інформаційної безпеки системи публічного управління, є відсутність чіткого визначення поняття «інформаційна безпека» (подібну думку також висловлює О.А. Панченко). Крім того, відмічає науковець, іншою суттєвою проблемою є відсутність ефективного механізму для функціонування системи електронного урядування. Третім важливим аспектом є розвиток інноваційних інформаційних загроз, які вимагають негайного та результативного вирішення. Додатково, підкреслює автор, необхідно звернути увагу на питання підготовки кваліфікованого персоналу для системи публічного управління у галузі інформаційної безпеки та відсутність ефективних механізмів для забезпечення інформаційної безпеки. Не останнім аспектом є відсутність інституцій, які можуть комплексно забезпечити систему інформаційної безпеки у публічному управлінні [156].

М.В. Саврук у своєму дослідженні ретельно розглядає проблеми, пов'язані із забезпеченням інформаційної безпеки України. Він звертає увагу на кілька ключових аспектів: недостатня якість іноземної теле-, радіо- та друкованої продукції в Україні; зниження наукового потенціалу у галузі інформатизації, телекомунікацій та зв'язку; зростання мовної проблеми; розповсюдження в світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України в зовнішній політиці; відставання вітчизняних наукоємних та високотехнологічних галузей, зокрема у сфері комп'ютерно-

телекомунікаційних засобів і технологій; запізнення України у впровадженні інформатизації соціогуманітарної сфери, особливо в системі освіти, охорони здоров'я, соціального забезпечення та культурних послуг; розголошення інформації, яка становить державну та іншу таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на задоволення потреб і національних інтересів суспільства і держави [137]. У підсумку, автор наголошує на необхідності впровадження послідовної державної інформаційної політики, залученні значних інвестицій і внесенні змін у суспільну свідомість для розв'язання цих проблем в інформаційній сфері України. Україна, як держава, має приділяти особливу увагу забезпеченню ефективної політики інформаційної безпеки, запобіганню інформаційній залежності, інформаційній експансії з боку інших держав та міжнародних структур, а також інтеграції України в світовий інформаційний простір.

Таким чином, аналіз наведених вище наукових позицій дає змогу констатувати, що переважна більшість із теоретичних розробок: по-перше, втратили свою актуальність, оскільки були написані ще до повномасштабного вторгнення, а відтак вони не враховують всю специфіку сучасної інформаційної війни, яка наразі відбувається у медійному просторі; по-друге, переважна більшість робіт спрямована на покращення саме організаційного забезпечення інформаційної безпеки, в той час я покращенню норм чинного законодавства увага приділялась досить поверхнево. Тож, ми, спираючись на аналіз наукових поглядів вчених, а також норм чинного законодавства, вважаємо, що перспективними напрямами вдосконалення правового регулювання інформаційної безпеки України є наступні:

1) Розробка нової «Стратегії інформаційної безпеки України», адже незважаючи на те, що попередня Стратегія була прийнята у 2021 році і розрахована до 2025 року, перші півроку повномасштабної війни показали, що нашій державі досить складно протистояти зовнішньому ворогу. Втім, далі ситуація змінювалось у кращий бік і Україна отримала перевагу. А

відтак, розроблення нової Стратегії буде здійснюватись з урахуванням набутого досвіду, та враховуючи сучасні виклики та загрози;

2) Вбачається необхідною розробка ряду законодавчих актів у сфері забезпечення інформаційної безпеки. Як показав зарубіжний досвід, в більшості розвинутих держав законодавство у відповідній сфері є досить широким та охоплює різні сфері суспільного життя. З огляду на це, вбачається необхідним розробити та прийняти Закони України: «Про захист інформації в сфері охорони здоров'я»; «Про електронний підпис»; «Про мережу та інформаційну безпеку»; «Про кіберзахист критичних інфраструктур»; «Про кіберзахист урядових систем». Прийняття вказаних нормативно-правових актів, як вбачається: а) розширить сфери забезпечення інформаційної безпеки; б)створить сприятливі умови для захисту інформації в окремих важливих галузях, наприклад, діяльності уряду, а також критичних інфраструктур;

3) Необхідно розробити підзаконний нормативно-правовий акт «Про порядок взаємодії суб’єктів забезпечення інформаційної безпеки». Останній має бути спрямовано на визначення правових та організаційних засад здійснення діяльності спеціально уповноважених суб’єктів у досліджуваній сфері.

Разом із тим, покращення правового регулювання не може здійснюватись поза вдосконаленням організаційних засад забезпечення інформаційної безпеки в Україні. В даному контексті, перш за все, необхідно покращити кадрове забезпечення галузі реалізації інформаційної безпеки. М.В Мельничук відмічає той факт, що кадрове забезпечення слід розглядати у двох аспектах. З одного боку, це наявність підконтрольних об'єктів, які виконують завдання, необхідні для підготовки та реалізації управлінських рішень. З іншого боку, кадрове забезпечення - це суб'єкти управлінської діяльності, які організовують, аналізують, контролюють, координують та виконують інші завдання, щоб досягти конкретних результатів в сфері державного управління. Ефективність роботи органу виконавчої влади

залежить не лише від матеріального забезпечення, але й від вольових дій та переконань учасників державного управління, спрямованих на досягнення конкретних цілей. Без високого професіоналізму та належних особистих якостей кадрів важко забезпечити ефективність управлінської діяльності, яка визначає динаміку роботи органу виконавчої влади [67, с.68].

Н.В. Прижиналінська визначає кадрове забезпечення - це комплекс заходів, спрямованих на пошук, оцінку і установлення заздалегідь передбачених трудових відносин, як для розвитку кар'єри на самому підприємстві, так і для залучення нових працівників як тимчасових, так і постійних співробітників. Цей процес включає в себе керування підприємством, планування, організацію персоналу, аналіз відносин з управління, забезпечення умов праці та розвиток кадрового потенціалу. З точки зору керування персоналом кадрове забезпечення може суттєво впливати на досягнення цілей підприємства, якщо всі елементи взаємодії з персоналом (набір, відбір, адаптація, розвиток кар'єри, оцінка результатів праці, сучасні методи мотивації і організації праці) об'єднані в єдину програму, що є невід'ємною частиною кадрової стратегії підприємства. У контексті формування кадрового резерву підприємства важливою є підготовка інноваційно налаштованих кадрів - кваліфікованих співробітників, які мають здатність до творчої праці, професійного розвитку та освоєння науково-інформаційних технологій. Це можливо завдяки розвитку системи безперервної освіти та навчання протягом життя [84].

Таким чином, кадрове забезпечення органів державної влади – це надважливий елемент забезпечення інформаційної безпеки в Україні. Зазначене пояснюється тим, що тільки висококваліфікований та професійний персонал може якісно та ефективно виконувати надскладні завдання у досліджуваній сфері. На сьогоднішній день, нажаль, ми можемо констатувати суттєві проблеми у цій сфері, які пов’язані: по-перше, із зниженням якості освіти відповідних фахівців, що обумовлено військовим станом та поширенням дистанційного навчання; по-друге, постійним відтоком

професійних кадрів із України; по-третє, відсутністю державних механізмів до стимулювання праці даної категорії працівників.

А відтак, з метою вдосконалення кадрового забезпечення в розрізі реалізації інформаційної безпеки вбачається необхідним здійснити наступні кроки:

- по-перше, розробити ефективну систему навчання та перепідготовки кадрів у галузі інформаційної безпеки;
- по-друге, розвивати інноваційний інформаційний простір, де фахівці можуть розробляти та впроваджувати нові методи та технології інформаційної безпеки, а держава має фінансово та матеріально підтримувати відповідні дії;
- по-третє, підвищити рівень зацікавленості науковців у здійсненні науково-дослідної роботи у відповідній сфері, а також забезпечити та сприятиме співпраці між науковими установами;
- по-четверте, привертати увагу молоді до інформаційної галузі, що має бути реалізовано шляхом проведення різноманітних конкурсів;
- по-п’яте, розвивати міжнародну співпрацю з іншими країнами та міжнародними організаціями в сфері інформаційної безпеки для обміну досвідом та кращими практиками.
- по-шосте, важливим кроком, безумовно, має бути фінансове стимулювання фахівців здійснювати діяльність у напрямку забезпечення інформаційної безпеки саме у державному секторі. Адже наразі, кошти, які дані спеціалісти отримують у приватному секторі, є значно більшими.

Не менш важливим напрямком покращення організаційних засад є покращення інформаційного забезпечення суб’єктів, що реалізують свою діяльність у відповідному напрямку. Так, Г.І. Купалова пише, що інформаційне забезпечення – це система обробки даних з метою прийняття управлінських рішень. Воно охоплює різні сфери діяльності, такі як виробництво, продаж, обслуговування, поліпшення технологій виробництва, якість продукції, витрати, рекламу, інформацію про асортимент та ціни на

продукцію, організацію обслуговування та інше. Отже, інформаційне забезпечення є ключовим етапом та необхідною умовою для проведення економічного аналізу. Це пояснюється тим, що якість та зміст вихідних даних впливає на ефективність аналітичного дослідження та об'єктивність його результатів. Інформаційне забезпечення економічного аналізу включає створення бази даних і комплексу інструментів, необхідних для вивчення господарської діяльності та прийняття управлінських рішень [59; 57].

