ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

Кваліфікаційна наукова праця
на правах рукопису

БАРАН МАРІЯ ВОЛОДИМИРІВНА

УДК 342.9.351.4:746(477)(043)

ДИСЕРТАЦІЯ

АДМІНІСТРАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

081 «Право»
08 «Право»

Подається на здобуття освітньо-наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ **М. В. Баран**

Науковий керівник **Єсімов Сергій Сергійович**
кандидат юридичних наук, доцент

Львів – 2022

АНОТАЦІЯ

Баран М. В. Адміністративно-правове забезпечення інформаційної безпеки в Україні. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 081 «Право». Львівський державний університет внутрішніх справ. Львів, 2022.

У дисертації здійснено аналіз адміністративно-правового забезпечення інформаційної безпеки в Україні в контексті сучасного державотворення, розвитку адміністративно-правової науки та інформаційного права, цифрової трансформації суспільства та національної економіки в умовах європейської інтеграції України та збройної агресії Росії.

Підкреслено, що дослідження правової природи адміністративно-правового забезпечення інформаційної безпеки в Україні на основі вивчення досвіду інституціоналізації механізму захисту інформації та захисту особи, суспільства та держави від деструктивного інформаційного впливу у правових системах країн Європейського Союзу та Північноатлантичного альянсу (НАТО), дозволили виявити правові характеристики інформаційної безпеки, показати місце та роль у правовій державі.

Зазначено, що методологічною основою дослідження адміністративно-правового забезпечення інформаційної безпеки є міждисциплінарний підхід, який дає можливість осмислити цілеспрямовану активність особи, суспільства та держави в інформаційному просторі як єдність мети, правових засобів забезпечення. Це дозволило зробити висновки, які дають уявлення про забезпечення інформаційної безпеки особи, суспільства та держави, що охоплює захист інформації та захист від деструктивного інформаційного впливу в єдину сукупність та сформулювати засновані на емпіричному та теоретичному матеріалі методологічні засади дослідження адміністративно-правового забезпечення інформаційної безпеки в умовах цифрової трансформації.

Констатовано, що систему правового забезпечення інформаційної

безпеки в умовах цифрової трансформації доцільно охарактеризувати, як міжгалузеву зі складною внутрішньою структурою, що перебуває у динамічному розвитку, маючи ціннісний, нормативно-правовий, функціональний та інституційний виміри. Ціннісний вимір вказує, що забезпечення інформаційної безпеки перебуває у системних зв'язках із конституційними цінностями та слугує забезпеченню суспільно корисної мети – гарантованості й захищеності людини, суспільства та держави. Нормативно-правовий вимір визначає на законодавчому рівні адміністративно-правові засоби та механізми забезпечення інформаційної безпеки. Функціональний вимір забезпечує реалізацію компенсаторної, правоохоронної, каральної, виховної функцій та функції поновлення права.

Аргументовано, що інституціоналізація інформаційної безпеки в інформаційному праві розвивається відповідно до темпів розвитку цифрової трансформації суспільства на підставі впровадження інформаційно-комунікаційних технологій та систем, підпорядковується логіці інституційної динаміки, закладеної у минулому. Інституціоналізація інформаційної безпеки – це процес виділення, становлення, формування, розвитку та закріплення інститутів і їх коригування, направлених на забезпечення захисту інформації, особи, суспільства та держави від деструктивного інформаційного впливу. Це свідчить про особливості змісту адміністративно-правових засад забезпечення інформаційної безпеки, що залежить від структури органів публічної влади у компетенцію яких входить діяльність у сфері, що досліджується.

Обґрунтовано, що адміністративно-правове забезпечення інформаційної безпеки – це врегульована нормами адміністративного права державно-управлінська діяльність публічних органів влади та їх посадових осіб у контексті захисту інформації, виявлення деструктивного інформаційного впливу на особу, суспільство та державу, запобігання розповсюдженню шляхом блокування або видалення протиправних відомостей, що здійснюється на основі застосування відповідних адміністративно-правових заходів. Адміністративно-правові засоби запобігання інформаційної безпеки – це

способи адміністративно-правового впливу держави на осіб, які здійснюють інформаційну діяльність щодо запобігання правопорушенням у інформаційному просторі України. Механізм адміністративно-правового регулювання у сфері забезпечення інформаційної безпеки – юридично закріплена, організована система адміністративно-правових засобів, що становить нормативно-правову, інституційну та інструментальну основу стану захищеності національних інтересів в інформаційному просторі, інформаційних ресурсів, особи, суспільства та держави від деструктивного інформаційного впливу та їх наслідків. Ключовим елементом заходів забезпечення, які дозволяють гарантувати захист інформаційних прав, є обмеження у розповсюдженні, блокуванні та виділенні деструктивної інформації суб'єктами владних повноважень.

Наголошено, що правові обмеження в інформаційному праві в діяльності засобів масової інформації відіграють правоохоронну функцію. Метою інституту правових обмежень в інформаційному праві є: захист територіальної цілісності, суверенітету держави, публічних інтересів в інформаційному просторі; захист приватних інтересів; стримування протиправної або небажаної поведінки суб'єктів інформаційної діяльності; регулювання суспільних відносин в інформаційному просторі у специфічних умовах режимів воєнного та надзвичайного стану; виявлення негативних правових наслідків обмеження прав громадян у зв'язку із застосуванням заходів примусу. Застосування правових обмежень у діяльності засобів масової інформації зумовлені механізмом інформаційного впливу на психіку людини і суспільну психологію.

Підкреслено, що специфіка мережі Інтернет (багаторівнева організаційна структурованість; транскордонний характер функціонування та використання її базових компонентів тощо), зумовлює правове регулювання інформаційної безпеки. У мережі Інтернет представлено коло осіб, які безпосередньо пов'язані із забезпеченням інформаційної безпеки: громадяни, які є користувачами; технічні суб'єкти, дії яких спрямовані на забезпечення роботи Інтернету; бізнес, громадянське суспільство, зацікавлені в розширенні інформаційних

можливостей; державні суб’єкти, у завдання яких входять правове врегулювання відносин в Інтернеті; міжнародні організації – координація питань, розробка технічних і правових стандартів, пов’язаних з Інтернетом. Регулювання правових відносин повинно будуватися на нормах галузевого законодавства, технічно-правових, охоронних, регулятивних, міжнародних засобах, які складуть ефективний механізм правового врегулювання інформаційної безпеки в Інтернеті.

Зазначено, що правове регулювання юридичної відповідальності за порушення інформаційної безпеки у межах спеціальних законів, що обумовлюють запровадження та дію юрисдикційних правових механізмів, є незавершеним та системним. Принциповою особливістю юридичної відповідальності у сфері забезпечення інформаційної безпеки в умовах воєнного стану є її підвищений та обмежений у часі характер, домінування компенсаторної та охоронної функцій.

У системі забезпечення інформаційної безпеки правопорушення становлять особливу правову конструкцію, виражену у застосуванні спеціальних примусових заходів: блокування інформаційного ресурсу, сайту й інформації та інші. Процесуальне законодавство, процесуальні дії, засоби, способи і умови реалізації заходів інформаційного примусу будуть тоді ефективними, коли буде досягнуто процесуально правильне, законне та обґрунтоване, на належному професійному рівні рішення щодо їх застосування.

Підкреслено, що правове вдосконалення інституту адміністративно-правового забезпечення інформаційної безпеки в Україні має спиратися на правову основу й новітні доктринально-правові напрацювання в контексті європейської інтеграції України та забезпечення інформаційної безпеки щодо захисту інформації (національних інформаційних ресурсів), захисту особи, суспільства і держави від деструктивного інформаційного впливу в умовах воєнного стану; передбачати процесуальне закріплення відповідних матеріальних норм, доповнення їх належними гарантіями та санкціями юридичної відповідальності за порушення; забезпечувати поєднання

загальнодержавних, суспільних та індивідуальних інтересів. Належне унормування відповідних суспільних відносин покликане сприяти усуненню поширенню інформації, яка потенційно може загрожувати державі, суспільству, правам і свободам людини, територіальної цілісності та суверенітету України.

Показано, що існує зв'язок між формуванням інформаційної культури та розвитком соціальних процесів, оскільки інформаційна культура особистості є важливим чинником успішної професійної та непрофесійної діяльності, а також соціальної захищеності особи в інформаційному суспільстві.

Обґрунтовано, що з метою формування культури інформаційної безпеки особи та суспільства за умов цифрової трансформації суспільства, посиленню інформаційного протиборства демократичних і тоталітарних країн необхідно розробити документи планування; розвивати правове просвітництво, охоплюючи питання відповідальності за правопорушення в інформаційній сфері; визначення викликів і загроз інформаційній безпеці; постановку короткострокових і довгострокових завдань, що охоплюють активне залучення до цього процесу закладів освіти та установ культури, інститутів громадянського суспільства; розвиток механізмів саморегулювання користувачів засобів масової комунікації, соціальних мереж та інших можливостей інформаційних технологій та систем.

Зазначено, що інститут забезпечення інформаційної безпеки крокує шляхом удосконалення у частині збільшення ступеня захищеності прав і законних інтересів зацікавлених суб'єктів в інформаційному просторі. Є позитивні тенденції та перспективи розвитку інституту адміністративно-правового забезпечення інформаційної безпеки в України, які дозволять розкрити потенціал ефективного функціонування інституту інформаційної безпеки та адаптувати до вимог Європейського Союзу та Північноатлантичного альянсу (НАТО).

Ключові слова: адміністративно-правове регулювання, захист, Інтернет, інформація, деструктивний інформаційний вплив, національні інтереси, інформаційна сфера, інформаційна культура, юридична відповідальність.

SUMMARY

Baran M. V. Administrative and legal provision of information security in Ukraine. – Qualifying scientific work on manuscript rights.

Dissertation for obtaining the degree of Doctor of Philosophy in specialty 081 – Law. Lviv State University of Internal Affairs. Lviv, 2022.

The dissertation analyzes the administrative and legal provision of information security in Ukraine in the context of modern state formation, the development of administrative and legal science and information law, the digital transformation of society and the national economy in the context of the European integration of Ukraine and Russia's aggression, including information.

It is emphasized that the study of the legal nature of the administrative and legal provision of information security in Ukraine, based on the study of the experience of institutionalization of the information protection mechanism and the protection of individuals, society and the state from destructive informational influence in the legal systems of the countries of the European Union and the North Atlantic Alliance (NATO), made it possible to identify legal characteristics of this phenomenon, to show its place and role in the rule of law.

It is noted that the methodological basis of the study of the administrative and legal provision of information security is an interdisciplinary approach, which makes it possible to understand the purposeful activity of the individual, society and the state in the information space as a unity of purpose, legal means of provision, conscious and voluntary activity of subjects in the process of implementation. This made it possible to draw conclusions that give an idea of the provision of information security of a person, society and the state, which includes information protection and protection against destructive informational influence in a single aggregate and to formulate the methodological principles of the study of administrative and legal provision of information security in the conditions based on empirical and theoretical material digital transformation.

It has been established that the system of legal support of information security

in the conditions of digital transformation should be characterized as an interdisciplinary one with a complex internal structure that is in dynamic development, having value, regulatory, functional and institutional dimensions. The value dimension indicates that the provision of information security is in systemic relations with constitutional values and serves to ensure a socially useful goal - the guarantee and protection of a person, society and the state. The normative-legal dimension defines administrative-legal means and mechanisms for ensuring information security at the legislative level. The functional dimension ensures the implementation of compensatory, law enforcement, punitive, educational functions and the function of restoring the right.

It is argued that the institutionalization of information security in information law develops in accordance with the pace of development of the digital transformation of society based on the introduction of information and communication technologies and systems, and is subject to the logic of institutional dynamics established in the past. Institutionalization of information security is the process of selection, establishment, formation, development and consolidation of institutions and their adjustment aimed at ensuring the protection of information, individuals, society and the state from destructive informational influence. This testifies to the peculiarities of the content of the administrative and legal principles of ensuring information security, which depends on the structure of public authorities whose competence includes activity in the field under investigation.

It is substantiated that the administrative-legal provision of information security is the state-management activity of public authorities and their officials regulated by the norms of administrative law in the context of information protection, detection of destructive information impact on the individual, society and the state, prevention of dissemination by blocking or removing illegal information, which is carried out on the basis of the application of appropriate administrative and legal measures. Administrative and legal means of preventing information security are methods of administrative and legal influence of the state on persons who carry out information activities in order to prevent offenses in the information space of

Ukraine. The mechanism of administrative and legal regulation in the field of ensuring information security is a legally established, organized system of administrative and legal means that constitutes the regulatory, legal, institutional and instrumental basis of the state of protection of national interests in the information space, information resources, individuals, society and the state from destructive information impact and their consequences. A key element of security measures, which allows guaranteeing the protection of information rights, is the limitation in the distribution, blocking and allocation of destructive information by subjects of power.

It is emphasized that legal restrictions in information law in the activities of mass media play a law enforcement function. The purpose of the institute of legal restrictions in information law is: protection of territorial integrity, state sovereignty, public interests in the information space; protection of private interests; restraining illegal or undesirable behavior of subjects of information activity; regulation of public relations in the information space in the specific conditions of military and state of emergency regimes; identifying the negative legal consequences of limiting the rights of citizens in connection with the use of coercive measures. The application of legal restrictions in the activities of the mass media is determined by the mechanism of informational influence on the human psyche and social psychology.

It is emphasized that the specificity of the Internet (multilevel organizational structure; cross-border nature of functioning and use of its basic components, etc.) determines the legal regulation of information security. The Internet includes a circle of persons who are directly related to the provision of information security: citizens who act as users; technical subjects whose actions are aimed at ensuring the Internet; business, civil society, interested in expanding information opportunities; state entities whose tasks include legal regulation of relations on the Internet; international organizations - coordination of issues, development of technical and legal standards related to the Internet. The regulation of legal relations should be based on the norms of industry legislation, technical-legal, protective, regulatory, international means, which will constitute an effective mechanism of legal regulation of information security on the Internet.

It is noted that the legal regulation of legal responsibility for violations of information security within the limits of special laws that determine the introduction and operation of jurisdictional legal mechanisms is incomplete and systemic. A fundamental feature of legal responsibility in the field of ensuring information security in the conditions of martial law is its increased and time-limited nature, the dominance of compensatory functions and protective functions.

In the system of ensuring information security, offenses constitute a special legal structure expressed in the application of special coercive measures: blocking of an information resource, site and information, and others. Procedural legislation, procedural actions, means, methods and conditions for the implementation of information coercion measures will be effective when a procedurally correct, legal and justified decision on their application is reached at the appropriate professional level.

It is emphasized that the legal improvement of the institute of administrative and legal provision of information security in Ukraine must be based on the legal basis and the latest doctrinal and legal developments in the context of the European integration of Ukraine and the provision of information security regarding the protection of information (national information resources), the protection of individuals, society and the state from destructive information influence in the conditions of martial law; to provide for the procedural consolidation of relevant material norms, supplementing them with appropriate guarantees and sanctions of legal liability for violations; ensure a combination of national, public and individual interests. The proper normalization of relevant social relations is intended to contribute to the elimination of the dissemination of information that could potentially threaten the state, society, human rights and freedoms, territorial integrity and sovereignty of Ukraine.

It is shown that there is a connection between the formation of information culture and the development of social processes, since the information culture of an individual is an important factor in successful professional and non-professional activities, as well as the social security of a person in the information society.

It is substantiated that in order to form a culture of information security of individuals and society under the conditions of digital transformation of society, to strengthen the information struggle of democratic and totalitarian countries, it is necessary to develop planning documents; to develop legal education, including the issue of responsibility for offenses in the information sphere; identification of challenges and threats to information security; setting short-term and long-term tasks, which include the active involvement of educational and cultural institutions, civil-society institutions in this process; development of mechanisms of self-regulation of users of mass communication, social networks and other possibilities of information technologies and systems.

It is noted that the institution of ensuring information security is improving in terms of increasing the degree of protection of the rights and legitimate interests of interested subjects in the information space. There are positive trends and prospects for the development of the institute of administrative and legal support of information security in Ukraine, which will allow us to reveal the potential of the effective functioning of the institute of information security and to adapt it to the requirements of the European Union and the North Atlantic Alliance (NATO).

Keywords: administrative and legal regulation, protection, Internet, information, destructive information influence, national interest, information sphere, information culture, legal responsibility.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА,

у яких опубліковані основні наукові результати дисертації відповідно до постанови Кабінету Міністрів Україні від 12 січня 2022 року № 44:

1. Баран М. В. Інформаційна безпека як предмет адміністративно-правового регулювання. *Соціально-правові студії.* 2021. Випуск 3 (13). С. 50-56.

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

3. Баран М. В. Захист інформації у контексті забезпечення інформаційної безпеки. *Аналітично-порівняльне правознавство.* 2022. № 3. С. 150-155.

4. Баран М. В. Суб'єкти забезпечення інформаційної безпеки в Україні. *Юридичний науковий електронний журнал*. 2022. № 6. С. 220-223.

інші:

1. Баран М. В. Механізм адміністративно-правового регулювання інформаційної безпеки. *Visegrad journal on human rights*. 2021. № 4. С. 25-30.

які засвідчують апробацію матеріалів дисертації:

1. Баран М. В. Аналіз комунікативної діяльності людини в інформаційному просторі в контексті інформаційної безпеки. *Теоретико-прикладні проблеми правового регулювання в Україні:* матеріали Всеукраїнської науково-практичної конференції (м. Львів, 11 грудня 2020 р.) / за заг. ред. І. В. Красницького. Львів: ЛьвДУВС, 2020. С. 20-24.

2. Баран М. В. Електронні торги в аспекті інформаційної безпеки. *Інформаційні технології в освіті та практиці*: матеріали Всеукраїнської науково-практичної конференції (м. Львів, 18 грудня 2020 р.) / упорядник: Т. В. Магеровська. Львів : ЛьвДУВС, 2020. С. 89-90.

3. Баран М. В. Інформаційно-правова специфіка соціалізації військовослужбовців в аспекті інформаційної безпеки. *Проблеми розвитку адміністративного, фінансового та інформаційного права в контексті євроінтеграційних процесів»:* збірник тез *міжнародної науково-практичної конференції* (м. Львів, 15 квітня 2021 р.). Київ: ПП «Комп'ютерний дизайн», 2021. С. 18-19.

4. Баран М. В. Конституційне право особи на свободу отримання і поширення інформації у контексті забезпечення інформаційної безпеки. *Сучасний конституціоналізм: проблеми теорії та практики:* матеріали наукового семінару (м. Львів, 25 червня 2021 р.). Львів: ЛьвДУВС, 2021. С. 11-15.

5. Баран М. В. Захист прав людини в умовах розвитку цифрових технологій і формування інформаційної безпеки. *Теоретико-прикладні проблеми правового регулювання в Україні:* матеріали V Всеукраїнської науково-практичної конференції (м. Львів, 10 грудня 2021 р.) / за заг. ред. І. В. Красницького. Львів: ЛьвДУВС, 2021. С. 13-16.

6. Баран М. В. Проблеми забезпечення інформаційної безпеки особи в адміністративному процесі. *Проблеми розвитку адміністративного, фінансового та інформаційного права в контексті євроінтеграційних процесів*: збірник. тез міжнародної науково-практичної конференції (м. Львів, 3 червня 2022 р.). Київ: Комп'ютерний дизайн, 2022. С. 27-30.

7. Баран М. В. Адміністративні форми та методи забезпечення інформаційної безпеки у Збройних Силах в умовах воєнного стану. *Конституційні права і свободи людини та громадянина в умовах воєнного стану:* матеріали наукового семінару (м. Львів, 23 червня 2022 р.). Львів: ЛьвДУВС, 2022. С. 24-27.

ЗМІСТ

ВСТУП

Актуальність теми дисертаційного дослідження. Розвиток інформаційного суспільства та процесів цифрової трансформації суттєво підвищило значущість інформаційної сфери. В інформаційному просторі відбувся стрибок у розвитку інформаційних загроз. Нові досягнення у сфері інформаційно-комунікаційних технологій, посилення ролі масової комунікації та розвиток когнітивних технологій збільшили можливості деструктивного інформаційного впливу на людину та суспільство. Поряд з унікальними можливостями для соціального прогресу цифрове середовище породило нові виклики та загрози для національної безпеки, які потребують адекватного реагування. Це зумовило виділення інформаційної безпеки як однієї з підсистем національної безпеки, значимість якої у міру розвитку науково-технічного прогресу інформаційно-комунікаційних технологій продовжує зростати. Це передбачає необхідність проведення фундаментальних досліджень адміністративно-правового забезпечення інформаційної безпеки та системного реформування правового регулювання відносин у цій сфері.