В рамках окресленого питання обов’язково навести точку зору Ю.О. Корнєва, який, узагальнюючи і критично оцінюючи опрацьовані наукові погляди щодо визначення поняття «інформаційне забезпечення», сформулював найбільш важливі характеристики окресленого терміну [53]: 1) інформаційне забезпечення є функціональним комплексом, що забезпечує органічну взаємодію технічних засобів, методів і технологій роботи з інформацією; 2) інформаційне забезпечення – це сукупність інформаційних ресурсів, засобів, методів і технологій, яка сприяє ефективній реалізації процесу управління; 3) інформаційне забезпечення є інструментом, що генерує інформацію, яка складається з важливих даних та не дає відволікатись керівникам на зайву та громіздку інформацію; 4) інформаційне забезпечення – це безперервний процес постійного забезпечення можливості збирання, пошуку, групування, аналізу, зберігання та поширення інформації серед працівників правоохоронних органів; 5) інформаційне забезпечення є інструментом, що забезпечує надходження інформації про стан та параметри функціонування певних об’єктів управління; 6) інформаційне забезпечення – це управлінська технологія, оскільки відображає інформацію щодо стану керованого об’єкта і є основою для прийняття управлінських рішень; 7) інформаційне забезпечення – специфічний вид професійної діяльності, оскільки враховує інформаційні потреби різних суб’єктів; 8) інформаційне забезпечення є складовою системи та процесу управління, виражаючи на міжсуб’єктивному рівні відносини [53, с.21].

Таким чином, інформаційне забезпечення - це процес, спрямований на забезпечення доступності, цілісності, конфіденційності та якості інформації, необхідної для ефективного функціонування організації або вирішення певних конкретних завдань. Цей процес включає збір, обробку, зберігання та розповсюдження інформації з метою задоволення потреб користувачів та досягнення стратегічних цілей організації. Окрім того, інформаційне забезпечення може включати розробку та підтримку інформаційних систем та технологій для оптимізації використання інформації в організаційному процесі.

Тож, вдосконалення інформаційного забезпечення в розрізі представленої проблематики має включати:

- покращення науково-методичного забезпечення, що в свою чергу має включати розвиток наукових досліджень у галузі інформаційної безпеки, включаючи аналіз і прогнозування загроз, розробку інструкцій та стандартів безпеки, а також навчання кадрів у досліджуваній галузі;
- оновлення та модернізацію інформаційних систем державних установ, що дозволить підвищити їх стійкість до кіберзагроз;
- створення інтегрованих інформаційних платформ для обміну даними, що сприятиме якісній взаємодії та координації спеціально уповноважених органів у відповідній сфері;
- розробку та впровадження стратегій та технічних рішень для збереження, захисту та резервного копіювання важливих державних даних та інформації;
- застосування сучасних технологій, таких як: штучний інтелект, машинне навчання та блокчейн;
- запровадження заходів для забезпечення стійкості та безпеки критичних інфраструктур, таких як енергетика, транспорт, комунікації тощо.

Специфіка сфери забезпечення інформаційної безпеки обумовлює необхідність вдосконалення матеріально-технічного забезпечення відповідної сфери. У найбільш загальному розумінні «матеріально-технічне

забезпечення» – це сукупність суспільних відносин, урегульованих нормативними актами або договорами по забезпеченню матеріально-технічними ресурсами, необхідними для своєчасного та безперебійного проведення циклу робіт з виробництва, переробки й реалізації продукції, а також для виконання економічних, соціальних та інших завдань з метою задоволення певних потреб [54, с.56]. Вдосконалення матеріально технічного забезпечення в розрізі представленої проблематики має включати: а) постійне оновлення комп'ютерних систем, що дозволить більш швидко виявляти порушення у відповідній та реагувати на них; б) покращення технічного забезпечення суб'єктів, до компетенції яких входить забезпечення інформаційної безпеки в державі; в) забезпечення надійності мережевих з'єднань, включаючи використання волоконно-оптичних ліній та інших передових технологій; г) встановлення резервних джерел живлення та систем автоматичного переходу на резервне живлення для унеможливлення зупинок через відключення електроенергії.

Із матеріально-технічним забезпеченням тісно пов'язане забезпечення фінансове. Взагалі, фінансове забезпечення - це формування цільових грошових фондів господарюючих суб'єктів у достатньому розмірі та їх ефективне використання. Воно здійснюється у таких формах: самофінансування (фінансування діяльності суб'єкта господарювання за рахунок власних фінансових ресурсів); бюджетне фінансування (надання коштів з бюджету на безповоротних засадах); кредитування (надання коштів на принципах поворотності, платності, терміновості, забезпеченості та цільового використання); оренда (передача майна у користування на визначений угодою термін і за певну плату); інвестування (вкладання коштів у певні об'єкти з метою отримання додаткового доходу) [149]. Тож, вдосконалення інформаційного забезпечення в розрізі реалізації інформаційної безпеки України має передбачати загальне підвищення рівня фінансування всіх аспектів реалізації відповідної діяльності. А відтак, важливим є загальне збільшення фінансування різних державних програм у

сфері забезпечення інформаційної безпеки, підвищення рівня фінансування спеціально уповноважених органів державної влади, а також підвищення матеріального стимулювання працівників, зайнятих у відповідній галузі.

Таким чином, вдосконалення організаційно-правового забезпечення реалізації інформаційної безпеки України має гармонічно поєднувати покращення норм чинного законодавства та організаційних засад здійснення відповідної діяльності. А відтак, запровадження запропонованих нами змін та доповнень, як вбачається, стане важливим кроком у напрямку покращення загального функціонування сфері інформаційної безпеки української держави та суспільства.

Висновки до розділу 3

Акцентовано увагу на тому, що забезпечення інформаційної безпеки у всіх сферах суспільного життя, особливо в умовах сьогодення, є важливим та надскладним викликом для будь-якої сучасної держави, і Україна у даному контексті не є виключенням. Втім, технологічний прогрес по-різному торкнувся різних держав, а відтак і механізми забезпечення реалізації інформаційної безпеки також відрізняються одне від одного. З огляду на це, для українського законодавця важливим є вивчення позитивного зарубіжного досвіду, запровадження якого дозволить якісно покращити правові та організаційні засади забезпечення реалізації інформаційної безпеки в реаліях, яких опинилась наша країна сьогодні.

Доведено, що забезпечення інформаційної безпеки в США має глибокі коріння. У XX столітті, ця держава відіграли ключову роль у розвитку інформаційних технологій, що дозволило їм бути «першопрохідниками» у боротьбі з інформаційними загрозами. А відтак, саме США була однією із перших країн, яка розробила державну політику і систему державного регулювання в інформаційній сфері. На сьогоднішній день ця система

забезпечує ефективне використання інформаційних технологій для прискорення розвитку американської економіки, а також забезпечує національну безпеку через контроль і захист важливих інформаційних інфраструктур. США також здійснюють великі інвестиції у дослідження та розвиток нових технологій для захисту від кібератак та інших загроз. Проте, в умовах постійного розвитку технологій і появи нових загроз і викликів, завдання щодо забезпечення інформаційної безпеки ніколи не закінчується. США продовжують працювати над посиленням своєї інформаційної безпеки та адаптувати свою стратегію до сучасних реалій, звертаючи увагу на нові виклики, такі як кіберзлочини та дезінформація. У цілому, Сполучені Штати Америки мають значний досвід і великі ресурси для забезпечення інформаційної безпеки, проте вони залишаються у відкритому стані для подальшого розвитку та удосконалення у цій важливій сфері.

Встановлено, що забезпечення інформаційної безпеки в Канаді визначається як один із найважливіших аспектів національної безпеки та економічного розвитку. Ця країна відзначається високим рівнем залученості до використання сучасних інформаційних технологій у різних сферах, включаючи бізнес, урядову діяльність та громадянські послуги. Центр безпеки комунікацій Канади (CSEC) відіграє ключову роль у забезпеченні країни важливими функціями, включаючи зовнішню радіоелектронну розвідку, захист урядових інформаційних мереж, криптографію та радіоелектронну розвідку. Організація також надає підтримку федеральним правоохоронним структурам та агентствам, що важливо для забезпечення національної безпеки. Втім, зростаючий обсяг послуг та інформації, які надаються електронним шляхом, вказує на необхідність постійного розвитку та підвищення рівня інформаційної безпеки. Канада постійно адаптує свою стратегію та інфраструктуру до зростаючих загроз, включаючи кіберзлочини та кібератаки. Важливим чинником успіху в цій сфері є забезпечення захисту не лише урядових органів, але й громадянського сектору, оскільки ефективний захист інформації має вирішальне значення для усіх аспектів

суспільного та економічного життя. Отже, Канада постійно вдосконалює свої механізми забезпечення інформаційної безпеки, розпізнаючи її важливість для суверенітету, національної безпеки та стабільності суспільства. Захист інформації та інформаційних ресурсів є пріоритетом і здійснюється через співпрацю урядових та неурядових структур, а також за участі громадськості та бізнесу.

Узагальнено, що на сьогоднішній день всі провідні держави Європи та Світу прагнуть створити належні правові та організаційні умови для забезпечення інформаційної безпеки. А відтак, з позитивного боку слід виділити наступний зарубіжний досвід, який варто використати вітчизняному законодавцю в рамках вдосконалення правового регулювання забезпечення реалізації інформаційної безпеки в українських реаліях: по-перше, вбачається необхідним значно розширити нормативно-правовому базу шляхом прийняття ряду законодавчих актів, наприклад, законів, спрямованих на регулювання кіберзахисту урядових систем, критичних інфраструктур, тощо; по-друге, в окремих країнах, зокрема США, суттєва увага приділяється підготовці фахівців, що будуть здійснювати діяльність у сфері забезпечення інформаційної безпеки; по-третє, значний рівень фінансового забезпечення урядових програм, спрямованих на якісне покращення інформаційної безпеки в державі; по-четверте, розширення співпраці не тільки між різними органами державної влади, а й іншими недержавними суб’єктами, зокрема фахівцями з IT-сфери, а також іншими підприємствами, організаціями, які здійснюють свою діяльність у галузі інформаційних технологій; по-п’яте, в переважній більшості країн існують просунуті Стратегії кібербезпеки, які постійно оновлюються та враховують виклики сучасності.

Відмічено, що законодавство у сфері забезпечення реалізації інформаційної безпеки України представляє собою системну сукупність нормативно-правових актів різної юридичної сили, норми яких спрямовані на врегулювання суспільних відносин у відповідній сфері. З огляду на запропоноване визначення, а також наведені вище наукові позиції, цілком

справедливим буде говорити про те, що недосконаліть законодавства у досліджуваній галузі обумовлена наявністю прогалин у ньому, тобто відсутністю необхідних норм та/або їх недосконалим змістом.

Доведено, що переважна більшість теоретичних розробок у сфері забезпечення реалізації інформаційної безпеки: по-перше, втратили свою актуальність, оскільки були написані ще до повномасштабного вторгнення, а відтак вони не враховують всю специфіку сучасної інформаційної війни, яка наразі відбувається у медійному просторі; по-друге, переважна більшість робіт спрямована на покращення саме організаційного забезпечення інформаційної безпеки, в той час я покращенню норм чинного законодавства увага приділялась досить поверхнево.

З’ясовано, що перспективними напрямами вдосконалення правового регулювання інформаційної безпеки України є наступні:

1) Розробка нової «Стратегії інформаційної безпеки України», адже незважаючи на те, що попередня Стратегія була прийнята у 2021 році і розрахована до 2025 року, перші півроку повномасштабної війни показали, що нашій державі досить складно протистояти зовнішньому ворогу. Втім, далі ситуація змінювалось у кращий бік і Україна отримала перевагу. А відтак, розроблення нової Стратегії буде здійснюватись з урахуванням набутого досвіду, та враховуючи сучасні виклики та загрози;

2) Вбачається необхідною розробка ряду законодавчих актів у сфері забезпечення інформаційної безпеки. Як показав зарубіжний досвід, в більшості розвинутих держав законодавство у відповідній сфері є досить широким та охоплює різні сфері суспільного життя. З огляду на це, вбачається необхідним розробити та прийняти Закони України: «Про захист інформації в сфері охорони здоров'я»; «Про електронний підпис»; «Про мережу та інформаційну безпеку»; «Про кіберзахист критичних інфраструктур»; «Про кіберзахист урядових систем». Прийняття вказаних нормативно-правових актів, як вбачається: а) розширить сфери забезпечення інформаційної безпеки; б)створить сприятливі умови для захисту інформації

в окремих важливих галузях, наприклад, діяльності уряду, а також критичних інфраструктур;

3) Необхідно розробити підзаконний нормативно-правовий акт «Про порядок взаємодії суб'єктів забезпечення інформаційної безпеки». Останній має бути спрямовано на визначення правових та організаційних засад здійснення діяльності спеціально уповноважених суб'єктів у досліджуваній сфері.

Встановлено, що кадрове забезпечення органів державної влади – це надважливий елемент забезпечення інформаційної безпеки в Україні. Зазначене пояснюється тим, що тільки висококваліфікований та професійний персонал може якісно та ефективно виконувати надскладні завдання у досліджуваній сфері. На сьогоднішній день, нажаль, ми можемо констатувати суттєві проблеми у цій сфері, які пов'язані: по-перше, із зниженням якості освіти відповідних фахівців, що обумовлено військовим станом та поширенням дистанційного навчання; по-друге, постійним відтоком професійних кадрів із України; по-третє, відсутністю державних механізмів до стимулювання праці даної категорії працівників.

З метою вдосконалення кадрового забезпечення в розрізі реалізації інформаційної безпеки запропоновано здійснити наступні кроки: по-перше, розробити ефективну систему навчання та перепідготовки кадрів у галузі інформаційної безпеки; по-друге, розвивати інноваційний інформаційний простір, де фахівці можуть розробляти та впроваджувати нові методи та технології інформаційної безпеки, а держава має фінансово та матеріально підтримувати відповідні дії; по-третє, підвищити рівень зацікавленості науковців у здійсненні науково-дослідної роботи у відповідній сфері, а також забезпечити та сприятиме співпраці між науковими установами; по-четверте, привертати увагу молоді до інформаційної галузі, що має бути реалізовано шляхом проведення різноманітних конкурсів; по-п'яте, розвивати міжнародну співпрацю з іншими країнами та міжнародними організаціями в сфері інформаційної безпеки для обміну досвідом та кращими практиками; по-

шосте, важливим кроком, безумовно, має бути фінансове стимулювання фахівців здійснювати діяльність у напрямку забезпечення інформаційної безпеки саме у державному секторі. Адже наразі, кошти, які дані спеціалісти отримують у приватному секторі, є значно більшими.

З'ясовано, що інформаційне забезпечення - це процес, спрямований на забезпечення доступності, цілісності, конфіденційності та якості інформації, необхідної для ефективного функціонування організації або вирішення певних конкретних завдань. Цей процес включає збір, обробку, зберігання та розповсюдження інформації з метою задоволення потреб користувачів та досягнення стратегічних цілей організації. Окрім того, інформаційне забезпечення може включати розробку та підтримку інформаційних систем та технологій для оптимізації використання інформації в організаційному процесі.

Аргументовано, що вдосконалення інформаційного забезпечення в розрізі представленої проблематики має включати: покращення науково-методичного забезпечення, що в свою чергу має включати розвиток наукових досліджень у галузі інформаційної безпеки, включаючи аналіз і прогнозування загроз, розробку інструкцій та стандартів безпеки, а також навчання кадрів у досліджуваній галузі; оновлення та модернізацію інформаційних систем державних установ, що дозволить підвищити їх стійкість до кіберзагроз; створення інтегрованих інформаційних платформ для обміну даними, що сприятиме якісній взаємодії та координації спеціально уповноважених органів у відповідній сфері; розробку та впровадження стратегій та технічних рішень для збереження, захисту та резервного копіювання важливих державних даних та інформації; застосування сучасних технологій, таких як: штучний інтелект, машинне навчання та блокчейн; запровадження заходів для забезпечення стійкості та безпеки критичних інфраструктур, таких як енергетика, транспорт, комунікації тощо.

Відмічено, що вдосконалення фінансового забезпечення в розрізі реалізації інформаційної безпеки України має передбачати загальне підвищення рівня фінансування всіх аспектів реалізації відповідної діяльності. А відтак, важливим є загальне збільшення фінансування різних державних програм у сфері забезпечення інформаційної безпеки, підвищення рівня фінансування спеціально уповноважених органів державної влади, а також матеріального стимулювання працівників, зайнятих у відповідній галузі.

ВИСНОВКИ

У висновках наведено теоретичне узагальнення та нове розв’язання наукового завдання, яке полягає у тому, щоб розкрити сутність та особливості організаційно-правових засад реалізації інформаційної безпеки України, на основі чого розробити пропозиції та рекомендації спрямовані на вдосконалення правових та організаційних засад здійснення відповідної діяльності. У результаті дослідження сформульовано низку нових наукових висновків, основні з них такі:

1. Виокремлено ключові етапи становлення та розвитку інформаційної безпеки України:

– перший етап (1990 – 1996 роки). На даному етапі відбувається визнання офіційною владою інформаційної сфери як окремої, самостійної і вкрай важливої галузі суспільного життя. Окрім того, в цей час закріплюється, що інформація та інформаційна діяльність не лише сприяють розвитку держави і суспільства, але можуть становити суттєву загрозу для їх інтересів;

– другий етап (1998 – 2006 роки), на якому було вперше з моменту проголошення незалежності України сформульовано та закріплено на офіційному рівні деякі концептуальні засади та програмні цілі і завдання забезпечення інформаційної безпеки в нашій державі;

– третій етап (2007 – 2014 роки). Даний етап характеризується тим, що в цей час було сформульоване і закріплено на законодавчому рівні поняття інформаційної безпеки; інформаційна безпека була віднесена до однієї із ключових і пріоритетних на даному етапі суспільного розвитку сфер державної політики; закріплено пріоритет національних інтересів у сфері інформаційної безпеки перед індивідуальними; визначено основні проблеми забезпечення інформаційної безпеки в Україні, а також засоби і шляхи їх усунення та подальшого удосконалення механізму інформаційної безпеки;

починають впроваджуватися міжнародні стандарти і норми протидії злочинній активності у інформаційному (зокрема кібернетичному) просторі;

– четвертий етап, який розпочався у 2014 році після російської агресії проти нашої держави і триває до теперішнього часу. Саме ця подія досить чітко вказала на те: що війна може бути не лише у вигляді збройного протистояння, але й інформаційною, а фронт, відповідно може бути як військовий, так й інформаційний; що інформаційний суверенітет – це не якесь абстрактне, а цілком реальне явище, від забезпечення якого залежать і державність, і територіальна цілісність, і національна ідентичність; що для того, щоб захистити національні інтереси недостатньо запровадити заходи протидії лише окремим проявам злочинної активності в інформаційній сфері, натомість має бути сформований цілісний, комплексний, дієвий механізм, який би дозволяв вчасно виявляти та ефективно протистояти інформаційним загрозам будь-якого характеру і масштабу.