Стратегія інформаційної безпеки України визначила інформаційну безпеку як стратегічний національний пріоритет, тобто важливий напрям забезпечення національної безпеки. Серед ключових національних інтересів України виділено розвиток безпечного інформаційного простору, захист суспільства від деструктивного інформаційного впливу.

Відкриті новою інформаційною реальністю можливості були використані з метою надання деструктивного інформаційно-психологічного впливу на індивідуальну, групову та суспільну свідомість. Істотно зросла активність в інформаційному просторі російських спецслужб, сепаратистських організацій. Мережа Інтернет та мобільний зв’язок вивели на новий рівень загрози поширення негативної інформації.

Анонімне цифрове середовище з кожним роком все активніше генерує ризики розповсюдження кримінальних та інших антисоціальних ідей,

розпалювання ненависті та ворожнечі, поширення протиправного контенту, обману та маніпуляції свідомістю, залучення до терористичної та сепаратистської діяльності, споживання наркотиків та суспільно небезпечної поведінки. Агресія Росії щодо України різко загострила проблему поширення недостовірної суспільнозначущої інформації у засобах масової інформації та інтернет-ресурсах. Технології штучного інтелекту, віртуальної та доповненої реальності здатні вивести інформаційні загрози на новий рівень небезпеки.

У зв'язку з цим нових науково обґрунтованих підходів та правового осмислення вимагають проблеми забезпечення інформаційної безпеки. Реалізація поставлених у Стратегії національної безпеки України, Стратегії інформаційної безпеки України та інших документів стратегічного планування завдань щодо забезпечення надійного захисту особи, суспільства та держави від зростаючих інформаційних загроз детермінує необхідність на основі системного аналізу законодавства у сфері розробки пропозицій щодо подальшого формування системи адміністративно-правового забезпечення інформаційної безпеки України з урахуванням стандартів Північноатлантичного альянсу (НАТО) та досвіду країн Європейського Союзу. Вказані обставини зумовили актуальність теми дисертаційного дослідження.

Ступінь розробленості теми дослідження. Адміністративно-правові аспекти забезпечення інформаційних прав, свобод і законних інтересів в інформаційному просторі, охоплюючи інформаційну безпеку, досліджувалися у працях: В. Б. Авер'янова, В. М. Бевзенка, А. І. Берлача, Ю. П. Битяка, Н. П. Бортник, П. В. Діхтієвського, І. С. Гриценка, О. В. Карасса, Л. Є. Кисіль, А. А. Козловського, В. К. Колпакова, О. В. Кузьменко, В. І. Курила, Є. В. Курінного, Н. В. Лесько, Р. С. Мельника, В. Я. Настюка, О. І. Остапенка, А. О. Селіванова, О. І. Харитонової, В. В. Цвєткова, Я. М. Шевченко, Ю. С. Шемчушенка та інших.

З позицій інформаційного права досліджувалися окремі проблеми, що стосуються правового забезпечення інформаційної безпеки, проте здебільшого вони орієнтовані на розвиток напряму забезпечення національної безпеки,

охоплюючи безпеку держави в інформаційній сфері, закономірності розвитку інформаційного суспільства. Ці та низка інших актуальних питань досліджувалися в наукових та дисертаційних роботах: І. В. Арістової, О. А. Баранова, І. В. Діордіці, О. П. Дзьобаня, О. Д. Довганя, О. О. Золотар, С. С. Єсімова, Р. А. Калюжного, М. В. Коваліва, Б. А. Кормича, Т. В. Костецької, О. Кохановської, В. А. Ліпкана, Ю. П. Лісовської, А. І. Марущака, В. Я. Настюка, Г. В. Новицького, Т. С. Перуна, В. Г. Пилипчука, А. О. Селіванова, О. М. Солодкої, Т. Ю. Ткачука, О. О. Тихомирова, В. Г. Цимбалюка, М. Я. Швеця, І. М. Шопіної, О. Г. Яреми та ін. У 2017 році Ю. П. Лісовська захистила дисертацію на тему «Адміністративно-правове забезпечення інформаційної безпеки в Україні».

У сучасних умовах ця тема заслуговує на пильну увагу до питання забезпечення інформаційної безпеки особи, суспільства та держави, виявляючи об’єктивну потребу комплексного дослідження в умовах цифрової трансформації.

Науково-теоретичним підґрунтям дисертації стали науково-теоретичні та науково-практичні розробки вчених та практиків у галузі теорії держави і права, адміністративного, інформаційного, конституційного, цивільного, кримінального права.

Зв’язок роботи з науковими програмами, планами, темами. Наукове дослідження виконане відповідно до Переліку пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 2022 року, затвердженому постановою Кабінету Міністрів від 12.07.2022 р. № 942, пункту 5 «Правове забезпечення функціональних напрямів інформаційної діяльності адміністративні послуги і доступ до публічної інформації; засоби масової інформації, реклама; видавнича, бібліотечна, архівна і музейна справи; державна статистика, документообіг; інформаційна діяльність в галузях освіти і науки, культури і мистецтв, в економічній, фінансовій, банківській та інших сферах», глави 1.9 «Правове забезпечення інформаційної сфери» Пріоритетних напрямів фундаментальних та прикладних наукових

досліджень у галузі права Національної академії правових наук України на 2021-2025 роки. Дослідження проводилося відповідно до теми державної реєстрації Львівського державного університету внутрішніх справ на 2019–2022 роки «Проблеми правового регулювання публічного управління у сфері правоохоронної діяльності» (номер державної реєстрації 0119U001743), на 2022–2027 роки «Проблеми правового регулювання публічного управління у сфері правоохоронної діяльності» (номер державної реєстрації 0122U200304).

Мета і завдання дослідження. Мета дослідження полягає у вирішенні важливої наукової проблеми – розробці теоретико-методологічної концепції адміністративно-правового забезпечення інформаційної безпеки в умовах цифрової трансформації суспільства, спрямованої на вдосконалення інформаційного законодавства.

Дослідження поставленої наукової проблеми здійснювалося на основі вирішення таких завдань:

- провести теоретико-правовий аналіз методологічних підстав дослідження інформаційної безпеки в інформаційному праві;

- проаналізувати характеристику системи правового забезпечення інформаційної безпеки в умовах цифрової трансформації;

- розкрити інституціоналізацію інформаційної безпеки у системі інформаційного права;

- розглянути адміністративно-правові засоби та механізми забезпечення інформаційної безпеки;

- дослідити правові обмеження в інформаційному праві на прикладі засобів масової інформації;

- визначити правове регулювання забезпечення інформаційної безпеки в мережі Інтернет:

- охарактеризувати юридичну відповідальність у сфері забезпечення інформаційної безпеки у контексті переходу до цифрового суспільства;

- визначити пріоритетні напрями вдосконалення законодавства у сфері забезпечення інформаційної безпеки в умовах цифрової трансформації;

- обґрунтувати необхідність формування культури інформаційної безпеки.

Об'єктом дослідження визначено систему суспільних відносин у галузі адміністративно-правового забезпечення інформаційної безпеки в Україні в умовах цифрової трансформації.

Предметом дослідження є адміністративно-правове забезпечення інформаційної безпеки в Україні.

Методи дослідження. Методологічна основа дослідження – комплекс загальнонаукових та спеціальних юридичних методів пізнання. При дослідженні закономірностей забезпечення інформаційної безпеки в умовах цифрової трансформації використовувався діалектичний метод. Формально-логічний метод застосовувався під час аналізу норм інформаційного законодавства, визначенні змісту основних понять, систематизації матеріалу з метою отримання узагальнювальних висновків у межах заявленої проблематики (підрозділи 1.2., 1.3). Порівняльно-правовий метод сприяв виявленню тенденцій та зіставленню підходів держав Європейського Союзу та НАТО. З метою отримання та узагальнення знань про сутність та етапи розвитку інститутів інформаційної безпеки застосовувався історично-правовий метод (підрозділ 1.1). Системний аналіз дозволив провести оцінку підходів, що склалися, до забезпечення інформаційної безпеки особи, суспільства та держави, зіставити з об'єктивно складними суспільними відносинами, а соціологічний метод – провести оцінку факторів, що впливають на поведінку особи як суб'єкта інформаційних відносин (підрозділ 2.1). Прогностичний метод – у вигляді моделювання застосовувався щодо перспектив розвитку законодавства, спрямованого на створення системи ефективного забезпечення інформаційної безпеки (підрозділ 3.1).

В основу методології наукового дослідження покладено факторний, причинно-наслідковий аналіз, спрямований на виявлення обставин, що становлять небезпеку для особи і суспільства в інформаційній сфері, та визначення характеру їхнього впливу на ефективність реалізації інтересів в

інформаційному просторі (підрозділ 2.2). Беручи до уваги, що факторний аналіз як методика застосовується у різних галузях знань, авторка пропонує використання для комплексного та системного дослідження характеру впливу певних факторів у вигляді викликів та загроз інформаційній безпеці (підрозділи 2.3, 2.4).

Дослідницька мотивація спрямована на виявлення шляхом факторного аналізу взаємозв'язків, взаємообумовленостей між можливостями, що надаються інформаційно-комунікаційними технологіями зі стримуючими факторами, пов'язаними з різноманітністю викликів та загроз інформаційній безпеці, на розробку пропозицій, спрямованих на вдосконалення правового забезпечення інформаційної безпеки.

Науково-теоретичною основою дисертаційної роботи слугували наукові дослідження українських і закордонних науковців. Документальним і фактологічним підґрунтям дисертації стали національні статистичні дані, чинне законодавство.

Нормативну базу дослідження складають Конституція України, Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, закони та інші нормативні акти України, нормативні акти Європейського Союзу у сфері забезпечення інформаційної безпеки, правоохоронна практика у досліджуваній сфері.

Емпіричною базою дослідження є статистично-довідкові матеріали, що стосуються теми дослідження, узагальнені дані судової практики, публікації в засобах масової інформації.

Наукова новизна одержаних результатів. Наукова новизна дисертаційного дослідження визначається постановкою та рішенням актуальної та багатоаспектної наукової проблеми адміністративно-правового забезпечення інформаційної безпеки. У роботі авторка вперше досліджує адміністративно-правове забезпечення інформаційної безпеки в організаційно-правовому аспекті у межах Національної економічної стратегії на період до 2030 року щодо

цифрової трансформації та Стратегії інформаційної безпеки України щодо захисту національного інформаційного простору в умовах агресії Росії. У результаті дослідження сформульовано низку наукових положень, висновків та рекомендацій, зокрема:

уперше:

- здійснено системну характеристику адміністративно-правового забезпечення інформаційної безпеки в контексті цифрової трансформації суспільства, розвитку науки адміністративного та інформаційного права, що дозволило обґрунтувати необхідність її формування як системи адміністративно-правових перетворень, орієнтованих на досягнення соціально значущих цілей щодо захисту особи, суспільства та держави від деструктивного інформаційного впливу та реалізації національних інтересів в інформаційній сфері на основі процедур, що призводять до зміни форм, методів і змісту діяльності органів публічної адміністрації та, як наслідок, до зміни суспільних відносин у сфері, що досліджується;

- доведено, що основними правовими механізмами забезпечення інформаційної безпеки є: встановлення правових заборон та інших обмежень поширення певних видів негативної інформації; встановлення спеціальних правил обороту інформаційної продукції певних видів; закріплення обов’язків суб’єктів інформаційних правовідносин щодо забезпечення інформаційної безпеки; ідентифікація особи абонентів, користувачів мережі Інтернет та цифрових сервісів; видалення чи обмеження доступу до протиправного контенту; встановлення юридичної відповідальності за правопорушення, що посягають на інформаційну безпеку; правове закріплення заходів контрпропаганди; правове стимулювання розвитку цифрової грамотності та формування культури інформаційної безпеки;

- зазначено, що адміністративно-правове забезпечення інформаційної безпеки в умовах цифрової трансформації передбачає комплексне та гнучке використання різних моделей правового регулювання відносин в аналізованій сфері, охоплюючи державне регулювання та саморегулювання. Серед інших

соціальних регуляторів у механізмі правового забезпечення інформаційно-психологічної безпеки важливе значення мають мораль та етичні норми, тоді як роль технічного регулювання обмежується закріпленням нормативів захисту людини від негативного впливу технологічного характеру.

удосконалено:

- систему правового забезпечення інформаційної безпеки в умовах цифрової трансформації як закріпленого правовими нормами різновиду юридичної діяльності в інформаційному просторі. Система за соціальною сутністю має складний політико-правовий характер, базується на засадах національної безпеки, верховенства права та пріоритету прав людини, реалізується у сфері інформаційно-правових відносин;

- адміністративно-правові засоби та механізми забезпечення інформаційної безпеки;

- правові засади юридичної відповідальності у сфері забезпечення інформаційної безпеки;

- наукові погляди на специфіку культури інформаційної безпеки в сучасній Україні, які детерміновані єдністю з засадами інформаційної безпеки особи та суспільства;

дістали подальшого розвитку:

- методологічні підходи дослідження інформаційної безпеки в інформаційному праві;

- адміністративно-правові засоби та механізми забезпечення інформаційної безпеки, як ключової інституції серед форм реалізації заходів безпеки;

- правове регулювання забезпечення інформаційної безпеки в мережі Інтернет.

Внесено пропозиції щодо змін і доповнень до чинного законодавства.

Теоретичне та практичне значення одержаних результатів проведеного дослідження полягає в тому, що викладені в дисертації положення, висновки, пропозиції та рекомендації мають науково-теоретичне значення,

можуть бути використані в:

- науково-дослідній діяльності – для проведення подальших наукових досліджень адміністративно-правового забезпечення інформаційної безпеки;

- правотворчій діяльності – для подальшого удосконалення чинного законодавства щодо інформаційної безпеки;

- правозастосовній діяльності – для підвищення ефективності практичної діяльності органів публічної адміністрації щодо реалізації нормативних положень у сфері інформаційної безпеки (довідка від 14.09.2022);

- навчальному процесі – під час підготовки дидактичних матеріалів з навчальної дисципліни «Інформаційне право України» (акт впровадження № 40 від 20.09.2022).

Особистий внесок здобувача. Сформульовані в дисертації положення, узагальнення, висновки, рекомендації, пропозиції обґрунтовані на підставі особистих досліджень у результаті опрацювання та аналізу наукових, нормативних і статистичних джерел.

Апробація результатів дисертації. Основні положення роботи апробовані на науково-практичних заходах: регіональній науково-практичній конференції «Теоретико-прикладні проблеми правового регулювання в Україні» (м. Львів 11 грудня 2020 р.); всеукраїнській науково-практичній конференції «Інформаційні технології в освіті та практиці : матеріали (м. Львів, 18 грудня 2020 р.); міжнародній науково-практичній конференції «Проблеми розвитку адміністративного, фінансового та інформаційного права в контексті євроінтеграційних процесів» (м. Львів, 15 квітня 2021 р.); науковому семінарі «Сучасний конституціоналізм: проблеми теорії та практики» (м. Львів, 25 червня 2021 р.); всеукраїнській науково-практичній конференції «Теоретико-прикладні проблеми правового регулювання в Україні» (м. Львів, 10 грудня 2021 р.); міжнародній науково-практичній конференції «Проблеми розвитку адміністративного, фінансового та інформаційного права в контексті євроінтеграційних процесів» (м. Львів, 3 червня 2022 р.); науковому семінарі «Конституційні права і свободи людини та громадянина в умовах воєнного

стану (м. Львів, 23 червня 2022 р.).

Публікації. Основні положення дисертації висвітлено у: 12 наукових публікаціях, із яких: 5 наукових статей, зокрема 4 у виданнях, які входять до переліку наукових фахових видань України, 1 – у зарубіжному фаховому виданні (Словацька Республіка) та 7 тез-виступів на науково-практичних заходах.

Обсяг і структура дисертації. Дисертаційна робота викладена на 244 сторінках, складається зі вступу, трьох розділів, висновків, списку використаних джерел, 8 додатків. Обсяг основного тексту дисертації складає 204 сторінки тексту. Список використаних джерел містить 284 найменування, викладені на 29 сторінках.

РОЗДІЛ І
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

1.1. Методологічні підходи дослідження інформаційної безпеки в інформаційному праві

На етапі становлення та розвитку інформаційного суспільства процес інформатизації є глобальним, всеохопним, таким, що проникає у всі сфери життя. Він перетворюється на один з основних факторів суспільного розвитку та багато в чому характеризує сучасну соціальну динаміку.

Завдяки процесу інформатизації в суспільстві відбуваються системні зміни, відповідно до яких всі сегменти суспільства, кожна людина залучаються до глобального інформаційного простору, стаючи елементами глобальної інформаційної системи та відповідно тією чи іншою мірою залежними від неї.

Зазначена інформаційна залежність стосується всього світу, усіх держав і людей, які беруть участь у процесі виробництва, зберігання та використання інформації в ході інформаційного обміну та інформаційної взаємодії. Інформаційна взаємодія стала планетарним фактором, породивши цілу низку соціальних трансформацій та ввівши в систему соціальних відносин такі процеси та якості, як: інформаційні війни, інформаційна зброя, інформаційний тероризм, інформаційна злочинність та інформаційна безпека.

Сучасні соціальні практики показують, що суспільний розвиток на основі глобальної інформатизації породжує якісно нові виклики, загрози та ризики інформаційній безпеці. Ця обставина робить актуальним дослідження теоретико-правових засад інформаційної безпеки.

У науці інформаційного права склався певний алгоритм аналізу проблем правового забезпечення інформаційної безпеки. Він передбачає визначення понятійного апарату у сфері, що досліджується, місця та ролі інформаційної

безпеки у системі національної безпеки, встановлення національних інтересів у цій галузі, розкриття змісту принципів, завдань та функцій забезпечення інформаційної безпеки, характеристик системи правового регулювання суспільних відносин в аналізованій сфері. На вказане звертає увагу С. Г. Онопрієнко в дослідженні «Методологічні засади дослідження інформаційної безпеки у науці права національної безпеки та військового права» [1, с. 186-187].

У сучасній науці використовуються два основні підходи до дослідження інформаційної безпеки – технологічний та інформаційний. Їхня відмінність полягає у використанні різних критеріїв безпеки. Технологічний підхід основними критеріями виділяє забезпечення конфіденційності, цілісності та доступності інформації [2]. Інформаційний концентрується на захисті від інформаційних загроз, здатних призвести до руйнування традиційних духовно-моральних цінностей суспільства, розмивання ідентичності особистості, дестабілізації політичної системи та втрати державного суверенітету [3, с. 84-85]. Комплексне дослідження інформаційної безпеки поєднує два підходи.

Теоретико-методологічні засади дослідження інформаційної безпеки базуються на наукових працях із загальної теорії права, філософії права, соціології права, конституційного права, кримінології, адміністративного та кримінального права, теорії державного управління. Значний внесок зробили вчені: В. Б. Авер'янов, І. В. Арістова, Є. О. Архипова, О. А. Баранов, В. Л. Бурячок, Д. О. Біленська, О. Д. Довгань, І. М. Доронін, С. С. Єсімов, О. О. Золотар, Л. П. Коваленко, М. В. Ковалів, В. А. Кудінов, В. А. Ліпкан, О. Є. Малашко, І. В. Мукомела, О. І. Остапенко, О. В. Рибальський, І. М. Сопілко, О. М. Селезньова, В. В. Ткаченко, Т. Ю. Ткачук, О. Д. Тихомиров, В. Г. Хахановський, О. В. Шамрай, Ю. С. Шемшученко, І. М. Шопіна та інші [4-25].

Це передбачає на основі міждисциплінарної методології дослідження правових явищ розгляд такої проблеми під кутом виявлення характерологічних рис інформаційного суспільства з позицій інформаційних і комунікаційних

технологій, з позицій нових соціальних властивостей сучасного суспільства, людини – як члена цього суспільства, розуміння його як суб'єкта нового типу соціальних відносин у розрізі таких характеристик людини, як інформаційна цілісність, інформаційні права, інформаційна безпека.