2. З’ясовано, що ключовими напрямками забезпечення реалізації інформаційної безпеки України є: 1) ідеологічний; 2) нормативно-правовий; 3) організаційно-управлінський; 4) культурно-освітній; 5) налагодження ефективної, системної та систематичної внутрішньодержавної взаємодії та міжнародної співпраці з питань інформації та інформаційної безпеки; 6) інноваційний напрямок. Наголошено, що законодавець повинен здійснювати належне правове регулювання за всіма без винятку виокремленими напрямками забезпечення реалізації інформаційної безпеки.

3. Сучасний стан нормативно-правового регулювання забезпечення реалізації інформаційної безпеки України охарактеризовано як такий, що потребує подальшого вдосконалення, адже на сьогодні в нашій державі прийнято цілу низку нормативно-правових актів різної юридичної сили, які визначають концептуальні, матеріально-правові, процедурні аспекти реалізації зазначеної безпеки. Наразі інформаційна безпека на офіційному рівні визнана неодмінною і вкрай важливою складовою забезпечення національної, державної та воєнної безпеки держави, а нормативно-правові

засади механізму забезпечення реалізації безпосередньо самої інформаційної безпеки розраховані не лише на боротьбу із конкретними нагальними загрозами і небезпеками, а й на всебічне зміцнення і розвиток інформаційної сфери України з урахуванням як національних, так і міжнародних інтересів нашої держави. Наголошено на необхідності прийняття закону України «Про інформаційну безпеку України», який мав би стати стрижневим у системі нормативно-правових актів з питань інформаційної безпеки, і сприяти узгодженій та послідовній реалізації цієї безпеки.

4. Констатовано, що правове регулювання забезпечення реалізації інформаційної безпеки є явищем комплексним і його не можна звести до засобів та (або) методів якоїсь окремої галузі права. Зокрема за допомогою адміністративно-правових засобів і механізмів врегульовані такі питання як: адміністративно-правовий статус центральних та територіальних органів виконавчої влади, які у тій чи іншій мірі залучені до забезпечення реалізації інформаційної безпеки в Україні; концептуальні та стратегічні засади забезпечення й розвитку інформаційної безпеки; пріоритетні напрямки діяльності та взаємодії суб'єктів публічної влади з питань інформаційної безпеки, а також координація їх діяльності; процедури та заходи протидії загрозам і викликам у сфері інформаційної безпеки України як на внутрішньому, так і зовнішньому рівнях; адміністративна відповідальність за порушення інформаційного законодавства та порядок притягнення до адміністративної відповідальності. У свою чергу нормами інформаційного права врегульовані ті відносини, процеси, факти, які стосуються: форм і способів створення (виготовлення, виробництва) інформації, її накопичення, зберігання, режимів використання і розповсюдження; реалізації індивідуальними і колективними суб'єктами своїх інформаційних прав та обов'язків; формування інформаційної культури населення та проведення відповідної просвітницької діяльності. Акцентовано увагу, що поряд із нормами адміністративного та інформаційного права забезпечення

реалізації інформаційної безпеки врегульовано нормами і конституційного права. Саме нормами Конституції України: встановлено загальне правове поле, в межах якого відбувається реалізація зазначеної безпеки; закріплено основоположні гарантії та пріоритети на яких ґрунтується суспільно-державне життя в цілому та його інформаційна сфера зокрема; врегульовано правове становище суб'єктів загальної компетенції, які визначають організаційно-правові, ідеологічні, управлінські та інші основи державної політики щодо забезпечення інформаційної безпеки.

5. Обґрунтовано, що на сьогодні в Україні створена та функціонує розгалужена і багаторівнева система суб'єктів забезпечення реалізації інформаційної безпеки. Всередині цієї системи існує доволі чітке розмежування компетенцій між зазначеними суб'єктами, кожен з яких виконує певний обсяг роботи, орієнтованої на забезпечення зазначеної безпеки. Так одні визначать загальні правові засади і принципи її забезпечення, другі – концептуальні засади, стратегічні напрямки та пріоритети зміцнення і розвитку інформаційної безпеки;

треті – розробляють програми реалізації зазначених концептуальних і стратегічних засад, визначають матеріальні і процедурні аспекти виконання закріплених правових засад і принципів з огляду на реалії і потреби сьогодення; четверті – контролюють та координують практичну реалізацію заходів інформаційної безпеки у відповідності до вимог законності та ключових засад державної політики у цій сфері, а також опікуються питаннями ресурсного забезпечення діяльності, спрямованої на забезпечення інформаційної безпеки; п'яті – безпосередньо на практиці виконують конкретні заходи правового, організаційного, технічного та іншого характеру, спрямовані на протидію загрозам інформаційній безпеці України, зміцнення стійкості національного інформаційного простору, захист прав і законних інтересів його індивідуальних та колективних учасників, зокрема держави і суспільства в цілому. Наголошено, що особлива роль у сфері забезпечення реалізації інформаційної безпеки

відводиться Службі безпеки України, яка має здійснювати комплекс заходів, що передбачають протидію ворожому впливу і агресії в інформаційному середовищі як шляхом відбиття атак, так і через здійснення активних атакуючих дій, спрямованих на ліквідацію чи пригнічення ворожих інформаційних ресурсів та інфраструктури, що забезпечує їх функціонування.

6. Встановлено, що форми реалізації інформаційної безпеки України являють собою зовнішній прояв практичної діяльності спеціально уповноважених суб'єктів, яка спрямована на створення правових та організаційних умов для забезпечення конфіденційності, цілісності та доступності інформації, а також на захист інформаційних ресурсів від несанкціонованого доступу, втрати, зміни, руйнування або розголошення. Констатовано, що відповідні форми найбільш доцільно поділити на три групи: 1) нормативно-правові (нормотворча, установча та правозастосовна форми); 2) організаційно-управлінські (проведення зборів (нарад); науково-практичних конференцій; розробка прогнозів, програм у сфері забезпечення інформаційної безпеки; матеріально-технічне забезпечення); 3) спеціальні форми, що властиві саме для реалізації інформаційної безпеки (інформаційний патронат; інформаційна кооперація; інформаційне протиборство).

Під методами реалізації інформаційної безпеки України запропоновано розуміти сукупність визначених у нормах чинного законодавства механізмів, інструментів та засобів, які використовують в своїй діяльності спеціально-уповноважені суб'єкти задля досягнення кінцевої мети у відповідній сфері. Відповідні методи запропоновано поділити на дві групи: 1) загальні (переконання та примусу); та 2) спеціальні, зокрема: шифрування даних; аудит інформаційної безпеки; кіберзахист; управління доступом; інформаційна гігієна; моніторинг і виявлення загроз; метод кризового управління.

7. Узагальнено, що на сьогоднішній день всі провідні держави світу прагнуть створити належні правові та організаційні умови для забезпечення інформаційної безпеки. А відтак, з позитивного боку слід виділити такий зарубіжний досвід, який варто використати вітчизняному законодавцю в межах вдосконалення правового регулювання забезпечення реалізації інформаційної безпеки в українських реаліях: по-перше, вбачається необхідним значно розширити чинну нормативно-правову базу шляхом прийняття низки законодавчих актів, наприклад, законів, спрямованих на регулювання кіберзахисту урядових систем, критичних інфраструктур, тощо; по-друге, в окремих країнах, зокрема США, суттєва увага приділяється підготовці фахівців, що будуть здійснювати діяльність у сфері забезпечення інформаційної безпеки; по-третє, значний рівень фінансового забезпечення урядових програм, спрямованих на якісне покращення інформаційної безпеки в державі; по-четверте, розширення співпраці не тільки між різними органами державної влади, а й недержавними суб'єктами, зокрема фахівцями IT-сфери, а також іншими підприємствами, організаціями, які здійснюють свою діяльність у галузі інформаційних технологій; по-п'яте, в переважній більшості країн існують «просунуті» стратегії кібербезпеки, які постійно оновлюються та враховують виклики сучасності.

8. Обґрунтовано, що покращення забезпечення реалізації інформаційної безпеки України має здійснювати за двома ключовими напрямками:

1) вдосконалення законодавства у відповідній сфері, що має включати:

– розробку нової «Стратегії інформаційної безпеки України», адже незважаючи на те, що попередня Стратегія була прийнята у 2021 році і розрахована до 2025 року, перші півроку повномасштабної війни показали, що нашій державі досить складно протистояти зовнішньому ворогу. Втім, далі ситуація змінювалася у кращий бік і Україна отримала перевагу, а відтак, розроблення нової Стратегії буде здійснюватись з урахуванням набутого досвіду, та враховувати сучасні виклики та загрози;

– розробку та прийняття Законів України: «Про захист інформації в сфері охорони здоров'я»; «Про електронний підпис»; «Про мережу та інформаційну безпеку»; «Про кіберзахист критичних інфраструктур»; «Про кіберзахист урядових систем». Прийняття вказаних нормативно-правових актів дозволить: а) розширити сферу забезпечення інформаційної безпеки; б) створити сприятливі умови для захисту інформації в окремих важливих галузях, наприклад, діяльності уряду, а також критичних інфраструктур;

– розробити та прийняти «Порядок взаємодії суб'єктів забезпечення інформаційної безпеки», який має бути спрямовано на визначення правових та організаційних засад здійснення спільної діяльності спеціально уповноважених суб'єктів у досліджуваній сфері.

2) покращення організаційно-управлінських аспектів здійснення відповідної діяльності, що має включати вдосконалення: а) кадрового забезпечення суб'єктів, що реалізують свою діяльність у напрямку реалізації інформаційної безпеки; б) системи інформаційного забезпечення; в) фінансового та матеріально-технічного забезпечення інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Авер'янов В. Б. Адміністративне право України : академічний курс : у 2 т. / Авер'янов В. Б. / ред. кол. : В. Б. Авер'янов (голова). К. : Вид-во «Юридична думка», 2004. 584 с.

2. Адміністративне право України: Підручник / Ю. П. Битяк, В. М. Гаращук, О. В. Дьяченко та ін.; За ред. Ю. П. Битяка. К.: Юрінком Інтер, 2007. 544 с.

3. Адміністративне право України. Повний курс: підручник / за ред. В. Галунька, О. Правоторової. Видання третє. Київ: Академія адміністративно-правових наук, 2020. 466 с.

4. Акт проголошення незалежності України від 24.08.1991 р. / . URL: https://zakon.rada.gov.ua/laws/show/1427-12#Text

5. Алфьоров С. М., Ващенко С. В., Долгополова М. М., Купін А. П. Адміністративне право. Загальна частина. Навч. посіб. К.: Центр учбової літератури, 2011. 216 с.

6. Андрійко О. Ф. Адміністративне право // Велика українська енциклопедія. URL: https://vue.gov.ua/Адміністративне право

7. Андріяш В. І. Державна політика: концептуальні аспекти визначення / Державне управління: удосконалення та розвиток № 9, 2013. URL: http://www.dy.nayka.com.ua/?op=1&z=626

8. Антонова С. Є., Мартинюк Г. Ф. Інформаційна безпека. Державне управління: удосконалення та розвиток. 2019. № 11. URL: http://www.dy.nayka.com.ua/?op=1&z=1528 (дата звернення: 13.08.2023). DOI: 10.32702/2307-2156-2019.11.36

9. Бабій І. В. Управлінське рішення в антикризовому менеджменті підприємства / І. В. Бабій // Інвестиції: практика та досвід. 2015. № 5. С. 38-41

10. Баран М. В. Принципи правового регулювання інституту інформаційної безпеки. Науковий вісник Ужгородського національного університету. Серія: Право. 2021. Том 66. С. 129-134.

11. Бортник В. А. Адміністративне право України: навч. посіб. / В. А. Бортник. К.: ДП «Вид. дім «Персонал», 2012. 222 с.

12. Валюшко І. О. Інформаційна безпека України: трансформація законодавства після російського вторгнення / І. О. Валюшко // Історико-політичні студії. Збірник наукових праць. 2017. № 2 (8). С. 30 43.

13. Вдовін І.О. До проблеми розмежування галузей права у правовому регулюванні забезпечення реалізації інформаційної безпеки України. *Науковий вісник публічного та приватного права.* 2023. Вип. 5. С. 91–95.

14. Вдовін І.О. До характеристики ідеологічного напрямку державної політики у сфері забезпечення реалізації інформаційної безпеки України. *Виклики сучасності та наукові підходи до їх вирішення*: матеріали міжнародної науково-практичної конференції (Київ, 12–13 серп. 2020 р.). Київ: Науково-дослідний інститут публічного права, 2020. С. 88–90.

15. Вдовін І.О. До характеристики напрямків розвитку державної політики у сфері забезпечення реалізації інформаційної безпеки України. *Юридичний науковий електронний журнал.* 2022. № 10. С. 847–849. http://www.lsej.org.ua/10_2022/213.pdf

16. Вдовін І.О. До характеристики правового статусу суб'єктів спеціальної компетенції забезпечення реалізації інформаційної безпеки України. *Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення:* матеріали міжнародної науково-практичної конференції (Київ, 22–23 верес. 2021 р.). Київ: Науково-дослідний інститут публічного права, 2021. С. 71–74.

17. Вдовін І.О. До характеристики сучасного стану правового регулювання забезпечення реалізації інформаційної безпеки України. *Науковий вісник публічного та приватного права.* 2023. Вип. 4. С. 86–90.

18. Вдовін І.О. Проблеми нормативно-правового напрямку формування та розвитку державної політики у сфері забезпечення реалізації інформаційної безпеки України. *Актуальні проблеми імплементації*

наукових досягнень у практичну діяльність: матеріали міжнародної науково-практичної конференції, (Київ, 19–20 січ. 2022 р.). Київ: Науково-дослідний інститут публічного права, 2022. С. 57–59.

19. Вдовін І. Сучасний розвиток інформаційної безпеки України. *KELM*. 2022. № 7(51). С. 259–263.

20. Великий тлумачний словник сучасної української мови / Уклад. В.Т. Бусел К., 2001. С.43

21. Виноградова Г. В. Інформаційне право України: Навч. посіб. К. : МАУП, 2006. 144 с. Бібліогр. : С. 132–143.

22. Голод К. Інформаційна безпека США: сучасний стан та уроки для України / К. Голод // Геополітика України: історія і сучасність. 2017. Вип. 2. С. 91-107. URL: http://nbuv.gov.ua/UJRN/gpuis_2017_2_7

23. Гончарук С.Т. Адміністративне право України: Загальна та Особлива частини: Навч. посібник (на допомогу слухачам, що здають державні та поточні іспити з адміністративного права) / НАВСУ. К., 2000. 239 с.

24. Грабар Н. С. Формування культури кібербезпеки в суспільстві актуальне завдання сучасності. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/12389/1/stGrabar1.pdf

25. Грайворонський, М. В. Безпека інформаційно-комунікаційних систем [Електронний ресурс] : підручник / М. В. Грайворонський, О. М. Новіков. Електронні текстові дані (1 файл: 8,54 Мбайт). Київ : Видавнича група BHV, 2009. 698 с. (Серія «Інформатика»). Назва з екрана.

26. Гудима В. Закон про кібербезпеку: як і кого захищатимуть / піа «волинські новини». url: https://www.volynnews.com/news/society/zakon-pro-kiberbezpeku-iak-i-koho-zakhyshchatymut/

27. Давтян С. Г., Пойченко А. М., Саханенко С. Є. Організаційно-правовий механізм державного управління на місцевому рівні: навчальний посібник. Одеса: ОРІДУ НАДУ, 2006. 252 с.

28. Декларація про державний суверенітет України від 16.07.1990 р. / . URL: https://zakon.rada.gov.ua/laws/show/55-12#Text

29. Державна політика : підручник / Нац. акад. держ. упр. при Президентові України ; ред. кол. : Ю. В. Ковбасюк (голова), К. О. Ващенко (заст. голови), Ю. П. Сурмін (заст. голови) [та ін.]. К. : НАДУ, 2014. 448 с.

30. Державне управління в Україні: організаційно-правові засади : навч. посіб. / Н. Р. Нижник, С. Д. Дубенко, В. І. Мельниченко та ін. ; за заг. ред. проф. Н. Р. Нижник. К. : Вид-во УАДУ, 2002. 164 с.

31. Деякі питання діяльності Міністерства культури та інформаційної політики: Постанова КМУ від 16.10.2019 р. № 885 / . URL: https://zakon.rada.gov.ua/laws/show/885-2019-%D0%BF#Text

32. Дубов Д. В., Інформаційна підривна діяльність: проблеми нормативно-правового забезпечення протидії / Інформаційна безпека: сучасний стан, проблеми та перспективи: Матеріали І науково-практичної конференції. 20 вересня 2019 р., м. Київ. / Упоряд. : В. М. Фурашев, С. Ю. Петряєв. Київ : Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» Вид-во «Політехніка». 2019. 124 с. (с.12-17). URL: http://ippi.org.ua/sites/default/files/maket.pdf

33. Дудник І. М. Вступ до загальної теорії систем / Державний університет інформаційно-комунікаційних технологі. URL: https://duikt.edu.ua/uploads/l_1142_42884991.pdf

34. Енциклопедичний словник з державного управління / уклад. : Ю. П. Сурмін, В. Д. Бакуменко, А. М. Михненко та ін. ; за ред. Ю. В. Ковбасюка, В. П. Трощинського, Ю. П. Сурміна. К. : НАДУ, 2010. 820 с.

35. Ємельянов В. М. Державне управління: у визначеннях, поясненнях, схемах, таблицях : [навчальний посібник] / В. М. Ємельянов, О. Н. Євтушенко, В. І. Андріяш. Миколаїв : Вид-во ЧДУ ім. Петра Могили, 2015. 336 с.