Цілісність системи інформаційної безпеки конструюється на основі системного підходу, з виділенням її підсистем та елементів (будь-який елемент може бути розглянутий окремо як самостійна система), що виконують у структурі системи певну функцію та вирішують завдання, підпорядковуючись єдиній для системи меті.

Системний підхід не достатній для характеристики інформаційної безпеки як цілісності. Це пов'язано з тим, що в моделюванні системної цілісності не беруться до уваги зміни діючих чинників та його поєднання у конкретній ситуації. Динамізм факторів неможливо передбачити заздалегідь, він вносить новизну в ситуацію та порушує логічно сконструйовану цілісність системи.

Синергетичний підхід відкриває можливість виявляти різноманітні взаємозв'язки та взаємозалежності різних основ – природи, суспільства, культури та людини. Охоплення цих уявлень інформаційно-правововою науковою картиною взаємодії людини як суб'єкта права з об'єктами суспільних відносин створює передумови та нові можливості для додаткової правової рефлексії в бік упорядкованості інформаційної системи. Дослідження інформаційної безпеки з позицій синергетичного підходу вимагає розглядати її у межах іншої, більш загальної системи, якою є національна безпека. Це необхідно, щоб зрозуміти механізми змін, які визначаються як внутрішніми процесами так й зовнішніми чинниками.

Історичний метод при дослідженні проблеми інформаційної безпеки дозволяє виявити появу проблеми інформаційної безпеки в суспільстві, яке здійснило перехід від індустріальної до постіндустріальної стадії розвитку.

Соціологічний метод дозволяє розкрити соціальну обумовленість правових норм, зрозуміти механізм реальної дії норм права та дізнатися про їх

ефективність. Соціологічний метод дослідження інформаційної безпеки дає можливість виявити потребу у соціальних передумовах правового забезпечення. Він знаходить відображення у факторному аналізі об'єктивної дійсності, яка склалася, що зумовлює виділення інформаційної безпеки як об'єкта правового забезпечення.

При дослідженні проблеми інформаційної безпеки з допомогою формально-логічного методу стає можливим вивчити логічні конструкції норм, встановленні для правового забезпечення інформаційного права та інших галузях. Також цей метод дозволяє усвідомити і значення термінів, які використовуються законодавцем з метою правового забезпечення інформаційної безпеки.

Особливе місце у дослідженні займає порівняльно-правовий метод. Термін «порівняльне правознавство» має два основні смислові значення. По-перше, це спосіб, що називається як порівняльно-правовий, компаративний. По-друге, це галузь академічної правової науки. Порівняльне правознавство як метод юридичної науки представлений сукупністю прийомів пізнання правових явищ, з яких на основі вивчення правопорядків різних країн проводиться зіставлення з метою виявлення властивих загальних змістовних рис і загальних закономірностей історичного розвитку.

У контексті дослідження І. М. Ситара, цінність порівняльного правознавства стосовно інформаційного права полягає в тому, що воно дає можливість виявити та брати до уваги чужі помилки та досягнення, допомагає зрозуміти роль та значення інформаційного права як інструменту соціально-нормативного регулювання [26, с. 44]. При дослідженні інформаційної безпеки як об'єкта правової охорони застосування цього методу зумовлено тим, що Україна є частиною світової правової системи, а також процесами глобалізації, що посилилися.

Наведена сукупність методів дослідження інформаційної безпеки на підставі системного підходу дозволяє розглянути її з різних боків, у взаємозв'язку з іншими явищами та процесами та досягти мети дослідження.

Такий методологічний підхід дає можливість сформувати загальну універсальну міждисциплінарну картину інформаційної безпеки, яка об'єднує в органічну єдність систему різних дисциплінарних понять та дисциплінарних методологій, сукупність дескриптивної фактології, ряд конкретних моделей, які в універсальній картині розкривають соціокультурний, соціально-антропологічний, соціально-психологічний, інформаційно-технологічний, просторово-часовий підхід до зазначеної проблеми. Цей методологічний підхід дозволяє реалізувати дослідження складних систем, які передбачають поєднання різних дисциплінарних підходів та вихід за їх межі.

Основні принципи методології, що характеризує основну дослідницьку матрицю аналізу інформаційної безпеки охоплює такі принципи:

- принцип розвитку, згідно з яким інформаційна безпека, яка є системною якістю, має здатність саморозвитку, відображаючи вектори соціальної динаміки та втілюючи в один із найважливіших елементів цієї динаміки;

– принцип цілісності, згідно з яким інформаційна безпека – це цілісна якість з набором невід'ємних атрибутів;

– принципи системності та багатофакторності, згідно з якими інформаційна безпека є системною та багатофакторною якістю, що виражається в єдності множинності особистісних, громадянських, професійних та соціальних характеристик.

Відповідно до Стратегії національної безпеки України національна безпека є станом захищеності національних інтересів України від зовнішніх та внутрішніх загроз [27]. У документах стратегічного планування та законодавстві України спостерігаються різні підходи щодо визначення видів безпеки.

У Стратегії національної безпеки України виділено державну, громадську, інформаційну, екологічну та інші види безпеки. Також згадуються військова (оборона), економічна, транспортна, енергетична безпека, безпека особистості. У Законі України «Про національну безпеку України»

законодавець виділяє кібербезпеку, громадську, воєнну безпеку [28]. Подібне має місце і в науковій літературі, оскільки дослідники не завжди дбають про дотримання логічних правил класифікації.

Інформаційна складова наявна у всіх видах національної безпеки. А це дає підставу виділити інформаційну безпеку як основний елемент національної безпеки [29, с. 121]. Об'єктами інформаційної безпеки є держава, суспільство та особа.

Наше дослідження присвячене вивченню забезпечення інформаційної безпеки з погляду теоретико-правових аспектів, об'єднуючи інформаційну безпеку особи, суспільства та держави.

Виділення інформаційної безпеки (англ. informationsecurity) у системі видів безпеки є загальновизнаним в Україні та за кордоном.

Визнання субстантивної ролі інформаційної безпеки в системі національної безпеки в Україні відбулося у 2001 році з прийняттям Заходів щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України [30].

І. В. Горбенко, О. М. Потій, С. О. Черних, М. К. Прокоф'єв у науковому дослідження «Системний аналіз переходу від концепції національної інформаційної політики до доктрини інформаційної безпеки України», який опублікований у 2002 році, пропонували розробити доктрину інформаційної безпеки [31].

На виконання Рішення Ради національної безпеки і оборони України від 21 березня 2008 року «Про невідкладні заходи щодо забезпечення інформаційної безпеки України» 08 липня 2009 року затверджено Доктрину інформаційної безпеки України [32; 33]. Відповідно до вищезгаданого нормативно-правового документа, стан захищеності національних інтересів України в інформаційній сфері визначається сукупністю збалансованих інтересів особи, суспільства та держави. На підставі указу Президента України у 2014 році Доктрина інформаційної безпеки втратила актуальність та відповідно чинність у зв'язку зі збройною агресією Росії на сході України [34;

35].

У 2017 році затверджено нову Доктрину інформаційної безпеки України (далі – Доктрину інформаційної безпеки України 2017), яка закріпила дефініцію інформаційної безпеки як стан захищеності особи, суспільства та держави від внутрішніх та зовнішніх інформаційних загроз [36].

Обидві викладені дефініції мають досить широкий характер і наповнюються конкретним змістом через визначення національних інтересів України в інформаційній сфері.

Вивчення їх переліку (Доктрини інформаційної безпеки 2009 та Доктрини інформаційної безпеки 2017) прямо не виявляє особистий психологічний компонент інформаційної безпеки. Однак його сутнісні ознаки проглядаються в положеннях, що стосуються збереження культурних, історичних та духовно-моральних цінностей народу України, доведення до міжнародної громадськості достовірної інформації про державну політику України та її офіційної позиції щодо соціально значущих подій у країні та світі, застосування інформаційних технологій з метою забезпечення національної безпеки України в галузі культури, територіальної цілісності та суверенітету.

Аналіз розділів цих документів стратегічного планування, що визначають загрози та стан інформаційної безпеки та основні напрями забезпечення (Доктрини інформаційної безпеки 2009 та Доктрини інформаційної безпеки 2017), виявляє набагато чіткішу фіксацію блоку питань інформаційної безпеки.

У Доктрині інформаційної безпеки України 2017 року серед напрямів забезпечення інформаційної безпеки в галузі оборони країни виділено нейтралізацію інформаційно-психологічного впливу, у тому числі спрямованого на підрив традицій, пов’язаних із захистом Вітчизни.

У науці серед дослідників інформаційної безпеки протягом тривалого часу домінував вузький підхід до розуміння захисту інформації та інформаційних систем. Таке зрізане бачення лягло в основу базового законодавчого акту для інформаційної сфери 1990-х років – Законів України «Про інформацію» (1992 рік) та «Про захист інформації в інформаційно-

комунікаційних системах» (1994 рік) [37; 38].

Багато в чому підхід зберігся у Законі України «Про внесення змін до деяких законодавчих актів України у зв'язку з прийняттям Закону України «Про інформацію» та Закону України «Про доступ до публічної інформації», що вніс певні зміни у вказані нормативно-правові акти [39].

У зв'язку з цим С. С. Єсімов обґрунтовано наголошував на тому, що проблема інформаційної безпеки штучно звужується до технічних аспектів захисту інформації, при цьому нехтуються соціально-гуманітарні аспекти [40, с. 147].

Починаючи з кінця 1990-х років, багато дослідників розвивали альтернативний підхід. Серед них слід виділити одного із основоположників теорії правового забезпечення інформаційної безпеки Б. А. Кормича [41].

Надалі широкий підхід до трактування інформаційної безпеки, що передбачає включення до її змісту психологічних аспектів, знаходить усе більше прихильників.

Р. А. Калюжний та В. С. Цимбалюк вважають, що інформаційна безпека − це вид інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства й держави безпечних умов життєдіяльності, пов'язаних із створенням, розповсюдженням, зберіганням та використанням інформації. У практиці інформаційної безпеки виділяються два напрями: інформаційна безпека та захист інформації [42, с.110].

У навчальній літературі з інформаційної безпеки автори дотримуються розширеної парадигми розуміння [43]. У спеціалізованому словнику основою інформаційної безпеки суспільства визначено безпеку індивідуальної, групової та масової свідомості громадян за наявності інформаційних загроз, до яких насамперед слід віднести інформаційні впливи [44].

Важливе значення для затвердження інформаційної безпеки як складової предмета правового регулювання в галузі інформаційної безпеки мало її відображення у двох знакових наукових правотворчих ініціативах.

По-перше, у виданій у 2012 році Концепції кодифікації інформаційного

законодавства України, розробленої авторським колективом Інституту інформації, безпеки і права Національної академії правових наук України, серед основних державно-правових складових упорядкування інформаційних відносин у галузі правового забезпечення інформаційної безпеки названо визначення сучасних викликів і загроз інформаційній безпеці людини, суспільства і держави, адекватне реагування на реальні й потенційні загрози правовими, організаційними, технічними та іншими засобами [45].

В. М. Брижко, О. А. Баранов і В. С. Цимбалюк пропонували та обґрунтовували необхідністю охоплення положень про захист інформації та захист від деструктивного впливу на свідомість та поведінку масового споживача поширених відомостей.

Розробка Інформаційного кодексу України була передбачена Законом України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» та Стратегією розвитку інформаційного суспільства в Україні [46; 47].

Логічним, але революційним за своїм значенням кроком стало віднесення захисту суспільства від деструктивного інформаційного впливу до основних національних інтересів України у Стратегії державної безпеки України [48].

Інформаційна безпека – стан захищеності національних інтересів людини, суспільства і держави в інформаційній сфері, за якого унеможливлено завдання шкоди через: неповноту, невчасність та невірогідність інформації, що використовується, негативний інформаційний вплив; витік державної таємниці та службової інформації; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації, у тому числі шляхом проведення іноземними спецслужбами, окремими організаціями, групами, особами спеціальних інформаційних операцій та деструктивних інформаційних впливів, а також забезпечується своєчасне виявлення, запобігання та нейтралізація реальних і потенційних загроз національним інтересам та національній безпеці України. Інформаційна безпека є складовою національної

безпеки України (пункт 7 ст. 3 Стратегії державної безпеки України). У документі визначено низку завдань щодо забезпечення інформаційної безпеки.

Сьогодні можна впевнено зробити висновок про те, що інформаційна безпека людини, суспільства та держави входить до змісту інформаційної безпеки. З цього випливає, що інформаційна безпека має загальні ознаки, властиві такому виду безпеки, важливими з яких є інформаційний характер загроз безпеці та інформаційна сфера як галузь прояву цих загроз.

У чинному законодавстві України сформувалися такі правові інститути у структурі підгалузі правового забезпечення інформаційної безпеки: захист інформації, охоплюючи захист окремих видів інформації обмеженого доступу; захист критично важливих об'єктів інформаційної інфраструктури; захист дітей від негативного впливу продукції сексуального чи еротичного характеру [38; 48; 49; 50]. У важливому для досліджуваної галузі Законі України «Про захист суспільної моралі» щодо дітей (ст. 7) термін «інформаційна безпека» не використовується.

У Законі України «Про захист суспільної моралі» є необхідність запровадження поняття «інформаційна безпека» з таких причин: потреба в рельєфному позначенні психологічної складової інформаційної безпеки; наявність специфіки в системі інформаційної безпеки; наявність чіткої межі між захистом інформації та інформаційно-психологічною безпекою за критеріями об'єкта та методів впливу; існування комплексу специфічних загроз; спільність правового інструментарію, використовуваного захисту від різних форм деструктивного інформаційного впливу.

Принципова відмінність інформаційної безпеки традиційного блоку від інформаційної безпеки щодо суспільної моралі в тому, що її змістом є не захист інформації, а захист від інформації самої людини та суспільства, у тому числі дітей. З огляду на це, інформаційну безпеку можна визначити як захист особи та суспільства від негативного інформаційного впливу.

Б. А. Кормич у 2011 році зазначав, що дослідження навколо проблематики інформаційної безпеки так чи інакше фокусувалися навколо

поняття інформаційного впливу, а інформаційна безпека трактувалася як захищеність від цих впливів [51, с. 130]. Такої позиції дотримувалися інші провідні дослідники того періоду [52; 53]. Тут проходить межа між інформаційною та психологічною безпекою [54]. Ці питання перебувають за межами проблематики, що досліджується.

Як базовий методологічний підхід вивчення інформаційної безпеки вважаємо за необхідне використовувати міждисциплінарний підхід. У філософії міждисциплінарні дослідження трактуються як спосіб організації дослідницької діяльності, що передбачає взаємодію у вивченні одного й того самого об'єкта представників різних дисциплін.

Міждисциплінарний підхід як методологічний принцип проведення наукового дослідження передбачає запозичення та застосування знань та методів з інших сфер наукового знання [55]. Сьогодні розвиток міждисциплінарних правових знань є одним із ключових напрямів трансформації права в контексті знаходження юридичною наукою взаємозв'язку з іншими науковими дисциплінами технічного та гуманітарного профілю.

Аналізована предметна галузь інформаційної безпеки спочатку носить гібридний характер і перебуває на стику низки сфер: інформаційних технологій, психології та безпеки. Тому для вивчення проблеми правового забезпечення інформаційної безпеки, крім базової юридичної науки, більший інтерес становлять три галузі наукового знання: психологія, соціологія масової комунікації та науки про інформаційні технології.

Психологія вивчає зміст та механізм роботи індивідуальної та колективної психіки – основних об'єктів інформаційної безпеки, механізм інформаційного впливу. Психологічні знання дозволяють виявити потенційну небезпеку певної інформації для людей та соціальних груп різних категорій, наприклад, для дітей різних вікових груп.

Соціологія масової комунікації досліджує особливості інформаційного середовища суспільства, її вплив на соціум, а також вивчає основні інститути та

типи масової комунікації. Знання з цієї наукової галузі допомагають дібрати інструментарій для нейтралізації загроз інформаційної безпеки та їх джерел і виділяти за значимістю об’єкти для застосування.

Інформатика та інші науки про інформаційні технології вивчають канали та способи технічної передачі інформації, за допомогою якої виявляється деструктивний інформаційний вплив.

Ця галузь науки дозволяє розуміти особливості технічних каналів поширення негативної інформації та вибрати адекватні способи та засоби впливу на них. Застосування міждисциплінарного підходу дозволяє скласти уявлення про об’єкти інформаційної безпеки. Об’єкти безпеки є однією з ключових характеристик будь-якого виду безпеки, які визначають стратегію й інструменти забезпечення.

Теоретично під безпекою розуміють реальні явища, процеси та відносини, попередження чи усунення загроз, що становить мету та зміст політики безпеки [56, с. 70]. Щодо сфери інформаційної безпеки йдеться про об’єкти деструктивного інформаційного впливу.

Аналіз чинних документів стратегічного планування та законодавства дозволив стверджувати, що деструктивний інформаційний вплив у праві може ідентифікуватися як загроза безпеці; форми зловживання правом на інформацію та свободою масової інформації; правопорушення (злочини, адміністративні правопорушення, цивільно-правові делікти); виду співучасті у скоєнні злочину (організації, підбурювання, інтелектуального пособництва); обставини, що охоплюють злочинність дії (психічного примусу); пом’якшувальної обставини (вчинення злочину внаслідок психічного примусу, аморальність поведінки потерпілого, який став приводом для злочину); підстави для визнання недійсності правочину (вчинення правочину під впливом суттєвої помилки); підстави застосування заходів державного примусу, включаючи блокування інформаційного ресурсу. Це не повний список. Проте з аналізу проглядається міжгалузева правова природа проблематики деструктивного інформаційного впливу, що виявляється у різних правових поняттях та інститутах у

кримінальному, адміністративному, цивільному та інших галузях права.

У проєкті Закону України «Про інформаційну безпеку» як об’єкти інформаційної безпеки виділялися:

- щодо людини та громадянина: забезпечення конституційних прав і свобод людини і громадянина на збирання, зберігання, використання та поширення інформації; право на спілкування мовою походження;недопущення несанкціонованого втручання у зміст, процеси обробки, передачі та використання персональних даних;захищеність від негативного впливу інформаційних технологій та інформаційно-психологічного впливу;

- щодо суспільства: збереження та примноження духовних, культурних і моральних цінностей українського народу та громадян України всіх національностей;інформаційне забезпечення суспільно-політичної стабільності, міжетнічної і міжконфесійної злагоди та розвитку громадянського суспільства;

- щодо держави: забезпечення інформаційного суверенітету, запобігання інформаційній агресії, експансії та інформаційній блокаді України з боку іноземних держав, організацій, груп та осіб;формування та реалізація органами державної влади та інститутами громадянського суспільства ефективної державної політики в інформаційній сфері; інформаційно-інфраструктурне забезпечення суспільно-економічного й науково-технічного розвитку та формування позитивного іміджу України; становлення та розвиток інформаційного суспільства в Україні; інтеграція України у європейський та світовий інформаційний простір [57].

У Стратегії інформаційної безпеки України об’єктом захисту від деструктивного інформаційно-психологічного впливу названо суспільство [58]. У таких випадках спостерігається двоїстість об’єктів інформаційної безпеки: до них відносять людину, групу людей, суспільство, державу, психологічні складові – індивідуальну психіку та суспільну свідомість. У цьому випадку немає суперечності. Зазначене зумовлено різним рівнем деталізації при характеристиці об’єктів інформаційної безпеки.

У плані правового регулювання вибір необхідного рівня деталізації

залежатиме від характеру та предмета правового акта. Для базового закону або документа стратегічного планування доцільніше використовувати усі рівні. Для вузького предмета правового регулювання доцільно брати перший рівень деталізації.

У Стратегії інформаційної безпеки України йдеться про нейтралізацію інформаційної агресії, зокрема спеціальних інформаційних операцій держави-агресора, спрямованих на підрив державного суверенітету, територіальної цілісності України, забезпечення інформаційної стійкості суспільства та держави, створення ефективної системи взаємодії між органами державної влади, органами місцевого самоврядування та суспільством [58]; у розділі XII Кримінального кодексу України (далі – КК України) як видовий об'єкт злочинів виділено суспільну мораль [59, с. 168; 60]; безпосереднім об'єктом адміністративного правопорушення у сфері інформаційної безпеки передбаченим Кодексом України про адміністративні правопорушення (далі – КУпАП), визначено інформацію [61].

Об'єкт інформаційної безпеки на трьох рівнях деталізації має різні особливості з позиції загальної та соціальної психології та соціології.

На першому рівні об'єктами інформаційної безпеки є особа, великі та малі соціальні групи. Первинним об'єктом інформаційної безпеки є особа, на яку направлено інформаційно-психологічний вплив. Як зазначає О. О. Золотар, людина як особистість і соціальний суб'єкт, її психіка схильні до дії інформаційних факторів, які, трансформуючись через поведінку, мають несприятливий вплив на соціальні суб'єкти [14, с.142].

Наступним об'єктом інформаційної безпеки є соціальні групи. Т. М. Кузьменко дає визначення соціальної групи як групи людей, у якій спільність суспільно значущих рис виявляється у колективній ідентичності та контактах, що їх супроводжують, взаємодіях та соціальних відносинах [62].

Соціальні групи в науці розглядаються як психологічні спільності людей, які мають спільну ідентичність і групову психологію. У суспільних науках існує низка класифікацій соціальних груп, відповідно до яких поділяються на

великі, малі, первинні, вторинні, формальні, неформальні, стійкі, нестійкі, відкриті та закриті.

У контексті дослідження будемо розглядати великі та малі групи, оскільки зазначені групи відрізняються згідно з психологією. Під великою соціальною групою розуміється реальна, значна за розмірами, складно організована спільність людей, залучених у певну суспільну діяльність.

Вищим рівнем великих соціальних груп є суспільство, яке існує в межах державних кордонів. На наступному рівні виділяються різні види великих соціальних груп щодо соціальної стратифікації: соціальні класи, соціальні верстви, етнічні групи, гендерні та вікові групи.

Під малою соціальною групою розуміється нечисленна за складом група, члени якої об'єднані загальною соціальною діяльністю й перебувають в особистому спілкуванні, що є основою виникнення емоційних відносин і групових процесів. Приклади малої соціальної групою численні. До них можна віднести сім'ю, навчальний клас, трудовий колектив, спортивну команду. Великі та малі соціальні групи переважно є об'єктами впливу невибіркового чи обмежено вибіркового інформаційного впливу з боку засобів масової комунікації або під час масових онлайн заходів. Новим видом соціальних груп, що виник завдяки розвитку соціальних Інтернет-сервісів, стали віртуальні групи.

Формування та існування віртуального співтовариства як соціальної групи можливо за наявності в учасників мережевого ресурсу спільних інтересів, спільної мети та організованих дій щодо досягнення, яка реалізуються в єдиному комунікативному просторі.

Пріоритетним об'єктом правового захисту від деструктивного інформаційного впливу на рівні соціальних груп є діти через особливу вразливість, зумовлену психологічними особливостями, охоплюючи некритичність сприйняття інформації, нестійкість ціннісних орієнтацій та поведінкових установок.

Щодо особистості об'єктом інформаційної безпеки є психіка. Психіка

людини визначається як системна властивість високоорганізованої матерії, що полягає в активному відображенні суб'єктом об'єктивного світу, у побудові суб'єктом невідчужуваної від нього картини світу та регуляції на цій основі поведінки та діяльності [63]. Впливаючи на картину світу людини, можемо впливати на поведінку.

Характеризуючи психологічні компоненти соціальних груп як об'єктів інформаційної безпеки, зіштовхуємося з певними труднощами, спричиненими відсутністю усталеного термінологічного апарату. Щодо суті, йдеться про групову психіку. Колективні психічні структури не зводяться до суми психіки членів соціальних груп, становлять самостійну соціальну реальність як відокремлені об'єкти інформаційної безпеки.

Автори навчального посібника «Соціальна психологія» зазначають, що групова психологія постає як певна соціальна реальність, яка виходить за межі свідомості окремого індивіда і впливає на неї разом з іншими об'єктивними умовами життя [64, с. 138-139]. Більшість психічних характеристик соціальних груп сприймаються як елементи групової свідомості.

На другому рівні як об'єкти інформаційної безпеки визначені: психіка людини, що охоплює свідомість і несвідоме, групові психічні структури, що складаються з групової свідомості та колективної несвідомої.

На третьому рівні деталізації ми повинні виділити дрібніші психічні компоненти індивідуальної та групової психіки, які можуть бути об'єктом інформаційного впливу. Що стосується елементів індивідуальної психіки, то тут у психології сформовано чіткий понятійний апарат [65, с. 11-12].

Для системного вивчення використовуємо два підходи – динамічний та статичний. Динамічний підхід передбачає виділення у структурі психіки психічних процесів, які поділяються на три основні види: когнітивні, емоційні та регулятивно-вольові [65]. Статичний виходить із виділення психічних утворень, що є результатами проходження психічних процесів.

Незважаючи на складність та трудомісткість завдання побудови переліку психічних процесів та утворень, вирішення має значення для правильної

ідентифікації об’єктів правового захисту.

На відміну від загальної психології, соціальна психологія не має усталеного категоріального апарату для позначення елементів групової психіки. Одні поняття («групові інтереси», «громадська думка», «групова ідентичність») мають широке визнання та використання в науці, тоді як інші («групове мислення») трапляються лише в окремих дослідженнях.

Столяренко О. Б. виділив серед психологічних характеристик групи такі елементи: групові потреби, інтереси, цінності, норми, цілі, групова думка [65].

Автори підручника «Основи соціальної психології» зазначають, що, ведучи мову про соціально-психологічні механізми впливу, треба виходити з того, що один суб’єкт психічної активності своїми діями може викликати певну психічну активність іншого суб’єкта, а саме: певні відчуття, уявлення, спогади, думки, почуття, ставлення, мотиви, вольові дії тощо. Найбільш відомими в соціальній психології є такі механізми, як переконування, навіювання, санкціонування, наслідування, психічне зараження, маніпулювання. У практиці організації впливів відомо чимало випадків, коли правильно застосований механізм давав змогу досягти дивовижних результатів, а соціально-психологічна некомпетентність призводила до ефектів, протилежних очікуваним [66, с. 224].

Підсумовуючи проведений аналіз, доцільно виділити три основні групи об’єктів інформаційної безпеки:

- особистість, малі та великі соціальні групи, суспільство;

- психіка людини, групові психічні структури;

- індивідуальні та групові психічні процеси.

Науковці О. Д. Довгань та Т. Ю. Ткачук під негативним інформаційно-психологічним впливом розуміють такий вплив на особу чи групу осіб, який здійснюється на їх психіку, зокрема й усупереч їхній волі, із застосуванням спеціальних засобів і методів, що призводить до шкідливих для людини, суспільства та держави наслідків [10, с. 89].

На основі вищевикладеного визначаємо інформаційну безпеку як

складову частину системи національної безпеки, що становить стан захищеності особи, соціальних груп, суспільства від деструктивного інформаційного впливу.

Щодо інформаційної безпеки держави, то вчені зазначають, що чинниками забезпечення інформаційної безпеки держави є гарантування:

- безпеки інформації загального доступу, мереж зв'язку, інформаційно-телекомунікаційних систем, технічних та програмних засобів виконання маніпуляцій з інформацією, доступу до інформації;

- конфіденційності інформації з обмеженим доступом;

- захищеності особи, суспільства й держави від шкідливого впливу певних видів інформації (у цьому разі йдеться не про інформацію, віднесену до категорій з обмеженим доступом, а про такі види, котрі здатні зашкодити вказаним суб'єктам інформаційних відносин).[10, с. 89].

Такий підхід передбачає завдання визначені Стратегією інформаційної безпеки України. Засади інформаційної безпеки визначені в документах Європейського Союзу: Tackling online disinformation: a European Approach; Action Planagainst Disinformation, EU Codeof Practiceon Disinformation, у рекомендаціях Європейської Комісії та висновках Європейської ради [67, с. 28].

У монографії «Національна безпека: світоглядні та теоретико-методологічні засади» за загальною редакцією О. П. Дзьобаня (2021 рік) інформаційна безпека розглядається передусім як інформаційна безпека особистості, у подальшому на підставі безпеки особи забезпечення інформаційної безпеки суспільства та держави [68].

Науковці П. В. Квіткін, І. В. Дятлова та Л. О. Петрова зазначають, що актуальності проблема інформаційної безпеки особистості набуває для українського суспільства, яке є об'єктом інформаційно-пропагандистських та інформаційно-психологічних операцій противника (Російська Федерація). Реаліями сьогодення є проблеми в соціально-економічному розвитку країни, процесів політичної і духовної сфер суспільної життєдіяльності, які використовуються для дискредитації внутрішньої та зовнішньої політики

держави, національно-історичних цінностей і євроатлантичних прагнень українського народу.

Актуальність проблеми зумовлена наявністю протилежних підходів до розуміння сутності інформаційної безпеки особистості. У нормативно-правових актах і дослідженнях науковців домінують два основні підходи до вирішення проблеми: розуміння сутності інформаційної безпеки суспільства й особистості через захищеність, або як здатність суб'єкта зберігати свої системоутворювальні властивості й основні характеристики за впливів на кіберпростір, інформаційно-комунікаційні технології, як характеристика стану соціальної спільноти [69, с. 47].

Розглянувши методологічні підстави дослідження інформаційної безпеки в інформаційному праві, можемо зробити такі висновки.

Дослідження інформаційної безпеки характеризується обмеженістю конкретних дисциплінарних підходів та обґрунтуванням міждисциплінарної методології дослідження. Міждисциплінарний підхід вимагає пошуку та використання дієвих засобів, що допомагають поєднувати різноманітні – правові та не правові – методи аналізу правозастосовної діяльності, внаслідок чого дослідник максимально наближається до об'єкта, що вивчається. Міждисциплінарний методологічний аналіз дає можливість вийти за межі різноманітних дисциплінарних підходів до цієї проблеми, оскільки він дає можливість:

- розглядати інформаційну взаємодію у суспільстві у двох площинах: як суб'єкт-об'єктна та суб'єкт-суб'єктна взаємодія; для першого типу взаємодії характерне споживання та використання інформації, для другого типу міжсуб'єктна інформаційна взаємодія;

- забезпечувати інтегративну єдність різноманіття індивідуально-особистісних соціальних ролей та цінностей людей у глобальній інформаційній взаємодії, універсалізацію нових цінностей культури інформаційного суспільства – інформаційних цінностей;

- розглядати проблему інформаційної безпеки як гуманітарну проблему.

Зазначена методологія охоплює принципи: еволюційного розвитку, згідно з яким інформаційна безпека в інформаційну епоху, будучи системною якістю, має здатність саморозвитку, відбиваючи вектори соціальної динаміки та втілюючи один із важливих елементів цієї динаміки; цілісності, згідно з якою інформаційна безпека в інформаційну епоху – це цілісна якість із набором невід'ємних атрибутів; системності та багатофакторності, згідно з якими інформаційна безпека є системною та багатофакторною якістю, що виражається в єдності множинності особистісних, громадянських, професійних та соціальних характеристик.

1.2. Характеристика системи правового забезпечення інформаційної безпеки в умовах цифрової трансформації

Стимульовані інформаційними технологіями економічні та соціальні перетворення, загальна інформатизація, використання інформації як одного з ефективних засобів впливу на суспільну свідомість та технологічний прогрес, поява нових форм відносин в умовах активного інформаційного обміну призводять до необхідності перегляду принципів взаємодії в системі держава-суспільство-особа.

Настання інформаційного суспільства трансформує звичні моделі економічної, соціальної, політичної діяльності, що тягне перебудову державно-правової діяльності з урахуванням нових умов інформаційної відкритості та необхідності вирішення проблем забезпечення інформаційної безпеки.

Розвиток інформаційно-комунікаційних технологій та процесів цифрової трансформації ставить завдання реформування системи правового регулювання суспільних відносин у різних сферах. Це особливо актуально стосовно нових викликів цифрового середовища, кількість та небезпека яких стрімко зростають.

З початку нового тисячоліття процес нормативного регулювання інформаційної безпеки значно активізувався, особливо у зв'язку з ухваленням

Окінавської хартії глобального інформаційного суспільства та Доктрини інформаційної безпеки України (2009 рік) [70; 33]. Загалом, за останні двадцять років було проведено значну роботу, спрямовану на розвиток правового забезпечення інформаційної безпеки.

Останнім десятиліттям ця сфера законодавства стала однією з динамічних. Фрагментарні зміни, що вносяться в інформаційне та інше галузеве законодавство, викликані поточними проблемами, позбавлено системності та опори на наукову основу.

А. Ю. Нашинець-Наумова у монографії «Інформаційна безпека: питання правового регулювання» (2017 рік) зазначає, що сьогодні проблематика інформаційної безпеки держави досліджується в роботах багатьох українських учених: І. В. Арістової, В. К. Гіжевського, І. П. Голосніченка, Ю. В. Іщенка, Р. А. Калюжного, В. А. Ліпкана, В. С. Цимбалюка, М. Я. Швеця та інших. Проте зазначені дослідження та наукові праці стосувалися лише національної безпеки в інформаційній сфері. Залишаються недостатньо вивченими концептуальні засади системи забезпечення інформаційної безпеки держави [71, с. 27-28].

М. В. Гончаров, розглядаючи тенденції наукових поглядів у сфері нормативно-правового забезпечення інформаційної безпеки України (2022 рік), зазначає, що нормативно-правове забезпечення інформаційної безпеки в цілому та на елементному рівні характеризується науковістю, системністю та має багато аспектів. Нормативно-правове забезпечення інформаційної безпеки є науково обґрунтована, послідовна система правових засобів, за допомогою яких громадянське суспільство та держава здійснює вплив на інформаційні відносини та відносини, безпосередньо пов’язані з розробкою інформаційної безпеки країни, виходячи з черговості завдань і поставлених цілей, які існують перед суспільством [72, с. 26].

Аналізуючи систему правового забезпечення інформаційної безпеки, беремо за основу запропонований І. М. Шопіною концептуальний підхід до вирішення правових проблем забезпечення інформаційної безпеки [73, с. 137].

Цей підхід передбачає вивчення правових засобів забезпечення інформаційної безпеки у нерозривному зв'язку з цілями, завданнями та механізмами реалізації державної політики щодо забезпечення інформаційної безпеки.

Спроба детальної правової регламентації базових аспектів забезпечення інформаційної безпеки здійснювалася у законопроєкті «Про засади інформаційної безпеки України» [57]. У проєкті закону було визначено принципи забезпечення інформаційної безпеки, основні завдання державної політики у сфері забезпечення інформаційної безпеки, функції державної системи забезпечення інформаційної безпеки.

Поняття «забезпечення безпеки» належить до базових категорій у теорії безпеки. Термін «забезпечення», що лежить в основі, орієнтує на активну діяльність певних суб'єктів, спрямовану на досягнення стану захищеності об'єктів безпеки [74]. Змістом діяльності є реалізація уповноваженими суб'єктами політичних, правових, військових, соціально-економічних, інформаційних, організаційних та інших заходів, спрямованих на протидію загрозам національній безпеці.

У Стратегії інформаційної безпеки України забезпечення інформаційної безпеки визначається як здійснення комплексу взаємопов'язаних організаційних, правових та інших заходів щодо прогнозування, виявлення, стримування, запобігання, відображення інформаційних загроз та ліквідації їх негативних наслідків.

У Законі України «Про основи національної безпеки України», так само як і в законі, що прийшов йому на зміну «Про національну безпеку України», у забезпеченні безпеки виділено два рівні: державна політика у сфері забезпечення безпеки; діяльність із забезпечення безпеки [75: 28].

Такий підхід підтримується в науковій літературі. Суть такого розмежування зводиться до того, що на першому рівні здійснюється стратегічне планування забезпечення безпеки (постановка цілей, завдань, напрямів, визначення суб'єктів, форм і методів реалізації), на другому – безпосередня

реалізація системи заходів забезпечення безпеки відповідно до виробленого плану.

Під забезпеченням інформаційної безпеки розуміємо діяльність державних інститутів, інститутів громадянського суспільства щодо вироблення та реалізації системи правових, організаційних, інформаційних і інших заходів, спрямованих на забезпечення захищеності особи, соціальних груп та суспільства від деструктивного інформаційного впливу.

Поряд із протидією інформаційним загрозам до змісту забезпечення інформаційної безпеки додано заходи щодо підвищення стійкості людини, соціальних груп та суспільства до впливу загроз.

Останній напрям має важливе значення через неможливість повного захисту соціальних суб'єктів від негативного психологічного впливу та недостатньою ефективністю систем фільтрації інформації.

Третій змістовий блок забезпечення інформаційної безпеки становлять заходи щодо впливу на інформаційне середовище, у якому здійснюється деструктивний інформаційний вплив на особистість та соціальні групи. Активізуючи позитивні чинники та нейтралізуючи негативні елементи цифрового середовища, можна підвищувати рівень захищеності об'єктів. Цей напрям укладається в концепцію «інформаційної екології», що передбачає створення певного стану інформаційного середовища, безпечного для фізичного та психічного здоров'я людини, індивідуальної, групової та суспільної психології. Інформаційна екосистема – це система, що складається з людини, інформації, інформаційного середовища та інформаційних технологій [76].

Діяльність із забезпечення інформаційної безпеки охоплює чотири основні елементи: протидія джерелам загроз інформаційної безпеки; нівелювання чи зменшення деструктивного впливу загроз на об'єкти інформаційної безпеки; збільшення стійкості об'єктів щодо деструктивного інформаційного впливу; надання впливу на елементи цифрового середовища.

Заходи забезпечення інформаційної безпеки охоплюють: регулювання,

зокрема обмеження інформаційних потоків; організація інформаційних потоків, зокрема ініціювання поширення певної інформації; поширення способів й засобів обробки та оцінки інформації; формування групового і індивідуального психологічного захисту.

Важливу роль у механізмі забезпечення інформаційної безпеки відіграє правове забезпечення, оскільки саме право встановлює цілі, завдання та напрями забезпечення, регламентує форми, засоби та методи діяльності уповноважених суб'єктів щодо протидії загрозам інформаційної безпеки.

М. В. Гончаров визначає правове забезпечення національної безпеки як взаємопов'язану та впорядковану сукупність нормативно-правових актів, які закріплюють юридичні принципи та норми правового регулювання суспільних відносин у галузі забезпечення національної безпеки. Нормативно-правове забезпечення є більш широким поняттям порівняно з нормативно-правовим регулюванням, оскільки нормативно-правове регулювання може розглядатись лише як складова забезпечення інформаційної безпеки [72, с. 26].

Таке визначення, на нашу думку, не є повною мірою правильним. Правове забезпечення, як будь-яке забезпечення, являє собою певну діяльність з урахуванням реалізації системи заходів. Тому недоцільно зводити систему правових засобів до нормативно-правових актів.

Ґрунтовний аналіз поняття правового забезпечення інформаційної сфери провів О. А. Баранов. Вчений зіставляє його з більш розробленими в теорії права категоріями «правове регулювання» та «правовий вплив». Зрештою, учений дійшов висновку, що правове забезпечення охоплює правове регулювання та елементи правового впливу. До останніх відносить правосвідомість, правову культуру, правові принципи. У монографії «Правове забезпечення інформаційної сфери: теорія, методологія і практика» О. А. Баранов у контексті правового забезпечення забезпечувальних заходів, фрагментарно звертає увагу на заходи матеріально-технічного, організаційно-управлінського, кадрового, ідеологічного характеру [77].

Охоплення змістом правового забезпечення забезпечувальних заходів

матеріально-технічного, організаційно-управлінського, кадрового, ідеологічного характеру не має підтримки в науковій і навчальній літературі [43; 78; 79; 80].

На думку авторів наукової статті «Проблеми та перспективи забезпечення інформаційної безпеки в органах прокуратури України», правове регулювання відносин у сфері забезпечення інформаційної безпеки передбачає встановлення певних правових норм, їх застосування та охорону від порушення з використанням державного примусу [81].

Автори дослідження «Особливості правового забезпечення інформаційної безпеки при використанні хмарних технологій органами державної влади» зазначають, що правове забезпечення інформаційної безпеки, крім правового регулювання відносин, охоплює правозастосовну діяльність [82].

На нашу думку, правове забезпечення безпеки охоплює не тільки нормотворчість та застосування права, а й інші форми реалізації права. У теорії права визначають чотири форми реалізації права: дотримання, виконання, використання, застосування [83, с. 55]. Визначення правового забезпечення інформаційної безпеки доцільно через поняття «правові засоби», що лежать в основі механізму правового регулювання [84, с. 26].