36. Забезпечення інформаційної безпеки держави: підручник; за заг. ред. О.А. Семченка та В.М. Петрика. К.: ДНУ «Книжкова палата України», 2015. 672 с.

37. Загальна теорія держави і права [Текст] : підруч. для студ. юрид. спец. вищ. навч. закл. / [М. В. Цвік та ін.] ; за ред. д-ра юрид. наук, проф., акад. АПрН України М. В. Цвіка, д-ра юрид. наук, проф, акад. АПрН України О. В. Петришина ; Нац. юрид. акад. України ім. Ярослава Мудрого. Х. : Право, 2010. 583 с.

38. Залюбовська І. К. Парламентський контроль за діяльністю органів виконавчої влади як засіб забезпечення законності у сфері державного управління : автореф. дис. ... канд. юрид. наук : 12.00.07 / І. К. Залюбовська; кер. роботи С. В. Ківалов; Нац. ун.-т "Одеська юридична академія". Одеса, 2002. 20 с.

39. Захист інформаційного та кіберпростору / офіційний сайт СБУ. URL: https://ssu.gov.ua/zabezpechennia-informatsiinoi-bezpeky

40. Калюжний Р.А. Марценюк А.Г. Предмет та методи інформаційного права. Правова інформатика. 2008. № 3 (19). С. 5 9.

41. Калюжний Р.А., Баєв О.О., Нормативно-правове забезпечення інформаційної безпеки України Журнал "Правова інформатика". 4(24)/2009, с.5-12. URL: http://ippi.org.ua/sites/default/files/09kraibu.pdf

42. Капля О. М. (2023). Правове регулювання інформаційної безпеки громадянина під час дії воєнного стану. Експерт: парадигми юридичних наук і державного управління, (6(24), 16-20. https://doi.org/10.32689/2617-9660-2022-6(24)-16-20

43. Кельман Л.М. Соціально-політичні фактори впливу на правозастосовну діяльність: дисертація / Л.М. Кельман // Київ: Київський національний університет внутрішніх справ. 2007. 22 с.

44. Кириченко М. О. Формування ідеології інформаційного суспільства як фактор динамічного розвитку і безпеки сучасної України в

XXI столітті / М. О. Кириченко // Вісник Львівського ун-ту : зб. наук. праць. 2017. № 12. С. 74−81. − (Серія «Філософсько-політологічні студії»).

45. Кібербезпека як важлива складова всієї системи захисту держави / Офіційний веб сайт МО України. URL: https://www.mil.gov.ua/ukbs/kiberbezpeka-yak-vazhliva-skladova-vsiei-sistemi-zahistu-derzhavi.html

46. Кіберполіція / офіційний сайт. URL: https://cyberpolice.gov.ua/contacts/

47. Ківалова Т. С.До питання про поняття і складові методу правового регулювання / Т. С. Ківалова, Г. Є. Смелянець // Актуальні проблеми держави і права. - 2003. - Вип. 21. - С. 33-38.

48. Колпаков В.К., Гордєєв В.В. Настільна книга професійного судді при розгляді адміністративних справ. Посібник для судді. Х.: Харків юридичний, 2011. 476 с.

49. Комзюк А.Т. Адміністративний примус в правоохоронній діяльності міліції України: Дис...доктора юрид. наук:12.00.07. Х., 2002. 408 с.

50. Конвенція про кіберзлочинність від 23.11.2001 р. / Конвенцію ратифіковано із застереженнями і заявами Законом № 2824-IV від 07.09.2005 URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

51. Конституція України від 28.06.1996 р., URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80/ed19960628#Text

52. Кормич Б. А. Інформаційне право. Підручник. Харків: БУРУН і К., 2011. 334 с.

53. Корнєєв Ю.О. Інформаційне забезпечення розвитку підприємницької діяльності. Вісник НАН України. 2008. № 5. С. 24–31

54. Корнієнко Г. С. Правове регулювання матеріально-технічного забезпечення сільськогосподарських товаровиробників в умовах реформування АПК: дис. ... канд. юрид. наук. 12.00.06. / Корнієнко Ганна Сергіївна. К., 2003. 190 с.

55. Корчагин С. Інформаційне забезпечення військової політики ФРН / С. Корчагін // Закордонна військова освіта. 2008. №12. С.14 22.

56. Косогов О. М. Сучасна політика безпеки кіберпростору в умовах його мілітаризації / О. М. Косогов, А. О. Сірик // Сучасні інформаційні технології у сфері безпеки та оборони. 2015. № 3. С. 181-186

57. Костюк Т.В. Адміністративні процедури в діяльності податкових органів / дис. … канд. юрид. наук : 12.00.07.. Харків, 2021. 211 с.

58. Крут К. О. Адміністративно-правове забезпечення громадського контролю у сфері охорони здоров'я : дис. ... канд. юрид. наук : 12.00.07 / К. О. Крут; МВС України, Харк. нац. ун-т внутр. справ. - Харків, 2017. 215 с.

59. Купалова Г.І. Теорія економічного аналізу: Навч. посіб. К.: Знання, 2008. 639 с.

60. Курусь Т. В. Співвідношення нормативної діяльності із суміжними правовими поняттями. Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція. 2013. № 6-3. Т. 1. С. 9–11

61. Лаврук О. В. Сутність поняття державної політики / О. В. Лаврук // Університетські наукові записки. 2018. № 3-4. С. 254-263. URL: http://nbuv.gov.ua/UJRN/Unzap_2018_3-4_25

62. Левченко О. В. Нормативно-правове регулювання інформаційної безпеки України: стан та шляхи вирішення проблем / О. В. Левченко // Збірник наукових праць Харківського університету Повітряних Сил. - 2014. Вип. 3. С. 130-135. URL: http://nbuv.gov.ua/UJRN/ZKhUPS_2014_3_30

63. Лихолоб В. Г. Органи внутрішніх справ у боротьбі із злочинністю : морально-правовий аспект реалізації закону / Василь Григорович Лихолоб. К. : Вища школа, 1991. 176 с.

64. Любохинець Л. С. Світова практика забезпечення інформаційної безпеки в сучасному глобалізованому середовищі / Л. С. Любохинець, О. В. Поплавська // Бізнес-навігатор. 2017. Вип. 4-1. С. 93-97

65. Макух-Федоркова І. Нормативно-правові основи формування політики кібербезпеки Канади. Історико-політичні проблеми сучасного світу:

Збірник наукових статей. Чернівці: Чернівецький національний університет, 2022. Т. 45. С. 29-40 DOI: 10.3186 l/mhpi2022.45.29-40

66. Марущак А. І. Дослідження проблем інформаційної безпеки у юридичній науці / А. І. Марущак // Правова інформатика. 2010. № 3. С. 17-21

67. Мельничук М. В. Адміністративно-правові засади управлінської діяльності керівників органів виконавчої влади : дис. ... канд. юрид. наук: спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / М. В. Мельничук. К., 2009. 197 с.

68. Мельничук С. Проблемні питання класифікації форм здійснення функцій держави. Альманах сучасної науки і освіти. 2015. № 11 (101). С. 58–60.

69. Науково-методичні конференції / Науково-методичний центр Таврійський державний агротехнологічний університет імені Дмитра Моторного. URL: http://www.tsatu.edu.ua/nmc/metodychna-rada/metodychna-rada-rishennja-metod-rady/.

70. Нова стратегія кібербезпеки США: головні напрямки. URL: https://armyinform.com.ua/2023/03/07/nova-strategiya-kiberbezpeky-ssha-golovni-napryamky/

71. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання : монографія. Київ : Гельветика, 2017. 168 с

72. Німко О. Б. Адміністративно-правове регулювання державного молодіжного житлового кредитування : дис. ... канд. юрид. наук : 12.00.07 / Німко Ольга Борисівна К., 2008. 201 с.

73. Нові підходи Великої Британії до забезпечення національної стійкості. URL: https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/novi-pidkhody-velykoyi-brytaniyi-do-zabezpechennya-natsionalnoyi

74. Оніщенко Н.М. Система права та система законодавства: співвідношення та перспективи розвитку // Збірник наукових праць. Юридичні і політичні науки. Випуск 15. К.: Ін-т держави і права ім.В.М.Корецького НАН України, 2002. 608 с.

75. Опацький В.І. Організаційні засади здійснення державного контролю за діяльністю вищих навчальних закладів України / В. І. Опацький // Форум права. 2011. № 1. с.736-741

76. Панченко О. Інформаційна безпека в епоху турбулентності: державноуправлінський аспект: монографія. К.: КВІЦ. 2020. 332 с.

77. Панченко О.А. Проблеми правового забезпечення державного управління інформаційною безпекою. Державне управління: удосконалення та розвиток. 2019.№ 11. URL: http://www.dy.nayka.com.ua/?op=1&z=1561DOI: 10.32702/2307-2156-2019.11.3

78. Пархоменко Н.М. Джерела права: теоретико-методологічні засади: дисертація / Н.М. Пархоменко // Київ: Національна академія наук України інститут держави і права ім В.М. Корецького. 2009.