Н. В. Заяць визначає правові засоби як інституційні явища правової дійсності, що втілюють регулятивну силу права. Правові засоби – явище багатоаспектне, ця категорія використовується щодо права в цілому, у процесі аналізу правового регулювання, щодо прав людини, до правових режимів тощо [85, с. 205].

Н. Д. Гетманцева та Г. Г. Митрицька розглядають правові засоби, що становлять складник механізму правового регулювання, слугують для того, щоб досягнути кінцевої мети правового регулювання трудових відносин. Було б неправильним очікувати постановку кінцевої правової мети й визначення правових засобів, спрямованих на її досягнення, лише в нормативному правовому акті, вихідному від держави, оскільки в установленні кінцевої правової мети та виробленні відповідних їй правових засобів беруть участь

суб'єкти всіх рівнів: державного, індивідуально-договірного й колективно-договірного регулювання [86, с. 139].

Л. В. Вакарюк, характеризуючи правові засоби, які є елементами механізму правового регулювання, виділяє: норми права, юридичні факти, правовідносини, акти реалізації права та правозастосовні акти [87, с. 16].

Правове забезпечення інформаційної безпеки доцільно розглядати як діяльність із розробки та реалізації системи правових засобів, спрямованих на забезпечення захищеності особи, соціальних груп та суспільства від деструктивного інформаційного впливу.

У науці та документах стратегічного планування в галузі національної безпеки перед постановкою цілей та завдань забезпечення безпеки прийнято визначати національні інтереси.

У Стратегії національної безпеки України вони визначені як об'єктивно значущі потреби особистості, суспільства та держави у безпечному та сталому розвитку. Щодо інформаційної сфери національні інтереси визначаються тією роллю, яку відіграє інформація, інформаційна інфраструктура в забезпеченні сталого розвитку нації в конкретних історичних умовах.

Стратегія державної безпеки України закріплює національні інтереси України на сучасному етапі як захист конституційного ладу, суверенітету, незалежності, державної та територіальної цілісності України, зміцнення оборони країни; підтримання громадянського миру та згоди в країні; розвиток безпечного інформаційного простору; захист суспільства від деструктивного інформаційного впливу; зміцнення традиційних духовно-моральних цінностей, збереження культурної та історичної спадщини народу України.

Захист від деструктивного інформаційного впливу вперше виділено як один із національних інтересів у базовому документі стратегічного планування. У цьому плані необхідне внесення низки змін та доповнень до чинної Стратегії інформаційної безпеки України, у якій захист від деструктивного інформаційного впливу безпосередньо не відображено.

Окремі сутнісні елементи таких потреб проглядаються у формулюваннях

більш загальних національних інтересів, пов’язаних із захистом основних прав і свобод в інформаційній сфері, забезпечення безпеки в галузі культури, суверенітету країни, зміцнення національної згоди, політичної та соціальної стабільності, збереження традиційних цінностей та національної ідентичності (Національна стратегія у сфері прав людини, Довгострокова стратегія розвитку української культури – стратегія реформ [88; 89]).

З урахуванням проведеного аналізу вважаємо за можливе сформулювати перелік національних інтересів України в інформаційній сфері, що стосуються забезпечення інформаційної безпеки: забезпечення та захист конституційних прав і свобод людини та громадянина, охоплюючи право на свободу, недоторканість приватного життя, захист честі та доброго імені, свободу думки та слова, право на інформацію та свободу масової інформації; формування середовища довіри в цифровому середовищі; забезпечення доступу до інформації, що сприяє розвитку особистості та суспільства; захист особи, соціальних груп та суспільства від деструктивного інформаційного впливу; гарантування психічного здоров’я та благополуччя громадян; збереження традиційних духовно-моральних цінностей та національної ідентичності суспільства, підвищення культурного потенціалу країни; зміцнення національної згоди, політичної та соціальної стабільності; забезпечення інформаційного суверенітету України у контексті асоціації України і Європейського Союзу; покращення іміджу України та підвищення авторитету на міжнародній арені, посилення політичного та культурного впливу України у світі; сприяння формуванню системи інформаційної безпеки, спрямованої на протидію загрозам деструктивного інформаційного впливу на особистість, соціальні групи та суспільство, заснованої на стандартах Північноатлантичного альянсу (НАТО) та Європейського Союзу; входження у Європейський інформаційний простір.

У Стратегії національної безпеки України безпосередньо мета забезпечення інформаційної безпеки не визначена. Узагальнення інформаційних положень та зміцнення суверенітету в інформаційному просторі

і є метою забезпечення інформаційної безпеки [27].

У Стратегії інформаційної безпеки України загальну стратегічну мету забезпечення інформаційної безпеки визначено як 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 [58].

Стратегічною метою забезпечення інформаційної безпеки є підтримка стану захищеності особистості, соціальних груп та суспільства від деструктивного інформаційного впливу, що забезпечує гарантовану реалізацію національних інтересів України.

На наступному рівні визначення цілі необхідно дати характеристику завдань та функцій забезпечення інформаційної безпеки. Щодо завдань і функцій забезпечення інформаційної безпеки, то загальноприйнятого уявлення про завдання та функції забезпечення безпеки немає.

Аналіз Закону України «Про національну безпеку України» та документів стратегічного планування в галузі забезпечення національної безпеки показує відмінності в переліку завдань та функцій.

У ч. 2 ст. 36 Закону України «Про національну безпеку України» зазначено, що Стратегія національної безпеки України визначає: напрями та завдання реформування й розвитку сектору безпеки й оборони (пункт 4). У Стратегії національної безпеки України вказано, що держава повинна виконувати лише необхідні функції, насамперед безпекову, зовнішньополітичну, соціальну, регуляторну (пункт 50), а завдання не вказані.

У Законопроєкті «Про засади інформаційної безпеки України» було розмежовано завдання та функції забезпечення інформаційної безпеки. Але, аналізуючи відповідні положення, ми помітили їхнє часткове дублювання.

У Стратегії інформаційної безпеки України завдання забезпечення інформаційної безпеки не виділено, а його основні напрями визначено стосовно

окремих сфер державного управління: інформаційний вплив Російської Федерації як держави-агресора на населення України; інформаційне домінування Російської Федерації як держави-агресора на тимчасово окупованих територіях України; обмежені можливості реагування на дезінформаційні кампанії; несформованість системи стратегічних комунікацій; недосконалість регулювання відносин у сфері інформаційної діяльності та захисту професійної діяльності журналістів; спроби маніпуляції свідомістю громадян України щодо європейської та євроатлантичної інтеграції України; доступ до інформації на місцевому рівні; недостатній рівень інформаційної культури та медіаграмотності в суспільстві для протидії маніпулятивним та інформаційним впливам [58].

Позитивно вирізняється в цьому плані Стратегія державної безпеки України, де чітко окреслено основні завдання забезпечення інформаційної безпеки. Так, до сфери інформаційної безпеки належать:

- формування безпечного середовища обороту достовірної інформації в цифровому середовищі;

- розвиток системи прогнозування, виявлення та попередження загроз інформаційній безпеці України, визначення їх джерел, оперативної ліквідації наслідків реалізації таких загроз;

- створення умов для ефективного попередження, виявлення та припинення правопорушень, скоєних з використанням інформаційно-комунікаційних технологій;

- протидія використанню інформаційної інфраструктури терористичними організаціями, спеціальними службами та пропагандистськими структурами іноземних держав для здійснення деструктивного інформаційного впливу на громадян та суспільство.

Крім основного тематичного підрозділу, Стратегія державної безпеки України, положення про забезпечення інформаційної безпеки наявні в інших розділах документа, присвячених обороні країни, державній та громадській безпеці, захисту традиційних духовно-моральних цінностей, культури та

історичної пам’яті, стратегічній стабільності та взаємовигідному міжнародному співробітництву.

Аналіз Стратегії державної безпеки України дозволяє виділити додаткові завдання забезпечення інформаційної безпеки: підтримання морально-політичного та психологічного стану особового складу Збройних сил України та інших військових формувань, військово-патріотичне виховання; недопущення втручання у внутрішні справи України, припинення розвідувальної та іншої діяльності іноземних держав та окремих осіб проти національних інтересів України; попередження та нейтралізація соціальних, міжконфесійних та міжнаціональних конфліктів, деструктивних релігійних течій; реалізація державної інформаційної політики щодо зміцнення сприйняття суспільством євроатлантичних пріоритетів та європейських культурно-історичних цінностей, неприйняття громадянами деструктивних ідей, стереотипів; зміцнення культурного суверенітету України та збереження єдиного культурного простору, захист суспільства від зовнішнього деструктивного інформаційного впливу.

Стратегія національної безпеки України та Стратегія державної безпеки України детально визначає завдання щодо забезпечення інформаційної безпеки. Більша частина завдань закріплена в межах забезпечення неінформаційної безпеки та інших стратегічних національних пріоритетів.

При визначенні завдань забезпечення інформаційної безпеки важливо уникати низки методологічних установок, властивих законодавчим актам та документам стратегічного планування у сфері безпеки, на що звернули увагу автори колективної монографії «Національна безпека: світоглядні та теоретико-методологічні засади» [68, с. 456-470]. Вони полягають у змішуванні основних і забезпечувальних, загальних та приватних завдань забезпечення безпеки.

Альтернативно вчені пропонують розглядати як основні завдання забезпечення безпеки виявлення загроз безпеці та протидію їм, а до допоміжних завдань відносять: управління процесом забезпечення безпеки; підбір, підготовку та розташування сил та засобів забезпечення безпеки;

матеріально-технічне та фінансове забезпечення діяльності із забезпечення безпеки.

Теоретичні положення вказаної монографії доцільно використати при визначенні завдань інформаційної безпеки з урахуванням застережень: підтримати розмежування основних і допоміжних завдань забезпечення безпеки, але доцільно їх викласти в єдиному переліку; термін «допоміжні завдання» є не цілком вдалим, оскільки вирішення багатьох з них (постановка цілей, правове регулювання, визначення сил і засобів) передує діяльності з забезпечення безпеки; доцільно трактувати протидію загрозам з урахуванням підходів, що застосовуються у чинному законодавстві, як діяльність, що охоплює компоненти: профілактику загроз; боротьбу з загрозами (виявлення, попередження, припинення, правове переслідування); мінімізацію та ліквідацію наслідків впливу загроз; доцільно розширити кількість основних завдань забезпечення безпеки стосовно сфери інформаційної безпеки, доповнивши їх підвищенням життєстійкості об’єктів інформаційної безпеки в умовах розвитку цифрової трансформації, інформаційну безпеку державних інформаційних ресурсів, захисту інформації, у тому числі персональних даних у контексті частини 2 статті 7 розділу ІІ проєкту Закону України «Про Національну програму інформатизації» [90].

Узагальнюючи вищевикладене, до завдань забезпечення інформаційної безпеки слід зарахувати: прогнозування, виявлення, аналіз та оцінку загроз інформаційній безпеці, у тому числі щодо Законів України «Про боротьбу з тероризмом», «Про запобігання корупції» [91; 92]; аналіз та оцінку вразливості особи, соціальних груп і суспільства від деструктивного інформаційного впливу; стратегічне планування у сфері забезпечення інформаційної безпеки; правове регулювання у сфері забезпечення інформаційної безпеки; застосування комплексу оперативних та довготривалих заходів щодо превенції, припинення та усунення загроз інформаційній безпеці, мінімізації та ліквідації наслідків впливу; застосування комплексу оперативних і довготривалих заходів щодо підвищення здатності особи, соціальних груп та суспільства протистояти

деструктивному інформаційному впливу; організацію діяльності системи забезпечення інформаційної безпеки; кадрове, інформаційне, матеріально-технічне та фінансове забезпечення діяльності суб'єктів забезпечення інформаційної безпеки; співробітництво у сфері забезпечення інформаційної безпеки з країнами Європейського Союзу та Організації Північноатлантичного Союзу.

У цьому випадку доцільно говорити про системність законодавства, що проявляється в тому, що внутрішні елементи системи законодавства (нормативно-правові акти) взаємопов'язані – перебувають у координаційних (залежно від предмета правового регулювання) і субординаційних (залежно від юридичної сили) зв'язках [91, с. 46].

За умов розвитку глобального інформаційного суспільства значущою теоретичною проблемою інформаційного права стає відокремлення функцій держави щодо забезпечення інформаційної безпеки. Виділення напрямів забезпечення інформаційної безпеки є важливим не тільки для визначення предметного змісту діяльності уповноважених суб'єктів, але вказівки на основні вектори формування та розвитку законодавства в цій сфері.

Теоретично функції управління розглядаються як напрями (види) управлінської діяльності, які забезпечують досягнення мети управління та здійснювані спеціальними прийомами та методами.

Функція управління – це стійка сукупність завдань (операцій, дій) щодо реалізації процесу управління задля досягнення приватних цілей управління, засновану на розподілі управлінської праці органів управління.

В управлінні прийнято виділяти функції управління: планування, організація, координація, контроль. Стосовно галузі безпеки таке трактування функцій не коректне, оскільки позначає стадії управлінського процесу, а не орієнтує на напрями діяльності суб'єктів забезпечення безпеки.

У науковій літературі виділяють кілька функцій управління: функції-операції, що є функціями процесу управління, та функції-завдання, що є функціями системи управління.

Необхідно брати до уваги думку В. Б. Авер'янова про те, що у конкретній системі поняття «функція» залежить від сутності та сфери управління. Функція управління взагалі набуває змісту щодо конкретного історичного соціального організму – його системи, окремих частин [94, с. 260]. Це зобов'язує брати до уваги специфіку виду безпеки, що вивчається, та діяльності щодо забезпечення.

З урахуванням проведеного аналізу Закону України «Про національну безпеку України», документів стратегічного планування у галузі національної та інформаційної безпеки, Стратегії інформаційної безпеки України, наукової літератури за темою дисертаційного дослідження, дисертантка розробила концепцію основних напрямів (функцій) забезпечення інформаційної безпеки щодо захисту від деструктивного інформаційного впливу відповідно до Законів України «Про внесення змін до деяких законів України щодо заборони виготовлення та поширення інформаційної продукції, спрямованої на пропагування дій держави-агресора» [95-100].

При визначенні напрямів забезпечення безпеки недоцільно змішувати діяльність щодо вирішення основних та забезпечувальних завдань. Для визначення основних завдань напрями діяльності державних органів відштовхуються від загроз безпеки та сфер прояву (наприклад, протидія діяльності російських та іноземних спецслужб щодо деструктивного інформаційного впливу).

У кожному з напрямів діяльності необхідне вирішення однотипних забезпечувальних завдань у межах вироблення та реалізації державної політики забезпечення інформаційної безпеки (стратегічне планування, правове регулювання, матеріально-технічне забезпечення, підготовка кадрів).

Напрями діяльності щодо забезпечення інформаційної безпеки доцільно розглядати з позиції системного підходу, що використовується у правовій інформатиці. Діапазон проблем, що досліджуються та розв'язуються правовою інформатикою, від опрацювання правових даних до отримання нових знань і ухвалення управлінських рішень в інтересах громадян, суспільства, законодавчої, виконавчої та судової влади [101, с. 167].

З погляду на дослідження Л. М. Петренко «Системний підхід у правовій інформатиці», доцільно розробити два переліки: основних напрямів забезпечення інформаційної безпеки та основних напрямів діяльності щодо вироблення та реалізації державної політики забезпечення інформаційної безпеки [101]. Це, на нашу думку, зменшить негатив сучасної правозастосовної діяльності – відсутність узгодженості в правовому впливі на соціальні та економічні процеси.

Основні напрями забезпечення інформаційної безпеки: прогнозування, виявлення, аналіз та оцінка загроз інформаційній безпеці; протидія поширенню негативної інформації у засобах масової інформації та мережі Інтернет; протидія терористичній та сепаратистській пропаганді та вербувальній діяльності, розпалюванню національної чи соціальної ненависті та ворожнечі; протидія деструктивному інформаційному впливу з боку державних органів та спеціальних служб Росії та іноземних держав, російських неурядових організацій; забезпечення інформаційно-психологічної безпеки дітей та молоді; захист честі, гідності та ділової репутації громадянина, ділової репутації юридичної особи; захист органів публічної влади, посадових осіб від деструктивного інформаційного впливу; протидія фальсифікації історії України, у тому числі щодо єдності українського і російського народів; протидія поширенню деструктивних субкультур та інших форм негативного інформаційного впливу у духовній сфері у контексті пропаганди «русского мира и единства России и Украины»; протидія кримінальним та адміністративним правопорушенням, пов’язаним з наданням деструктивного інформаційного впливу; інформування української та зарубіжної громадськості про внутрішню та зовнішню політику України, офіційну позицію щодо соціально значущих подій в Україні та міжнародному житті; ведення контрпропаганди в Україні та за кордоном; формування цифрової грамотності громадян та культури інформаційної безпеки.

Цифрова грамотність («цифрова» компетентність) визнана Європейським Союзом однією з 8 ключових компетенцій для повноцінного життя та

діяльності. У 2016 році Європейський Союз презентував оновлений фреймворк Digital Competence (DigComp 2.0), що складається з п’яти основних блоків компетенцій: інформаційна грамотність та грамотність щодо роботи з даними; комунікація та взаємодія; цифровий контент; інформаційна безпека; вирішення проблем [102, с. 292].

Основні напрями діяльності з вироблення та реалізації державної політики забезпечення інформаційної безпеки щодо деструктивного інформаційного впливу: стратегічне планування у сфері забезпечення інформаційної безпеки; правове регулювання у сфері забезпечення інформаційної безпеки;здійснення державного контролю та нагляду у сфері забезпечення інформаційної безпеки; надання державних (адміністративних) послуг у сфері забезпечення інформаційної безпеки; координація діяльності суб’єктів забезпечення інформаційної безпеки; організація матеріально-технічного, фінансового та інформаційного забезпечення діяльності суб’єктів забезпечення інформаційної безпеки; проведення наукових досліджень у галузі забезпечення інформаційної безпеки; підготовка кадрів у галузі забезпечення інформаційної безпеки; здійснення міжнародного співробітництва у сфері інформаційної безпеки.

У Стратегії інформаційної безпеки України закріплено, що забезпечення інформаційної безпеки здійснюється на основі поєднання законодавчої, правозастосовної, правоохоронної, судової, контрольної та інших форм діяльності державних органів у взаємодії з органами місцевого самоврядування, фізичними та юридичними особами.

Ця діяльність здійснюється у звичайних і в особливих умовах спеціальних правових режимів. У Стратегії інформаційної безпеки України спеціально виділено низку напрямів забезпечення інформаційної безпеки в надзвичайних ситуаціях, що має суттєве значення в умовах воєнного стану [103].

До базових принципів забезпечення безпеки згідно Закону України «Про національну безпеку України» входить системність та комплексність

застосування органами публічної влади політичних, організаційних, соціально-економічних, інформаційних, правових та інших заходів забезпечення безпеки.

Реалізація цього принципу у сфері державного управління передбачає наявність системи забезпечення національної безпеки в Україні та відповідних підсистем забезпечення окремих видів безпеки. У чинному Законі України «Про національну безпеку України» поняття системи забезпечення безпеки не використовується.

Законодавці виділяли в системі забезпечення безпеки два основні елементи: інституційний (суб'єкти забезпечення безпеки) та нормативний (законодавство у сфері забезпечення безпеки).

У документах стратегічного планування став застосовуватися дещо інший підхід до визначення системи забезпечення безпеки. Виділено такі елементи, як сили та засоби забезпечення безпеки.

Цей підхід знайшов відображення у Стратегії національної безпеки України та Стратегії інформаційної безпеки України [27; 58]. Під силами забезпечення інформаційної безпеки розуміються державні органи, підрозділи та посадові особи державних органів, органів місцевого самоврядування, уповноважені на рішення відповідно до законодавства завдань забезпечення інформаційної безпеки, а під засобами – правові, організаційні, технічні та інші засоби, які використовуються силами забезпечення інформаційної безпеки. У Стратегії національної безпеки України складовими частинами системи забезпечення національної безпеки визначено сукупність органів публічної влади та нормативно-правових актів.

Забезпечення інформаційної безпеки охоплює сили, засоби та методи, правове регулювання.

У Стратегії інформаційної безпеки України йдеться про те, що система забезпечення інформаційної безпеки України є частиною системи забезпечення національної безпеки країни. Відповідно, виходячи з розгляду інформаційної безпеки як елемента національної безпеки, маємо зробити висновок про те, що система забезпечення інформаційної безпеки є частиною системи

(підсистемою) забезпечення національної безпеки та охоплює особу, суспільство та державу.

Ця теза має певну частку умовності, оскільки виділення різних систем забезпечення окремих видів інформаційної безпеки (особи, суспільства, держави) є більшою мірою розумовим конструктом, що охоплює певні державні органи й інші суб'єкти забезпечення безпеки. Більшість таких суб'єктів багатофункціональні, що зумовлює одночасну участь у багатьох системах забезпечення безпеки.

Відповідно до теорії систем моносистема у контексті інформаційної безпеки має найвищий потенціал стабільності, оскільки охоплює всі напрями. Але необхідною та достатньою умовою є високий ступінь інтеграції елементів цієї системи та внутрішньосистемна взаємодія, орієнтована на співпрацю.

Однак подібна ситуація не відповідає реальному стану справ у контексті інформаційної безпеки особи, інформаційної безпеки суспільства та інформаційної безпеки держави, де фактично складається кілька центрів розвитку за напрямами забезпечення. У такій ситуації розвитку одного напряму властивий низький потенціал стабільності забезпечення за високої ресурсомісткості з боку держави.

Система забезпечення інформаційної безпеки представляє підсистему забезпечення безпеки, що охоплює сукупність сил забезпечення інформаційної безпеки, засобів і методів, що використовуються, правового регулювання відносин у сфері забезпечення інформаційної безпеки.

У структурі виділяються інституційна (сили), інструментальна (засоби та методи) та нормативна (правове регулювання) підсистеми. Нормативна підсистема – система правового забезпечення інформаційної безпеки – відіграє особливу роль, оскільки саме правовими нормами регламентується весь процес забезпечення безпеки, охоплюючи визначення суб'єктів, завдань та функцій, засобів і методів діяльності, що застосовуються.

Система правового регулювання забезпечення інформаційної безпеки в Україні характеризується ієрархічністю структури. Елементами цієї системи

виступають правові норми, суб'єкти правовідносин, правові засоби, методи та принципи регулювання. Цей висновок ґрунтується на представленні досліджуваного об'єкту у вигляді системи, яка охоплює цілісність об'єкту з урахуванням усіх внутрішніх і зовнішніх взаємозв'язків і чинників, що характеризують правові відносини в інформаційній сфері.

З урахуванням викладеного, систему правового забезпечення інформаційної безпеки щодо деструктивного інформаційного впливу можна визначити як упорядкований комплекс правових засобів, які використовуються для підтримки стану захищеності особи, соціальних груп і суспільства від деструктивного інформаційного впливу.

Наукове осмислення проблем захисту від деструктивного інформаційного впливу в Україні відбувалося хвилеподібно та було пов'язане з важливими законодавчими ініціативами, охоплюючи розробку законопроєкту «Про засади інформаційної безпеки України».

Фундаментом правової основи забезпечення інформаційної безпеки стали Закони України «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про захист суспільної моралі», «Про електронні комунікації» [37; 38; 50; 104].

Безпосередньо інформаційна безпека у Законі України «Про електронні комунікації» не вказується. Але зазначено у ч. 7 ст. 2, що безпека мереж і послуг – здатність електронних комунікаційних мереж і послуг протистояти діям, що становлять загрозу доступності, цілісності чи конфіденційності таких мереж і послуг, а також даних, що зберігаються, передаються чи обробляються, та пов'язаних із ними послуг, що надаються або доступ до яких здійснюється через електронні комунікаційні мережі чи послуги [104].

Воєнний стан вимагає переосмислення ієрархії суспільних відносин, що охороняються кримінальним законом, серед яких окреме місце виділено інформаційній безпеці, що відображено у Законі України «Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної

продукції» [105].

Соціальна обумовленість забезпечення інформаційної безпеки визначається сукупністю факторів: соціально-економічних, історичних, політичних та соціально-правових, які в сукупності відображають суспільну потребу в необхідності посилення заходів, спрямованих на забезпечення інформаційної безпеки кримінально-правовими засобами – виділення її як самостійного об'єкта правової охорони.

Незважаючи на те, що в ухвалених концептуальних документах щодо інформаційної безпеки не акцентовано увагу на необхідності дотримання «балансу інтересів», ця проблема залишається актуальною. Баланс інтересів особи, суспільства і держави забезпечується системним характером правового регулювання, що передбачає забезпечення інформаційної безпеки різними галузями права. Баланс інтересів в інформаційному праві передбачає встановлення юридичної відповідальності за посягання на інтереси особи, суспільства, держави в інформаційній сфері.

Не можна нормативно закріплювати переважне становище інтересів окремого суб'єкта, оскільки це призведе до порушення системних (конституційних за природою) властивостей такого складного об'єкта забезпечення, як інформаційна безпека.

Водночас в умовах воєнного стану, поєднаного з цифровою трансформацією, з метою прискореного розвитку економіки України, що позначено у Законі України «Про стимулювання розвитку цифрової економіки в Україні», забезпечення інформаційної безпеки охоплює усі напрями: інформаційну безпеку особи, інформаційну безпеку суспільства, інформаційну безпеку держави [106].

Інформаційна безпека як об'єкт забезпечення є відкритою динамічною системою суспільних відносин, що забезпечують реалізацію інтересів особи, суспільства та держави в інформаційній сфері; охоплює суспільні відносини, що забезпечують реалізацію права на інформацію та охорону інформації від неправомірного доступу; суспільні відносини, які забезпечують безпеку

інформаційних ресурсів; суспільні відносини, що забезпечують безпеку використання інформаційно-комунікаційних технологій.

Розглянувши характеристику системи правового забезпечення інформаційної безпеки, доцільно зробити наступні висновки.

Системи правового забезпечення інформаційної безпеки подана як сукупність наукових знань, що становлять зміст теорії систем права та теорії інформаційного права, що розвиваються. Зазначена система представлена як цілісне складне утворення, що розвивається,охоплює основні взаємопов'язані підгалузі, що регулюють предметні інформаційні відносини. Характеризується цілісністю, зв'язком між елементами просторовим і функціональним, структурою і організацією, рівнями системи та їх ієрархію, специфічним способом регулювання, самоорганізацію системи, її функціонуванням та розвитком.

Певний вплив формування системи правового забезпечення інформаційної безпеки щодо деструктивного інформаційного впливу надають суміжні наукові теорії, розвиток яких істотно впливає на науковий рівень теорії та систему інформаційного права: правова теорія організації правових систем, правова кібернетика, теоретико-інформаційні основи ухвалення управлінських організаційно-правових рішень, факторний аналіз.

Система правового забезпечення інформаційної безпеки розвивається на методологічній базі адекватного проблемно орієнтованого варіанта системного інформаційно-кібернетичного підходу на основі синергетики з розподілом на кібербезпеку та інформаційну безпеку особи, суспільства та держави.

Для переходу до цифрової економіки державі необхідно створити інформаційну інфраструктуру, у якій відкритість та прозорість даних поєднуються з рівністю можливостей окремих осіб в економіці (інклюзивна економіка) та ефективною системою інформаційної безпеки, яка захистить інтереси особи, суспільства і держави.

1.3. Інституціоналізація інформаційної безпеки у системі інформаційного права

Сьогодні цифрові технології є одним з головних двигунів зростання та технологічного розвитку економіки. Впровадження цифрових технологій сприяє підвищенню конкурентоспроможності різних секторів економіки, створенню нових можливостей для бізнесу у плані підключення до цифрових глобальних ланцюжків створення вартості, появі нових ринків, прискореному виведенню нових цифрових товарів на ринок. Процес цифровізації не відбувається в різних країнах світу одночасно, у зв'язку з чим спостерігається певний розрив у мірі цифровізації національних економік. Політика, правові норми, традиції та культура, досягнутий рівень економічного розвитку, рівень освіти та технологічної бази, багато інших факторів відіграють істотну роль у процесі цифрової трансформації економіки країни.

Унаслідок цифрової трансформації виникають нові контури цифрової економіки, для якої характерне зростання потоків даних. У цих умовах для суб'єктів стає важливим не сам факт володіння яким-небудь ресурсом, а наявність даних про цей ресурс і можливість його використання з метою планування діяльності. Цифрова економіка сприяє розвитку нових моделей бізнесу, дозволяє поєднувати зусилля для створення інновацій, інвестування, пошуку співробітників, партнерів, ресурсів та ринків збуту. Цифрові технології можуть відігравати ключову роль у навчанні співробітників, обмін знаннями, реалізації інноваційних ідей, у тому числі й у соціальній сфері.

Національна економічна стратегія на період до 2030 року у напрямі 2 Стратегічний курс міжнародної економічної політики та торгівлі за стратегічною ціллю передбачає підвищення інформаційної безпеки (пункт 6) [107]

Процеси широкого проникнення цифрових технологій у всі сфери життя і викликані соціальні зміни зумовлюють необхідність реформування системи інформаційного права та інформаційної безпеки. Науково обґрунтована система

інформаційного права тим важливіша з погляду громадських інтересів, чим точніше відображає об'єктивні закономірності розвитку суспільства.

Система інформаційного права має досягти такої максимальної відповідності в процесах цифровізації та розвитку інформаційного суспільства, що відбуваються сьогодні. Зазначене об'єктивно впливає на посилення процесу інституціоналізації у зв'язку з розвитком проривних, конвергентних інформаційних технологій, охоплюючи розвиток інститутів, що мають міждисциплінарний характер, у тому числі інституту інформаційної безпеки.

Процес інституціоналізації у праві тісно пов'язаний із загальними тенденціями розвитку правової системи країни. У проблематиці правової інституціоналізації переломлюються багато правових явищ і процесів – від правової політики та правового регулювання відносин до реалізації права та відновлення правопорядку.

Як зазначає Г. В. Мороз, в юридичній науці домінує розуміння інституціоналізації, виходячи з інституціональної теорії як процесу створення інститутів, а інститут права сприймається як система норм права, об'єднаних за ознакою однорідності предмета. Результатом інституціоналізації є виникнення відповідних інститутів (формальних і неформальних). Інститути визначають певний порядок у характері взаємодій між суспільством і людиною [108, с. 271].

У юридичному словнику інститути права визначено як упорядкована сукупність юридичних норм, що регулюють певний вид суспільних відносин, які належать до однієї галузі [109].

Для визначення інформаційної безпеки як інституту інформаційного права необхідно визначитися з поняттям правового інституту взагалі та інституту в інформаційному праві зокрема.

О. С. Адамова визначає правовий інститут як порівняно невелику, стійку групу правових норм, що регулюють певний різновид суспільних відносин [110, с. 258]. Вони виділяють серед різних видів інститутів права галузеві та міжгалузеві правові інститути, прості та комплексні.

Правові інститути поділяються за галузями права, наприклад: цивільні, адміністративні, кримінальні, фінансові та інші. Кожній галузі права притаманні свої правові інститути, які регулюють від одного до кількох правових питань. Якщо правовий інститут регулює одне правове питання та не містить інших, то він є простим інститутом. Якщо інститут охоплює дрібні самостійні утворення (субінститути), його можна вважати комплексним чи складним.

Автори навчального посібника «Теорія держави і права» визначають правовий інститут як елемент галузі права, що охоплює сукупність юридичних норм, що регулюють якісно однорідну групу суспільних відносин [111, с.140].

Інститут є структурним елементом галузі права, її складовою. Правовий інститут суттєво менший, ніж підгалузь права. Його завдання полягає в регламентуванні невеликих сторін суспільного життя.

Кожен інститут визначає окреме самостійне правове питання. Доцільно зазначити, що термін «правовий інститут» слід чітко відокремлювати від терміна «інститут». Інститут може бути соціальний, політичний, громадський. Правовий інститут – це конкретне нормативне встановлення закону.

І. В. Мироненко вважає, що правовий інститут – це група норм права, які регулюють близькі за своїм характером та змістом суспільні відносини, що відрізняються суттєвими особливостями [112, с. 29].

О. О. Лавриненко під правовим інститутом розуміє в порівнянні з галуззю і підгалуззю вужчу (хоча досить велику) сукупність норм, пов’язаних і взаємно обумовлених спільністю предмета регулювання [113].

Автори Великої української юридичної енциклопедії визначають інститут права як відокремлений комплекс норм права, що регулюють вид однорідних суспільних відносин за допомогою специфічного методу правового регулювання [114, с. 185].

На нашу думку, правовий інститут – це система взаємопов’язаних норм, що регулюють самостійну сукупність у суспільних відносинах або якісь їх компоненти, властивості. Правовий інститут характеризується наявністю

загальних положень, специфічних юридичних понять та принципів, які спільно визначають особливий режим правового регулювання будь-яких об'єктів. Кожен правовий інститут призначений для виконання специфічних функцій та відрізняється від інших компонентів правової системи.

У різних галузях права правовий інститут описує один вид суспільних відносин, які відрізняються від інших певними особливостями. Підтвердженням є приклади правових інститутів, що перебувають у різних галузях права. Наприклад, у конституційному праві – це інститути правового статусу особи, свободи совісті та віросповідання, громадянства.

У цивільному праві – це інститути власності, поруки, позовної давності, зобов'язань, дарування, угоди, купівлі-продажу, заповіту, нотаріату, відшкодування збитків, примирення сторін, приватизації. У господарському праві – це інститути акціонерних угод, довірчого управління, неспроможності, банкрутства, ліквідації юридичних осіб.

В адміністративному праві – це інститути адміністративного правопорушення, адміністративної відповідальності, адміністративного нагляду, державної служби, посадової особи, ліцензування, адміністративної юрисдикції.

У кримінальному праві – це інститути необхідної оборони, неосудності тощо. У кримінальному процесі – це інститути судимості, присяжних засідателів, правового статусу потерпілого, підозрюваного, умовно-дострокового звільнення, реабілітації.

У сімейному праві – це інститут шлюбу, прав і обов'язків подружжя, прав і обов'язків батьків та дітей, опіки та піклування, аліментні зобов'язання.

У трудовому праві – це інститути трудового договору, робочого часу та часу відпочинку, заробітної плати, порядок вирішення трудових спорів.

В інформаційному праві – це інститут права на інформацію, державної таємниці, конфіденційної інформації, інформаційних ресурсів, правового регулювання Інтернету, інформаційної безпеки.

У правовий інститут входить відокремлена група норм, що регулюють

однорідні відносини та відрізняються якісною єдністю.

Можна зазначити, що правові інститути поділяються за галузями права, а також на матеріальні та процесуальні, на прості та складні, на регулятивні, охоронні та установчі, на галузеві та міжгалузеві.

Наприклад, складний правовий інститут бюджетного права у фінансовому праві (або підгалузь) поділяється на інші правові інститути: бюджетного устрою, бюджетних повноважень, бюджетного контролю, відповідальності за порушення бюджетного законодавства тощо. Правовий інститут бюджетного процесу належить до процесуальних інститутів, інші до – матеріальних інститутів.

Галузеві інститути складаються з норм однієї галузі права. У разі, якщо правові норми, що входять до інституту, належать до кількох галузей права, такий інститут вважається міжгалузевим правовим інститутом.

М. М. Драгомерецький зазначає, що міжгалузевий інститут права є відокремленим комплексом правових норм різної галузевої належності, що регулюють певний вид взаємопов'язаних, близьких за змістом суспільних відносин у межах специфічного правового режиму. Наведена характеристика міжгалузевого інституту права не вичерпує усього змісту досліджуваного поняття, тому подальшого вивчення потребує питання про правовий режим цього інституту [115, с. 24].

Міжгалузевий правовий інститут доцільно визначити, як групу норм, що належать до кількох різних галузей права, які регулюють суспільні відносини, що мають деякі загальні ознаки. Як приклад можна навести інститут виборчого права, що охоплює норми конституційного, адміністративного та кримінального права. Аналогічно, інститут права власності охоплює правові норми конституційного, цивільного, сімейного, адміністративного та інших галузей права.

Іншим прикладом може бути інститут зовнішньоекономічного права, який охоплює норми цивільного, конституційного, адміністративного, фінансового, митного та валютного права. Аналогічно, морське право є

комплексним правовим інститутом, який охоплює норми цивільного, адміністративного, фінансового та інших галузей права.

Окремо слід згадати міжгалузевий інститут малого та середнього підприємництва, який регулюється не лише фінансовим та податковим правом, а й цивільним та трудовим правом. Безпосередньо стосується податкового права комплексний міжгалузевий правовий інститут природоресурсних платежів, який охоплює, крім норм податкового права, правові норми адміністративного, земельного, екологічного, природно-ресурсного та інших видів законодавства.

Н. О. Левицька зазначає, що міжгалузеві інститути проявляються у сфері дії родинних галузей права, причому ці інститути є не механічна сукупність, а гармонійне об'єднання різногалузевих правових норм, що регулюють однорідні відносини. Такі інститути формуються на принципі несуперечності, внутрішньої узгодженості нормативно-правовим приписам, відповідності загальним внутрішнім закономірностям [116, с. 24].

Слід зазначити, що міжгалузеві правові інститути у розвитку перетворюються на окремі підгалузі чи галузі права. Цим шляхом свого часу пройшло податкове право, яке спочатку було частиною фінансово-правового інституту державних доходів. Згодом податкове право стало самостійним комплексним інститутом у складі фінансового права.

Можна навести приклад інформаційного права, яке сформувалося з правових інститутів, мають адміністративно-правовий, цивільно-правовий та кримінально-правовий характер, характеризують загальні системні ознаки функціональності та субстанційності в поєднанні. Базовими ознаками інституту права є предмет та метод правового регулювання. Предмет характеризує те, що регулює право, а спосіб – певні прийоми, методи, засоби впливу права на суспільні відносини. Інститут у правовому аспекті уособлює інтегровану форму існування норм права.

Автори розділу 5 «Доктринальні проблеми розвитку інформаційного права» Правової доктрини України визначають інститути інформаційного права

як такі блоки правових актів та норм, які, будучи згруповані за єдиною метою, забезпечують регулювання відносин у сфері використання інформаційно-комунікаційних технологій [117, с. 758].

О. А. Баранов трактує інститут інформаційного права як відносно стійку та визнану групу інформаційно-правових норм, що регулює певні види інформаційних правовідносин [118, с. 39-45].

У науці інформаційного права сталим є уявлення про розгляд правового регулювання забезпечення інформаційної безпеки як інституту інформаційного права, хоча низка дослідників ідентифікують як підгалузь інформаційного права.

На думку С. С. Єсімова та О. Г. Яреми, підгалузь правового забезпечення інформаційної безпеки регулює суспільні відносини, використовуючи норми різних галузей права (водночас єдність і цілісність цих галузей не порушуються), комплексно використовуючи різні галузеві методи правового регулювання. Крім того, природа інформації як об'єкта різних суспільних відносин, врегульованих нормами різних галузей права, також має комплексний характер [119, с. 248]. Прийняття Закону України «Про інформаційну безпеку» створить структурну стійкість усієї системи нормативних правових актів, що діють у вказаній сфері [119, с. 251].

З огляду на сучасний стан правового забезпечення інформаційної безпеки, О. Д. Довгань та Т. Ю. Ткачук розглядають її як підгалузі інформаційного права, що має міжгалузевий характер [10].

Автори Енциклопедії соціогуманітарної інформології зазначають, що аналіз різних підходів до визначення категорії інформаційної безпеки дозволяє зробити висновок про недоцільність суворого дотримання однієї позиції. Потрібен комплексний підхід, згідно з яким інформаційна безпека визначається через істотні риси, найбільш важливі основні функції, беручи до уваги постійну динаміку інформаційних і соціальних систем. У різних сферах науково-практичних знань поняття інформаційної безпеки має свої особливості формулювання та розуміння.

У контексті державної політики, зокрема національної безпеки, інформаційна безпека визначається як захищеність (стан захищеності) основних інтересів особи, суспільства, держави у сфері інформації, охоплюючи інформаційні й комунікаційну інфраструктуру і власне інформацію та її параметри, такі, як: повнота, об'єктивність, доступність і конфіденційність.

Інформаційна безпека в юридичному полі визначається як стан правових норм і відповідних їм інститутів безпеки, які гарантують постійну наявність даних для ухвалення стратегічних рішень і захист інформаційного простору країн [120, с. 55].

Таким чином, пропонуємо розглядати сукупність правових норм, що регулюють суспільні відносини у сфері інформаційної безпеки, як комплексно-правовий інститут – правове забезпечення інформаційної безпеки особи, суспільства і держави у складі названої підгалузі. Однак це твердження потребує доказів на основі викладених вище критеріїв.