79. Пирожик О. (2021). Про необхідність використання Україною позитивного досвіду США з питань розбудови системи інформаційної безпеки. Вісник Пенітенціарної асоціації України, (2), 64-73. https://doi.org/https://doi.org/10.34015/2523-4552.2021.2.07

80. Питання діяльності Міністерства інформаційної політики України: Постанова КМУ від 14.01.2015 р. № 2 // . URL: https://zakon.rada.gov.ua/laws/show/2-2015-%D0%BF#Text

81. Питання Міністерства цифрової трансформації: Постанова КМУ від 18.09.2019 р. № 856 / . URL: https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#n12

82. Планування на аграрному підприємстві / Нелеп В.М. К.: КНЕУ, 2004. 495 с. URL: https://buklib.net/books/21929/

83. Покровська А. В., Ісакова Т. О. Державно-приватне партнерство у сфері кібербезпеки: досвід Великої Британії. URL: http://old2.niss.gov.ua/content/articles/files/cybersecurity6ddd7.pdf

84. Прижиналінська Н.В. Формування кадрового потенціалу аграрного сектора регіону // Вісник аграрної науки Причорномор'я. - Миколаїв. Спеціальний випуск 3 (42) 2007. С.43-48

85. Про воєнну доктрину України: Указ президента України від 15.06.2004 р. № 648/2004 / . URL: https://zakon.rada.gov.ua/laws/show/648/2004#Text

86. Про державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.0.2.2006 р. № 3475-IV / . URL: https://zakon.rada.gov.ua/laws/show/3475-15/ed20060223#Text

87. Про державну таємницю: Закон України від 21.01.1994 р. № 3855-XII / . URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text

88. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI // . URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text

89. Про друковані засоби масової інформації (пресу) в Україні: Закон України від 06.11.1992 р. № 2782-XII, ВРУ / . URL: https://zakon.rada.gov.ua/laws/show/2782-12/ed19921116#Text

90. Про електронні комунікації: Закон України від 16.12.2020 № 1089-IX / / . URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text

91. Про засади внутрішньої і зовнішньої політики: Закон України від 01.07.2010 р. № 2411-VI, ВРУ / . URL: https://zakon.rada.gov.ua/laws/show/2411-17#Text

92. Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року: розпорядження КМУ від 30.03.2023 р. N 272-р. URL: https://ips.ligazakon.net/document/KR230272?an=2

93. Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України: Постанова КМУ від 03.09.2014 р. № 411// . URL: https://zakon.rada.gov.ua/laws/show/411-2014-%D0%BF#Text

94. Про затвердження Положення про Міністерство внутрішніх справ України: Постанова КМУ від 28.10.2015 р. № 878 / . URL: https://zakon.rada.gov.ua/laws/show/878-2015-%D0%BF#Text

95. Про затвердження Положення про Міністерство оборони України : Постанова КМУ від 26.11.2014 р. № 671 // . URL: https://zakon.rada.gov.ua/laws/show/671-2014-%D0%BF#Text

96. Про затвердження Положення про Міністерство освіти і науки України: Постанова КМУ від 16.10.2014 р. № 630 / . URL: https://zakon.rada.gov.ua/laws/show/630-2014-%D0%BF#Text

97. Про затвердження Положення про територіальний орган Адміністрації Державної служби спеціального зв'язку та захисту інформації України: наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України 01.09.2014 № 432 / . URL: https://zakon.rada.gov.ua/laws/show/z1142-14#n14

98. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 р. N 80/94-ВР, ВРУ / . URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80/ed19940705#Text

99. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI, ВРУ / . URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

100. Про інформаційні агентства: Закон України від 28.02.1995 р. N 74/95-ВР, ВРУ / . URL: https://zakon.rada.gov.ua/laws/show/74/95-%D0%B2%D1%80/ed19950228#Text

101. Про інформацію: Закон України від 02.10. 1992 р. N 2657-XII, ВРУ / . URL: https://zakon.rada.gov.ua/laws/show/2657-12/ed19921002#Text

102. Про Кабінет Міністрів України: Закон України від 27.02.2014 р. № 794-VII / / . URL: https://zakon.rada.gov.ua/laws/show/794-18#Text

103. Про Концепцію Національної програми інформатизації: Закон України від 04.02.1998 р. № 75/98-ВР, ВРУ / . URL: https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80/ed19980204#Text

104. Про медіа: Закон України від 13.12.2022 р. № 2849-XI / / . URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text

105. Про місцеві державні адміністрації: Закон України від 09.04.1999 р. № 586-XIV / Верховна Рада України – Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/586-14#Text

106. Про місцеве самоврядування в Україні: Закон України від 21.05.1997 р.№ 280/97-ВР / . URL: https://zakon.rada.gov.ua/laws/show/280/97-%D0%B2%D1%80#Text

107. Про науково-технічну інформацію: Закон України від 25.06.1993 р. № 3322-XII ВРУ / . URL: https://zakon.rada.gov.ua/laws/show/3322-12/ed19930625#Text

108. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII / . URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

109. Про Національну поліцію: Закон України від 02.07.2015 р. № 580-VIII / . URL: https://zakon.rada.gov.ua/laws/show/580-19#Text

110. Про Національну програму інформатизації: Закон України від 04.02.1998 р.№ 74/98-ВР, ВРУ / . URL: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80#Tex

111. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII // . URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

112. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 р. № 537-V, ВРУ / . URL: https://zakon.rada.gov.ua/laws/show/537-16#Text

113. Про прокуратуру: Закон України від 14.10.2014 р.№ 1697-VII / . URL: https://zakon.rada.gov.ua/laws/show/1697-18#Text

114. Про Раду національної безпеки і оборони України: Закон України від 05.03.1998 р.№ 183/98-ВР / / . URL: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text

115. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України": Указ

Президента України від 14.09.2020 р. № 392/2020. // . URL: URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text

116. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.2021 р. № 447/2021 URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

117. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки": Указ Президента України від 28.12.2021 року №685/2021 / Президент України Офіційне інтернет-представництво. https://www.president.gov.ua/documents/6852021-41069

118. Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року "Про нову редакцію Воєнної доктрини України": Указ Президента України від 24.09.2015 № 555/2015 / . URL: https://zakon.rada.gov.ua/laws/show/555/2015#Text

119. Про рішення Ради національної безпеки і оборони України від 22 жовтня 2021 року "Про Концепцію реформування Державної служби спеціального зв'язку та захисту інформації України": Указ Президента України від 22.10.2021 р. № 544/202 // . URL: https://zakon.rada.gov.ua/laws/show/544/2021#Text

120. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року "Про Стратегію воєнної безпеки України": Указ Президента України від 25.03.2021 р. № 121/2021/. URL: https://zakon.rada.gov.ua/laws/show/121/2021#Text

121. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України": Указ Президента України від 16.03.2016 № 96/2016 / Президент України Офіційне інтернет-представництво. URL: https://www.president.gov.ua/documents/962016-19836

122. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації

державної політики у сфері інформаційної безпеки України: Указ Президента України від 01.05.2014 р. № 449/2014. URL: https://zakon.rada.gov.ua/laws/show/449/2014#n2

123. 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/ Президент України Офіційне інтернет-представництво. URL: https://www.president.gov.ua/documents/472017-21374

124. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року "Про Стратегію забезпечення державної безпеки": Указ Президента України від 16.02.2022 р. №56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#Text

125. 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 / Президент України Офіційне інтернет-представництво. URL: https://www.president.gov.ua/documents/2872015-19070

126. Про службу безпеки України: Закон України від 25.03.1992 р. № 2229-XII / . URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text

127. Про Стратегію комунікації з питань євроатлантичної інтеграції України на період до 2025 року: Указ Президента України від 11.09.2021 р. № 348/2021 // . URL: https://zakon.rada.gov.ua/laws/show/348/2021#Text

128. Про Стратегію національної безпеки України: Указ Президента України від 12.02.2007 р.№ 105/2007. У законі від 09.01.2007 р. № 537-V ВРУ / . URL: https://zakon.rada.gov.ua/laws/show/105/2007#n10

129. Про судоустрій і статус суддів: Закон України від 02.06.2016 р.№ 1402-VIII / . URL: https://zakon.rada.gov.ua/laws/show/1402-19#Text

130. Про схвалення Стратегії інформаційної реінтеграції Автономної Республіки Крим та м. Севастополя: Указ Президента України від 27.12.2018

р. № 1100-р. URL: https://zakon.rada.gov.ua/laws/show/1100-2018-%D1%80#Text

131. Про телебачення і радіомовлення: Закон України від 21.12.1993 р. № 3759-XII URL: https://zakon.rada.gov.ua/laws/show/3759-12/ed19931221#Text

132. Про телекомунікації: Закон України від 18.11.2003 р. № 1280-IV, ВРУ URL: https://zakon.rada.gov.ua/laws/show/1280-15/ed20031118#Text

133. Про центральні органи виконавчої влади: Закон України від 17.03.2011 р. № 3166-VI / . URL: https://zakon.rada.gov.ua/laws/show/3166-17#Text

134. Размуков Д. Парламентський контроль: практичні поради та рекомендації для підвищення ефективності / ЄСПРООН з парламентської реформи. URL: https://www.undp.org/sites/g/files/zskgke326/files/migration/ua/PRP_Guide_Parliamentary_Oversight-UKR.pdf

135. Романов В. Є. Державна політика: аналіз та механізми її впровадження / В. Є. Романов, О. М. Рудік, Т. М. Брус. Дніпропетр. : ДРІДУ НАДУ, 2003. 72 с.