У навчальній літературі виділено ряд ознак правового інституту інформаційної безпеки, охоплюючи наявність упорядкованої системи інформаційно-правових норм, їх цільову орієнтованість на забезпечення життєво важливих інтересів.

У виділеного інституту є свій самостійний предмет правового регулювання – комплекс суспільних відносин, пов'язаних із захистом особи, соціальних груп та суспільства від деструктивного інформаційного впливу. Ця сфера відносин має достатню чітку грань, яка відокремлює її від іншого великого блоку відносин у рамках інформаційної безпеки – захисту інформації.

Названий предмет правового регулювання має достатню однорідність, оскільки в його основі лежить загальний механізм наведення деструктивного інформаційного впливу на індивідуальну психіку та суспільну свідомість, а також захисту від нього.

У сфері забезпечення інформаційної безпеки домінує імперативний метод правового регулювання, активно застосовуються правові засоби заборон та зобов'язань. Наприклад, законодавством встановлено правові заборони на

поширення певної негативної інформації, що доповнюються запровадженням юридичної відповідальності за порушення та наділення державних органів та інформаційних посередників обов'язками щодо обмеження поширення такого контенту у певних інформаційних середовищах.

Критерії єдності правових норм, нормативної відокремленості та повноти регульованих відносин виконуються лише частково, що свідчить про те, що інститут правого забезпечення інформаційної безпеки (інститут інформаційної безпеки особи, суспільства і держави, інститут захисту від інформаційного деструктивного впливу) перебуває у стадії формування. Водночас проглядається міжгалузева природа цього правового інституту, властива підгалузі.

Інститут права як системне правове утворення відрізняється високим рівнем інтеграції, що виходить за межі окремих галузей права, набуваючи міжгалузевого або загальноправового статусу.

Ця теза справедлива щодо досліджуваного інституту правового забезпечення інформаційної безпеки. Норми інформаційного права відіграють ключову роль у правовому регулюванні цілей, завдань, принципів та напрямів забезпечення інформаційної безпеки.

Прерогативою інформаційного права є регламентація питань протидії поширенню негативної інформації у засобах масової інформації та мережі Інтернет. Водночас інформаційно-правове регулювання не вичерпує всієї предметної галузі забезпечення інформаційної безпеки. Тому правову основу інформаційної безпеки становлять норми інших галузей права, охоплюючи конституційне, адміністративне, кримінальне, цивільне.

Конституційне право встановлює базові засади державного та громадського устрою, правового статусу особи, систему органів публічної влади в Україні, які мають відправне значення для всіх сфер безпеки. Норми конституційного законодавства в окремих галузях стосуються питань протидії деструктивному інформаційному впливу (наприклад, маніпуляції суспільною свідомістю у ході передвиборної агітації).

Роль адміністративного права проявляється в регламентації правового статусу органів публічної влади, що є основними суб'єктами забезпечення інформаційної безпеки. Адміністративне право, як і кримінальне право, встановлює юридичну відповідальність за правопорушення, пов'язані з наданням деструктивного інформаційного впливу на особистість та соціальні групи.

Правовий інститут забезпечення інформаційної безпеки має міжгалузевий характер.

У сфері інформаційної безпеки існує один спеціалізований закон, який опосередковано присвячений правовому регулюванню цієї правової категорії. Йдеться про Закон України «Про захист суспільної моралі» [50]. Відповідно до ст. 1 цього Закону, суспільна мораль – система етичних норм, правил поведінки, що склалися у суспільстві на основі традиційних духовних і культурних цінностей, уявлень про добро, честь, гідність, громадський обов'язок, совість, справедливість. Предмет регулювання становлять відносини, пов'язані із захистом суспільства від інформації, визначеної у ст. 2 Закону.

Ухвалення Закону України «Про захист суспільної моралі» у 2003 році було подією для розвитку системи правового забезпечення в країні. Закон встановив важливі правові механізми забезпечення інформаційної безпеки щодо деструктивного інформаційного впливу. Хоча норми закону регламентують більшість значущих форм поширення інформації (видовищні заходи, друковані видання, продукцію засобів масової інформації), вони практично не поширюють дію на інтернет-ресурси. Проте мережа Інтернет є головним джерелом загроз для інформаційної безпеки.

Для закриття важливої галузі прояву загроз інформаційній безпеці було внесено численні поправки до Закону України «Про захист інформації в інформаційно-комунікаційних системах» – базового джерела інформаційного права України. Саме його законодавець розглядає як основне правове джерело протидії інтернет-загрозам різного роду,охоплюючи загрози психологічного характеру.

Закони України «Про захист суспільної моралі» та «Про захист інформації в інформаційно-комунікаційних системах» регламентує такі основні аспекти забезпечення інформаційної безпеки: закріплення загальної правової заборони поширення протиправної інформації; встановлення обов'язків окремих суб'єктів щодо забезпечення інформаційної безпеки; регламентація порядку обмеження доступу до певних видів негативної інформації та інформаційних ресурсів [38; 50].

Закон України «Про захист інформації в інформаційно-комунікаційних системах» вперше закріпив правовий механізм обмеження доступу до шкідливої інформації в мережі Інтернет. Блок правових норм, спрямований на закріплення різних правових засобів та механізмів забезпечення інформаційної безпеки, суттєво зріс та продовжує постійно розширюватися.

Цілком обґрунтованов науковій літературі вказувалося на неадекватність назви закону у сфері регулювання та пропонувалося доповнити словами «та забезпечення інформаційної безпеки» – «Про захист інформації в інформаційно-комунікаційних системах та забезпечення інформаційної безпеки». Реалізація зазначеної ініціативи спричинить необхідність закріплення базового понятійного апарату в галузі інформаційної безпеки, охоплюючи інформаційну безпеку.

Доцільно доповнити статтю 28 «Неприпустимість зловживання правом на інформацію» Закону України «Про інформацію» положеннями, присвяченими організаційно-правовим засадам забезпечення інформаційної безпеки [37].

Визнаючи ключову роль Закону України «Про захист інформації в інформаційно-комунікаційних системах» у протидії інтернет-загрозам інформаційної безпеки, слід визнати, що Закон переважно передбачає правові механізми боротьби з протиправним контентом. Тоді як комунікаційних загроз у мережі Інтернет норми закону практично не торкаються.

Сфера засобів масової інформації через особливу значущість є предметом регулювання окремого законодавчого акту – Закону України «Про друковані засоби масової інформації (пресу) в Україні», одного з найстаріших джерел

інформаційного права України, Законів України «Про телебачення і радіомовлення», «Про інформаційні агентства», «Про суспільне телебачення і радіомовлення» та інших [121-124].

До засобів масової інформації з 2004 року з початку функціонування Національного електронного реєстру інформаційних ресурсів належать мережеві видання – значна частина інтернет-ресурсів [125].

Важливе значення для забезпечення інформаційної безпеки у діяльності засобів масової інформації має положення ст. 3 Закону України «Про друковані засоби масової інформації (пресу) в Україні», що регламентує неприпустимість зловживання свободою масової інформації. Під цим поняттям ховається велика кількість різних форм поширення протиправного контенту та інших суспільно небезпечних дій у сфері масової інформації.

Правову заборону на зловживання свободою масової інформації у Законі України «Про друковані засоби масової інформації (пресу) в Україні» підкріплено статтями Кодексу України про адміністративні правопорушення та Кримінального кодексу України, які встановлюють відповідальність за порушення.

Інформаційне законодавство містить комплекс правових норм, що регламентують питання забезпечення інформаційної безпеки в засобах масової інформації та мережі Інтернет – двох ключових джерел інформаційної безпеки.

Наскрізний характер має такий вид інформації, як реклама, оскільки охоплює традиційні та нові медіа, та офлайн-формати (зовнішня, друкована, сувенірна реклама). У зв’язку з повсюдною присутністю реклами та широким застосуванням методів інформаційного впливу вона потребує уваги в контексті забезпечення інформаційної безпеки.

Відносини у сфері реклами є предметом регулювання Закону України «Про рекламу» [126]. Під рекламою розуміється інформація про особу чи товар, розповсюджена в будь-якій формі та в будь-який спосіб і призначена сформувати або підтримати обізнаність споживачів реклами та їх інтерес щодо таких особи чи товару.

Закон України «Про рекламу» регламентує правові аспекти забезпечення інформаційної безпеки: загальні вимоги до реклами, охоплюючи критерії недобросовісної та неправомірної порівняльної реклами; відповідальність за порушення законодавства про рекламу; обмеження окремих способів поширення реклами й окремих видів товарів.

Розглянуті законодавчі акти, що стосуються джерел інформаційного права, регламентують окремі аспекти забезпечення інформаційної безпеки в офлайн- та онлайн- інформаційних середовищах, як-от: засоби масової інформації, інформаційно-комунікаційні мережі, охоплюючи мережу Інтернет, видовищні заходи та інші офлайн-форми розповсюдження інформації.

Інституціоналізація інституту інформаційної безпеки – це зумовлені історичним розвитком стійкі типи та форми діяльності, відповідні структурні елементи із забезпечення безпеки особи, суспільства та держави, інтегровані в різні сфери життєдіяльності, різноманітні за проявами та динамічні з розвитку функцій. Ці форми та типи діяльності сформувалися під впливом об’єктивних і суб’єктивних факторів та умов.

Виділяють компоненти інституційного середовища інформаційної безпеки: нормативно-правовий; організаційний; самоорганізаційний; соціально-культурний; когнітивний.

Перший компонент – нормативно-правовий. Основу структури інституційного середовища інформаційної безпеки створюють законодавчі та нормативні акти, що регулюють усі види та типи відносин у цій сфері. Головна функція нормативно-правового компонента – це регулювання відносин і взаємодій у сфері інформаційної безпеки, визначення пріоритетів, цілей та напрямів, структурування інституційного простору сфери інформаційної безпеки. Нормативно-правовий компонент інституційного середовища інформаційної безпеки можна поділити на три рівні: міжнародно-правовий, національно-правовий та об’єктно-правовий.

Міжнародно-правовий рівень відображає ступінь та якість залучення національної системи інформаційної безпеки до світових процесів забезпечення

глобальної інформаційної безпеки людства.

Національно-правовий рівень інституціоналізації інформаційної безпеки визначає напрями та пріоритети інформаційної безпеки, її види, форми та типи відносин, порядок взаємодії суб'єктів, принципи та норми регулювання. Концептуальні питання забезпечення висвітлено в Конституції України, Стратегії інформаційної безпеки України, у яких простежується увага держави до гуманітарних проблем інформаційної безпеки [127]. В Україні діє Закон України «Про захист інформації в інформаційно-комунікаційних системах»[38].

В Україні затверджуються документи, у яких інформаційна безпека трактується у техніко-технологічному ключі. Наприклад, ДСТУ ISO / IEC17799: 2005 «Інформаційні технології: практичні правила в управлінні інформаційною безпекою» [128].

Об'єктно-правовий рівень інституціоналізації інформаційної безпеки конкретизує у вигляді спеціалізованих напрямів законодавства інституційно-правові норми щодо окремих видів інформаційної безпеки. Законотворчість у створенні об'єктно-правового рівня нормативно-правового компонента інституційного середовища інформаційної безпеки не можна визнати достатнім. Інтереси особистості, тобто гуманітарні інтереси, дотримуються не повною мірою. Не розроблено проєкт Закону України «Про інформаційно-психологічну безпеку».

Другий компонент інституціоналізації інформаційної безпеки – організаційний. Важливою складовою інституційного середовища інформаційної безпеки є організаційна структура. Склад і функціональні властивості визначаються нормативно-правовими вимогами забезпечення інформаційної безпеки та відображають реальний стан системи. Організаційний компонент представлений державними органами влади та управління, до функціональних завдань і компетенції входять питання інформаційної безпеки.

Функції організаційного компонента поділяються на законодавче регулювання відносин безпеки, управлінський вплив органів публічної влади та забезпечення правового порядку та виконання норм інформаційної безпеки

судовими інстанціями. Це створює основу процесів організації інституційної структури безпеки, формування необхідних елементів, зв'язків, принципів взаємодії. Можна виділити такі організаційні рівні: державний, регіональний та місцевий.

1. Державний рівень представлений такими організаційними елементами, як Комітет з питань гуманітарної та інформаційної політики Верховної Ради України, Рада національної безпеки і оборони України, до компетенції яких входять питання забезпечення інформаційної безпеки, Конституційний та Верховний суди України, Генеральна прокуратура, Міністерство культури та інформаційної політики України, Міністерство цифрової трансформації України та органи, які визначають політику держави у сфері інформаційної безпеки та виконують роль головних регуляторів відносин у сфері безпеки [127-134]. До цього рівня належать функції міністерств і відомств щодо забезпечення інформаційної безпеки, у тому числі Державна служба спеціального зв'язку та захисту інформації України [135].

2. Регіональний рівень має суттєві особливості, пов'язані з різними причинами політико-географічного, економічного, соціального, національно-історичного розвитку, факторами суб'єктивного характеру.

Регіональна структура елементів та зв'язків інституційного середовища інформаційної безпеки пов'язана не тільки із загальнодержавною необхідністю та неминучістю виконання загальних інституційних норм, що визначаються Конституцією та законодавством України, а й безпосередньою участю у формуванні сфери інформаційної безпеки.

3. Рівень місцевих утворень є первинною організаційною основою інституційного середовища інформаційної безпеки, оскільки питання інформаційної безпеки набувають безпосереднього характеру забезпечення першочергових потреб особи: в інформації, у захисті персональних даних, у захисті від негативних інформаційних впливів.

Третій компонент інституціоналізації інформаційної безпеки – самоорганізаційний. Набув розвитку в громадянському суспільстві, що активно

формується в Україні. У громадянському суспільстві особистість формує систему цінностей, що визначають вільне та безпечне існування, а потреба в захисті цих цінностей (матеріальних, духовних, моральних та ін.) призводить до формування певних інститутів, що визначають порядок соціальних відносин, способів соціальної самоорганізації, механізмів взаємодій з інститутами держави, механізмів захисту інтересів та реалізації потреб.

Між державними та громадськими організаціями у сфері інформаційної безпеки виникають інституційні взаємодії: перші виконують регулятивні функції у суспільстві, інші прагнуть реалізувати мету підвищення рівня інформаційної безпеки у вигляді впливу діяльності державної влади. Структури громадянського суспільства є у сфері інформаційної безпеки самоорганізаційним компонентом інституційного середовища сфери інформаційної безпеки, які мають власну багаторівневу та багатофункціональну структуру та мету саморозвитку.

Інституційні зміни всередині громадянського суспільства у вигляді інституційних взаємодій призводять до інституційних змін у межах всієї соціальної системи, змінюючи ціннісні системи, мету, орієнтації, механізми реалізації та управління. У сфері інформаційної безпеки це виражається найбільшою мірою, тому що з трьох основних об’єктів два мають безпосереднє відношення до громадянського суспільства: особа як соціально-суб’єктна основа і суспільство, яке поступово трансформується у громадянський стан і основними цілями якого стає інформаційна безпека. Зазначене знайшло відображення в Національній стратегії сприяння розвитку громадянського суспільства в Україні на 2021-2026 роки [136].

Важливим інституційним аспектом інформаційної безпеки є створення в організаціях різних форм власності та галузевої приналежності спеціалізованих структурних підрозділів інформаційної безпеки.

Четвертий компонент інституціоналізації інформаційної безпеки – соціально-культурний. Важливою складовою є становлення культури інформаційної безпеки суспільства. Органічною частиною цієї культури є

культура інформаційної безпеки особи. Це неодмінна умова формування адекватного реаліям інституційного середовища сфери інформаційної безпеки.

Функціональне призначення культури інформаційної безпеки – створення та розвиток базових для розуміння цілей та цінностей щодо інформаційної безпеки простору існування (у соціально-філософському сенсі) та життєдіяльності (у соціологічній інтерпретації цього поняття) людини, що реалізує себе як особу, яка має власну систему ціннісних орієнтацій, ідеалів, соціальних установок, поведінкових стандартів тощо.

На думку Ю. Є. Муравської, культура інформаційної безпеки – це спосіб організації та розвитку людської життєдіяльності в інформаційному просторі, що забезпечує якісне інформаційне середовище (якість споживаної інформації, захищеність суб'єктів від негативних інформаційних впливів) та захищеність їх інформації, а тому створює можливість повністю задовольнити потреби суб'єктів [137]. При такому способі організації та розвитку життєдіяльності суб'єкт усвідомлює себе суб'єктом інформаційної безпеки, здатний виявити загрози, володіє технологіями захисту, дотримується норм інформаційної етики в процесі перетворення інформаційного середовища.

Культура інформаційної безпеки не просто робить специфічний вплив на інституційне середовище інформаційної безпеки, а є активатором, основою системи цілепокладання та ціннісної мотивації, вона впливає на інші компоненти інституційного середовища, що служить каталізатором процесів їх взаємної інтеграції в єдиному просторі сфери інформаційної безпеки.

Культура інформаційної безпеки – це інформаційно-культурний регулятор суспільства як інтегральної інформаційно-комунікаційної системи, здатної до саморозвитку, визначальною властивістю якої є можливість накопичення та передачі знань, які формують соціальну пам'ять [138, с. 95].

Слід констатувати, що, незважаючи на інтерес до культурологічних проблем інформаційної безпеки світової спільноти, проблема культури інформаційної безпеки вивчена в Україні мало і потребує наукових досліджень.

П'ятий компонент інституціоналізації інформаційної безпеки –

когнітивний. Гуманітарно-інституційні процеси у сфері інформаційної безпеки, вироблення гуманітарних критеріїв інформаційної безпеки, визначення цілей та пріоритетів є сферою наукового пошуку.

Зміст поняття інформаційна безпека передбачає та певною мірою визначає охоплення трьох складових, дві з яких мають гуманітарну природу: задоволення інформаційних потреб суб'єктів, включених до інформаційного середовища, забезпечення безпеки інформації та забезпечення захисту суб'єктів інформаційних відносин від негативного інформаційного впливу.

Дослідження гуманітарних закономірностей забезпечення інформаційної безпеки повинно охопити: розробку та вдосконалення загальної теорії та методології інформаційної безпеки, особливо теорії та методології гуманітарного характеру; розвиток спеціальних наукових теорій у предметному полі інформаційної безпеки, як-от: філософія інформаційної безпеки, соціологія інформаційної безпеки, політологія інформаційної безпеки (які є основою гуманітарних знань у галузі інформаційної безпеки), об'єктно-орієнтованих спеціальних теорій, до яких можна віднести, наприклад, освітню безпеку, соціологію інформаційно-психологічної безпеки особи тощо; формування наукових підрозділів у структурі Національної академії правових наук України та шкіл, що розробляють проблематику інформаційної безпеки в різних теоретичних та прикладних аспектах; організація наукових дискусій, публікацій з проблем інформаційної безпеки в традиційних гуманітарних періодичних і в спеціалізованих журналах, підготовка та випуск монографій, підручників, розробка навчальних програм та курсів тощо.

Процес інституціоналізації інформаційної безпеки завжди супроводжувався та підкріплювався професіоналізацією.

Розглядаючи інституціоналізацію інформаційної безпеки, доцільно відзначити, що за наявності досить різноманітних правових методів та засобів протидії загрозам інформаційної безпеки інформаційне законодавство не містить норм, що характеризують базові аспекти забезпечення інформаційної безпеки, охоплюючи понятійний апарат, загрози інформаційній безпеці, правові

принципи та напрями її забезпечення.

Наслідком цього є відсутність системності в правовому регулюванні забезпечення інформаційної безпеки. Інформаційно-правове регулювання посідає ключове місце в системі правового забезпечення інформаційної безпеки, проте не вичерпує його змісту.

Конституційне законодавство, крім основних норм Основного закону, що мають фундаментальну значущість для всієї національної правової системи України, охоплює законодавство, що регламентує окремі питання забезпечення інформаційної безпеки, зокрема у сфері виборчого процесу. До стадій виборчого процесу входить інформаційне забезпечення виборів та референдумів, що охоплює інформування виборців та учасників референдуму, передвиборну агітацію та агітацію з питань референдуму. У рамках цієї стадії застосовуються технології маніпуляції свідомістю електорату із боку кандидатів, виборчих об’єднань, інших зацікавлених сторін [139; 140].