136. Рябоконь О. Державна інформаційна політика формування інформаційного суспільства: зарубіжний досвід // Наукові праці Національної бібліотеки України імені В. І. Вернадського / редкол.: В. Попик (голова), Г. Боряк, В. Горовий [та ін.] ; відп. ред. В. Горовий ; НАН України, Нац. б-ка України ім. В. І. Вернадського, Асоц. б-к України. Київ, 2016. Вип. 43: С. 101– 110.

137. Саврук М.В. Проблеми забезпечення інформаційної безпеки України. Тези доповідей III міжнародної НПК «Інформаційна та економічна безпека» (INFECO-2010). URL: https://core.ac.uk/download/pdf/232881418.pdf

138. Саф'янюк В. Крок до ЄС та інформаційної безпеки / ВІКНА. URL: https://vikna.tv/video/ukrayina/zakon-pro-media-osnovni-polozhennya-yak-fiksuvatymut-porushennya/

139. Сафаров А. Аналіз стратегії інформаційної безпеки в порівнянні з чинною доктриною інформаційної безпеки / Інститут масової інформації. URL: https://imi.org.ua/monitorings/analiz-strategiyi-informatsijnoyi-bezpeky-v-porivnyanni-z-chynnoyu-doktrynoyu-informatsijnoyi-i38852

140. Семенюк О. Г. Теоретико-правовий аналіз поняття державної таємниці / "Інформація і право" № 3(18)/2016,- с.35-44

141. Ситніченко О. М. Окремі аспекти нормативно-правового регулювання забезпечення інформаційної безпеки / Вчені записки Таврійського національного університету імені В.І. Вернадського, Т.32, вип.№1, 2021, 86-91

142. Ситуаційний центр забезпечення кібербезпеки / офіційний сайт СБУ. URL: https://ssu.gov.ua/sytuatsiinyi-tsentr-zabezpechennia-kiberbezpeky

143. Скакун О. Ф. Теорія права і держави: Підручник. 3-те видання. К.: Алерта; ЦУП, 2011. 524 с.

144. Скакун О.Ф. Теорія держави і права (Енциклопедичний курс): [підручник] / Скакун О.Ф. Харків: Еспада, 2006. 776 с.

145. Скакун О.Ф. Теорія держави і права: Підручник / Пер. з рос. Харків: Консум, 2001. 656 с.

146. Скібіцька Л.І. Організація праці менеджера. Навч. посібник. - К.: Центр учбової літератури, 2010. 360 с.

147. Соснін О. Розуміння сутності національної безпеки: світоглядно-понятійні й науково-теоретичні засади / LexInform. URL: https://lexinform.com.ua/dumka-eksperta/rozuminnya-sutnosti-natsionalnoyi-bezpeky-svitoglyadno-ponyatijni-j-naukovo-teoretychni-zasady-chastyna-1/

148. Стешенко А. Парламент надав додаткові повноваження Держспецзв'язку щодо протидії ворожій агресії в кіберпросторі / LB.UA. URL: https://lb.ua/society/2022/07/28/524588_parlament_nadav_dodatkovi.html

149. Стойко О.Я. Дема Д.І. Фінанси: навч. посіб. / О.Я. Стойко, Д.І. Дема; за ред. О.Я. Стойка. К.: Алерта. 2014. 432 с.

150. Сунгуровський М. В., Чого бракує та що потрібно для побудови ефективної системи інформаційної безпеки/ Інформаційна безпека: сучасний стан, проблеми та перспективи: Матеріали І науково-практичної конференції. 20 вересня 2019 р., м. Київ. / Упоряд. : В. М. Фурашев, С. Ю. Петряєв. Київ : Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» Вид-во «Політехніка». 2019. 124 с. (с.12-14). URL: http://ippi.org.ua/sites/default/files/maket.pdf

151. Теорія держави і права: підруч. для студ. юрид. вищ. навч. закл. / О. В. Петришин, С. П. Погребняк, В. С. Смородинський та ін.; за ред. О. В. Петришина. Х.: Право, 2014. 368 с.

152. Теорія управління органами внутрішніх справ : підручник / за ред. Ю. Ф. Кравченка. К. : Нац. акад. внутр. справ України, 1999. 702 с.

153. Угровецький П. О. Адміністративні акти органів прокуратури: дис. … канд. юр. наук: 12.00.07 / ХНУВС. Харків, 2011. 195 с.

154. Уряд схвалив Стратегію інформаційної безпеки до 2025 року / Урядовий портал. URL: https://www.kmu.gov.ua/news/uryad-shvaliv-strategiyu-informacijnoyi-bezpeki-do-2025-roku

155. Фелик В. І. Адміністративно-правове забезпечення профілактичної діяльності Національної поліції України: монографія. Харків, 2016. 511 с.

156. Чмир Я. І. Проблеми забезпечення інформаційної безпеки в системі публічного управління / Я. І. Чмир // Аспекти публічного управління. 2018. Т. 6, № 9. С. 16-22

157. Чмир, Я. (2022). Сучасні проблеми інформаційної безпеки україни та перспективні напрями їх вирішення. Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління, (2(62), 149-154. https://doi.org/10.32689/2523-4625-2022-2(62)-23

158. Чорновол І. Інформаційна безпека США в контексті актуальних загроз і викликів. URL:

https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiWj8fxz4yCAxXGg_0HHaL5Ae0QFnoECAoQAQ&url=https%3A%2F%2Fjts.donnu.edu.ua%2Farticle%2Fview%2F8298%2F8297&usg=AOvVaw1bPSgxpVodIS2pMozk0Ag2&opi=89978449

159. Чубоха Н. Співвідношення категорій «форма» та «джерело» права. Історико-правовий часопис. 2018. № 2. С. 105–110.

160. Шегда, А. В. Менеджмент : Навч. посібник / А. В. Шегда. Київ : Знання, 2002. 583 с. URL: http://univer.nuczu.edu.ua/tmp_metod/525/Shegda.pdf

161. Яковлєв П.О. Досвід державного регулювання забезпечення інформаційної безпеки зарубіжних держав. Вісник Харківського національного університету імені В. Н. Каразіна. Серія «ПРАВО». Випуск 30, 2020, С.106-113

162. Act on the Federal Office for Information Security (BSI Act - BSIG): [Online tool], - Available at: https://www.bsi.bund. de/DE/DasBSI/Gesetz/ gesetz.html

163. Kormych B.A. Organizational and legal bases of information security policy of Ukraine [Organizacijno-pravovi osnovy` polity`ky` informacijnoyi bezpeky` Ukrayiny`] diss. ... Dr. Jurd. Sciences: Special. 12.00.07. Odessa, 2004. p.427.

164. U.S. General Services Administration. Information Security. URL: https://www.gsa.gov/reference/gsa-privacy-program/information-security

165. Vdovin I.O. The place of the Security Service of Ukraine in the system of entities ensuring information security. Entrepreneurship, Economy and Law. 2023. № 9. pp. 67-73.

ДОДАТКИ

Додаток А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

3. Вдовін І.О. До характеристики напрямків розвитку державної політики у сфері забезпечення реалізації інформаційної безпеки України. *Юридичний науковий електронний журнал.* 2022. № 10. С. 847–849. http://www.lsej.org.ua/10_2022/213.pdf

4. Вдовін І. Сучасний розвиток інформаційної безпеки України. *KELM*. 2022. № 7(51). С. 259–263.

3. Вдовін І.О. До характеристики сучасного стану правового регулювання забезпечення реалізації інформаційної безпеки України. *Науковий вісник публічного та приватного права.* 2023. Вип. 4. С. 86–90.

4. Вдовін І.О. До проблеми розмежування галузей права у правовому регулюванні забезпечення реалізації інформаційної безпеки України. *Науковий вісник публічного та приватного права.* 2023. Вип. 5. С. 91–95.

5. Vdovin I.O. The place of the Security Service of Ukraine in the system of entities ensuring information security. *Entrepreneurship, Economy and Law*. 2023. № 9. pp. 67–73.

які засвідчують апробацію матеріалів дисертації:

6. Вдовін І.О. До характеристики ідеологічного напрямку державної політики у сфері забезпечення реалізації інформаційної безпеки України. *Виклики сучасності та наукові підходи до їх вирішення*: матеріали міжнародної науково-практичної конференції (Київ, 12–13 серп. 2020 р.). Київ: Науково-дослідний інститут публічного права, 2020. С. 88–90.

7. Вдовін І.О. До характеристики правового статусу суб’єктів спеціальної компетенції забезпечення реалізації інформаційної безпеки України. *Науково-практичні засади розвитку наукової думки на сучасному*

етапі державотворення: матеріали міжнародної науково-практичної конференції (Київ, 22–23 верес. 2021 р.). Київ: Науково-дослідний інститут публічного права, 2021. С. 71–74.

8. Вдовін І.О. Проблеми нормативно-правового напрямку формування та розвитку державної політики у сфері забезпечення реалізації інформаційної безпеки України. *Актуальні проблеми імплементації наукових досягнень у практичну діяльність:* матеріали міжнародної науково-практичної конференції, (Київ, 19–20 січ. 2022 р.). Київ: Науково-дослідний інститут публічного права, 2022. С. 57–59.