Виборчий кодекс України та Закон України «Про всеукраїнський референдум» містять комплекс правових заходів, спрямованих на блокування методів деструктивного інформаційного впливу щодо виборців та гарантування принципу вільного волевиявлення.

Адміністративне законодавство регулює низку аспектів забезпечення інформаційної безпеки: правовий статус суб’єктів забезпечення інформаційної безпеки; правові механізми протидії проявам тероризму в інформаційному середовищі, насамперед протидії російській ідеології; правові заходи, спрямовані на протидію надання деструктивного інформаційного впливу державних органів і спеціальних служб іноземних держав, іноземних організацій; правові заходи, спрямовані на протидію деструктивним релігійним організаціям; правові механізми протидії правопорушенням, пов’язаним із наданням деструктивного інформаційного впливу; адміністративна відповідальність за правопорушення у сфері інформаційної безпеки.

Кримінальне законодавство України закріплює склади злочинів, пов’язаних із наданням деструктивного інформаційного впливу, та передбачає

кримінальні покарання. Діяльність з виявлення, розкриття, розслідування таких злочинів та розгляду кримінальних справ у судах регламентується Законом України «Про оперативно-розшукову діяльність» та Кримінальним процесуальним кодексом України [141; 142].

Цивільне право гарантує захист нематеріальних благ, охоплюючи гідність особи, честь та добре ім'я, ділову репутацію (ст. 297, 299 Цивільного кодексу України). Там поширюються основні засоби захисту цивільних прав. Цивільний кодекс України регламентує механізми компенсації моральної шкоди та захисту честі, гідності та ділової репутації [143]. Серед правових засобів захисту останніх нормами Цивільного кодексу України передбачені спростування інформації, що зневажають честь, гідність або ділову репутацію, видалення відповідної інформації, припинення або заборона подальшого поширення, відшкодування збитків, компенсація моральної шкоди.

Проведений аналіз законодавства довів тезу про міжгалузевий характер правового інституту забезпечення інформаційної безпеки та продемонстрував наявність досить розвиненого механізму правового регулювання в цій сфері.

Домінантну роль у структурі відіграють норми інформаційного права, проте значення в правовому регулюванні забезпечення інформаційної безпеки мають норми конституційного, адміністративного, кримінального та цивільного права. Водночас чинний механізм правового регулювання забезпечення інформаційної безпеки має низку недоліків. Важливим є відсутність правового закріплення відправних засад та принципів забезпечення інформаційної безпеки, що не дозволяють набути механізму повноцінної системності правового регулювання.

Є прогалини у правовій регламентації низки напрямів забезпечення інформаційної безпеки, охоплюючи: захист державних і місцевих органів, посадових осіб від деструктивного інформаційного впливу; протидію фальсифікації національної та світової історії на шкоду інтересам України; протидію поширенню деструктивних субкультур та інших форм негативного інформаційного впливу у духовній сфері; інформаційне забезпечення діяльності

Збройних сил, правоохоронних та інших державних органів; інформування української та зарубіжної громадськості про внутрішню та зовнішню політику України, офіційну позицію щодо соціально значущих подій життя.

У зв'язку з цим інститут правового забезпечення інформаційної безпеки потребує подальшого системного розвитку з метою реалізації положень Стратегії інформаційної безпеки України.

Інституціоналізація інформаційної безпеки – це логічний взаємопов'язаний науково обґрунтований процес, системна діяльність уповноважених осіб та носіїв суб'єктивних прав, сукупність інституційних засобів (прийомів та елементів), легальне врегулювання, упорядкування суспільних відносин, пов'язаних із виявленням, закріпленням (легітимацією), реалізацією суспільних відносин в інформаційному просторі.

Інституціоналізація інформаційної безпеки формулюється на основі положень інформаційного права та теорії інституцноналізму про правові інститути як важливі для суспільства сфери діяльності, регулювання яких забезпечується ієрархічною системою правових норм. Інституціоналізація інформаційної безпеки орієнтує правове регулювання, системоутворюючі зв'язки правових інститутів на забезпечення регулювання нормативної, організаційної, функціональної структури правовими нормами різних ієрархічних рівнів. Беручи до уваги трьохрівневий характер забезпечення інформаційної безпеки, забезпечення відбувається на державному, регіональному та місцевому рівнях.

Правова інституціоналізація інформаційної безпеки в інформаційному праві охоплює виявлення, упорядкування, приведення в системний порядок найбільш суттєвих, соціально значущих актуальних інформаційних прав особи, законних інтересів суспільства і держави в інформаційній сфері, їх легальне закріплення у принципах, положеннях і нормах права, захист порушених суб'єктивних прав та законних інтересів.

Висновки до розділу 1

Методологічні основи дослідження інформаційної безпеки в інформаційному праві базуються на міждисциплінарному підході до дослідження правових явищ. Міждисциплінарні дослідження в інформаційному праві необхідні та важливі, оскільки допомагають виявити загальні закономірності становлення, розвитку та функціонування таких явищ, як інформаційна безпека, вивчити закономірності, які притаманні всім напрямам інформаційної безпеки, незалежно від відмінностей. У цьому полягає цінність міждисциплінарних досліджень.

Багатоаспектність інформаційної безпеки як об'єкта дослідження передбачає вивчення положень з різних галузей знань: філософських, історичних, політичних, юридичних та інших наук. Адже кожна наука здатна зробити свій внесок у розвиток забезпечення інформаційної безпеки. Міждисциплінарний підхід дає низку переваг при дослідженні комплексних об'єктів, яким є інформаційна безпека, надає можливість вийти на новий рівень теоретико-методологічного бачення та розуміння об'єкта дослідження, глибоко та багатовимірно його вивчити.

Беручи до уваги взаємопов'язаність та взаємозалежність прав людини та забезпечення інформаційної безпеки, а також те, що вони реалізуються в різних сферах людської діяльності – соціальної, економічної, політичної та інших, розробка міждисциплінарних методологічних підходів має значення при створенні адекватних моделей забезпечення інформаційної безпеки, де необхідно охопити всю сукупність факторів, що впливають на інформаційний простір.

Правові дослідження в цій галузі ускладнює той факт, що стандарти інформаційної безпеки містяться не тільки в юридично обов'язкових документах, а й в актах, які, з формальної точки зору, не мають юридичної сили: резолюції міжнародних організацій, зауваження загального порядку та

рішення конвенційних органів тощо.

Під час дослідження специфічних закономірностей становлення, розвитку та функціонування інформаційної безпеки потрібен дисциплінарний підхід, орієнтований на з'ясування специфічних властивостей, які притаманні окремим соціальним явищам – інформаційній безпеці особи, суспільства та держави.

Під час дослідження інформаційної безпеки важливо встановити, як проявляється правове явище при регулюванні суспільних відносин, які суттєві ознаки цього явища. Це дозволяє сформулювати групи понять, що відображають правові явища, виявляють властивості, які будуть суттєвими ознаками інформаційної безпеки, формуючи систему правового забезпечення.

Характеристика системи правового забезпечення інформаційної безпеки представлена у контексті сукупності наукових знань, що становлять зміст теорії системи права та теорії інформаційного права. Сучасні тенденції особистісно орієнтованого підходу в галузі правового забезпечення інформаційної безпеки знаходять відображення у чинній Стратегії інформаційної безпеки України. У Стратегії інформаційної безпеки особа, її потреби та інтереси виділені як пріоритетні у дефініції «національні інтереси України в інформаційній сфері».

Системний аналіз законодавства показав, що правові норми, спрямовані на забезпечення інформаційної безпеки особи, містяться в різних галузях законодавства в інформаційному, а також конституційному, цивільному, трудовому, кримінальному, екологічному, виборчому, фінансовому, податковому, банківському, цивільному, господарському, кримінальному, адміністративному судочинстві тощо.

Це дозволило зробити висновок про міжгалузевий комплексний характер інституту правового забезпечення інформаційної безпеки особи, який є сукупністю юридичних норм, що регулюють однорідну групу суспільних відносин, що складаються з приводу забезпечення безпеки особи в інформаційній сфері в процесі реалізації різноманітних інтересів (матеріальних, духовних, майнових, пізнавальних, соціальних, політичних, екологічних та інших). Водночас ключове значення для правового забезпечення інформаційної

безпеки особи в умовах інформаційного суспільства мають норми інформаційного права, що є одним із критеріїв її галузевого відокремлення. Інформаційна безпека особи становить основу інформаційної безпеки суспільства і держави, хоча кожний з напрямів інформаційної безпеки має особливості та комплекс нормативного забезпечення.

Водночас загальнотеоретичні аспекти характерні для забезпечення усіх напрямів. Забезпечення інформаційної безпеки можливе шляхом застосування системного підходу, що бере до уваги всю різноманітність інформаційних відносин за участю особи, суспільства і держави, яка не нехтує зокрема, психологічним аспектом деструктивного інформаційного впливу. Інформаційна безпека повинна розглядатися під гуманітарним кутом зору, що є складовою гуманітарної безпеки, важливою складовою інформаційної культури та процесу формування духовності та національної самосвідомості.

Інституціоналізація інформаційної безпеки в системі інформаційного права заснована на нормативному підході до праворозуміння у сфері правотворчості та правозастосування. Інтегративне розуміння юридичного інституту забезпечення інформаційної безпеки зумовлене появою в законодавстві нових масивів правових норм і потребою систематизації з допомогою підвищення ступеня взаємодії та розвитком наукових поглядів на соціально-регулятивному значенні інформаційної безпеки.

До ознак юридичного інституту інформаційної безпеки як спільності правових норм належать: однорідний; системний характер; юридичну єдність; нормативну відособленість; цілісність; універсальність; специфіка змісту; наявність основного критерію відокремлення; наявність зовнішньої форми вираження.

В інформаційному суспільстві такий підхід необхідний для вдосконалення системи інформаційного законодавства та розвитку міжгалузевого інституту правового забезпечення інформаційної безпеки особи, суспільства і держави в правовій науці.

Юридичний інститут інформаційної безпеки визначено як специфічний

комплекс правових норм, принципів та конструкцій, що утворюють певну систему, відокремлений єдністю правовідносин (різновидом суспільних відносин) та режимом (предметом, методом та принципами) правового регулювання. Сучасний інституціональний підхід, що позначився в юридичній науці, свідчить про універсальний характер правової категорії цього інституту, розкриває потенціал як інструмент вираження нормативного змісту позитивних правових норм у регульованих громадських відносинах. Інституційна підсистема забезпечення інформаційної безпеки охоплює сукупність органів публічної влади, інститутів громадянського суспільства та інших недержавних суб'єктів, що беруть участь у забезпеченні інформаційної безпеки.

Ключову роль у системі забезпечення інформаційної безпеки відіграють профільні органи публічної влади. Найбільш важливі завдання щодо забезпечення інформаційно-психологічної безпеки виконують Міністерство культури та інформаційної політики України, які здійснюють регуляторні та контрольно-наглядові функції у галузі засобів масової інформації та масових комунікацій.

Крім органів публічної влади, важливі завдання у сфері забезпечення інформаційної безпеки вирішують інститути громадянського суспільства та інші структури, що входять до недержавної підсистеми забезпечення безпеки. До них належать засоби масової інформації, адміністратори та автори інтернет-ресурсів, блогери, інтернет-посередники, виробники засобів забезпечення інформаційної безпеки, неприбуткові організації, заклади освіти та науково-дослідні установи.

Основним вектором удосконалення інституційної системи забезпечення інформаційної безпеки є зміцнення потенціалу чинних державних структур, активне залучення можливостей громадянського суспільства.

РОЗДІЛ 2
ПРАВОВОЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВІЗАЦІЇ ІНФОРМАЦІЙНОГО ПРОСТОРУ

2.1. Адміністративно-правові засоби та механізми забезпечення інформаційної безпеки в умовах цифровізації

Правове регулювання використання інформаційно-комунікаційних технологій і систем створення та використання інформаційної інфраструктури в Україні безпосередньо пов’язане з правовим забезпечення інформаційної безпеки та кібербезпеки всіх учасників таких відносин [144]. Цифровізація інформаційної сфери безпосередньо пов’язана із зусиллями та ресурсами, що виділяються органами публічного сектору для виконання нормативних документів у момент впровадження та з часом. Критичну роль відіграє переплетення макро- та мікроінституціональних і технічних умов. Правова та інституційна основа цифровізації інформаційної сфери – це основа, у якій можуть відбуватися зміни, що насамперед торкаються інформаційної безпеки.

Використання інформаційної інфраструктури з метою забезпечення інформаційної безпеки створює суспільні відносини, регулювання яких має здійснюватися правовими нормами, а розробка, прийняття, застосування та виконання обов’язкових вимог до інформаційних технологій у контексті забезпечення інформаційної безпеки має здійснюватися нормами технічного регулювання [145].

Активне використання в суспільних відносинах технологій великих даних (англ. BigData), промислового Інтернету породжує необхідність визначення критеріїв і правових засад використовуваних інформаційних технологій та інформаційної інфраструктури; забезпечення інформаційної безпеки щодо інформації, яка збирається та обробляється цими технологіями, у тому числі персональних даних, відомостей, що становлять комерційну таємницю, інших

видів інформації обмеженого доступу, що розміщуються в інформаційній інфраструктурі.

Використання інформаційних технологій у контексті цифрової трансформації потребує зміни підходу до правового регулювання інформаційної безпеки, запровадження інститутів «цифрового права»; формування єдиних стандартів життєвого циклу інформаційних технологій. Предметом ІТ-права є відносини у цифровому середовищі (відносини з приводу створення, зберігання, передачі та захисту інформації в електронному вигляді) [146, с. 174].

Як зазначає Ж.О. Павленко, нова цифрова реальність висуває нові вимоги до правової науки та юридичної практики, що стосуються в тому числі розробки ефективних інструментів і моделей правового регулювання різних сфер суспільного життя. У сучасних умовах право стає не тільки інструментом, який забезпечує цифровізацію економіки, управління та інших сегментів соціального буття, але й об'єктом впливу цифровізації. Із розвитком цифрових технологій загострюється протиріччя між потребою в якісних, із точки зору форми та змісту, нормативно-правових актах, а також здатністю її задовольнити в короткі терміни. Завданням держави є забезпечення сприятливих умов, що сприяють цифровізації, та створення можливостей для реалізації [147, с. 74].

Дослідження механізму правового забезпечення інформаційної безпеки в умовах цифровізації передбачає вивчення правового інструментарію, використовуваного інформаційним та іншими галузями права щодо захисту особи та суспільства від деструктивного інформаційного впливу.

Сьогодні, зазначає О. В. Соскін, спостерігається перехід до комплексних методів у провідних країнах світу, основною метою яких є огляд можливостей цифрової трансформації державного управління і перспектив розвитку інформаційно-комунікаційної інфраструктури на технологічному підґрунті цифрових технологій. Інформаційно-комунікаційне середовище має дві складові: інформаційно-технічну (штучно створену людиною – світ техніки,

технологій тощо) та інформаційно-психологічну (світ живої природи, який охоплює й саму людину). Як наслідок, загалом інформаційну безпеку особистості, суспільства (держави) можна презентувати двома складовими частинами: інформаційно-технічною безпекою та інформаційно-психологічною (психофізичною) безпекою [148].

А. А. Андреєв визначав механізм правового регулювання як взяту в єдності систему правових засобів, за допомогою якої забезпечується результативний правовий вплив на суспільні відносини [149, с. 126].

Т. І. Тарахонич наголошувала на важливості дослідження цього механізму з метою визначення правових засобів і способів упорядкування регульованих відносин [150, с. 14].

У теорії права методи правового регулювання визначаються як сукупність прийомів, способів правового впливу на суспільні відносини. Традиційно виділяють два основні методи правового регулювання: імперативний, заснований на обов'язкових владних розпорядженнях та підпорядкуванні одних учасників іншим, та диспозитивний, що характеризується автономією та рівноправністю сторін, наданням суб'єктам можливості вибору варіантів поведінки.

В. Б. Авер'янов зазначав, що в галузях права такі первинні методи правового регулювання перебувають у різних варіаціях і поєднаннях залежно від характеру регульованих відносин та інших соціальних чинників [151, с. 76].

Інформаційне право належить до галузей публічного права, що визначає домінування імперативного способу правового регулювання, де реалізуються властивості владності та першості державної волі, які властиві адміністративно-правовим відносинам [152, с. 11]. Це характерно для відносин у сфері забезпечення інформаційної безпеки, де держава переважно діє через встановлення правил, обов'язків та заборон, підкріплених заходами юридичної відповідальності.

Більшість норм інформаційного законодавства містять владні розпорядження, пов'язані із здійсненням державними органами певних заходів

забезпечення інформаційної безпеки, дотриманням заборон та виконанням обов'язків фізичними та юридичними особами, неприбутковими організаціями.

Законом України «Про захист інформації в інформаційно-комунікаційних системах» не встановлені алгоритми обмеження доступу до інтернет-ресурсів, які містять протиправний контент. Обмеження доступу до такого контенту передбачає Закон України «Про телекомунікації» та його наступник – Закон України «Про електронні комунікації» [104; 153].

Обмежують доступ провайдери доступу до Інтернету за рішенням суду. Механіку втілення цього заходу в життя законодавство не передбачає. Не регламентуються правила дій державних та інших структур, залучених на кожному етапі процедури вилучення протиправного контенту.

Згідно з рішеннями Європейського суду з прав людини (ЄСПЛ), які було ухвалено у 2020 році, для того, щоб блокування веб-сайтів відповідало вимогам Конвенції, держава зобов'язана забезпечити такі вимоги:

- наявність запобіжників (safeguards). Незалежно від того, яким чином відбувалося блокування ресурсу, власників сайтів повинні повідомляти про захід. Їм необхідно надати можливість висловити власні аргументи стосовно підстав блокування, залучивши до процесу;

- необхідність проведення оцінки впливу заходів з блокування до впровадження. Варто зважати на розмежування між законним і протиправним контентом та розуміти, що окремі види блокувань (наприклад, URL всього сайту, а не окремої сторінки, що містить протиправний контент, блокування за IP-адресою, де розміщено декілька сайтів) будуть апріорі свавільними;

- використання судовими або іншими незалежними органами, які мають розглядати справи про блокування, практики ЄСПЛ і балансування інтересів власників, користувачів та держави при ухваленні відповідного рішення про блокування;

- чіткість визначення категорій протиправного контенту, за поширення яких сайт може підлягати блокуванню;

- будь-які формулювання, навіть розроблені національними судами або

іншими незалежними органами, з яких випливає блокування, повинні мати належне підґрунтя в законодавстві;

- оцінка протиправності контенту та оцінка правомірності блокування має проводитися окремо згідно з практикою Суду з цих питань [154, с. 47].

О. М. Волошин, досліджуючи підходи до захисту прав дітей в Інтернеті, пропонує розробити спрощений механізм видалення матеріалів, що зображують сексуальну експлуатацію та насильство над дітьми хостинг-провайдерами та інтернет-провайдерами, забезпечити можливість блокування ресурсів, що систематично поширюють такий контент, у позасудовому порядку (за зверненням Кіберполіції або органу, який виконуватиме функції забезпечення безпеки в інформаційному просторі). Необхідно відобразити всі елементи процедур у тексті закону, якщо такі процедури впроваджуватиме; впровадити механізми прозорості, зокрема публікувати інформацію щодо кількості ресурсів, до яких обмежено доступ, кількості запитів до іноземних правоохоронних органів (напряму чи через гарячі лінії), кількості вилученого контенту, оцінки кількості постраждалих від сексуальної експлуатації та насильства над дітьми та процесу надання психологічної та іншої допомоги [155].

Водночас в інформаційному праві загалом та правовому регулюванні інформаційної безпеки зокрема є місце та методи диспозитивного регулювання. Закон України «Про захист суспільної моралі» закріплює диспозитивну норму, згідно з якою інтернет-ресурс, що не є мережевим виданням, може містити вікове маркування інформаційної продукції, яке присвоюється самостійно.

Спосіб правового регулювання як найбільш загальна правова категорія охоплює комплекс елементів, якими є методи правового регулювання. Основні способи правового регулювання: дозвіл – надання особам права на власні дії; заборона – покладання на осіб обов’язків утримуватися від здійснення дій певного роду; позитивне зобов’язання – покладання на осіб обов’язків до активної поведінки.

А. В. Чемодурова як додаткові способи називає заохочення та

рекомендації – своєрідні стимули до правомірної поведінки [156, с. 265].

У механізмі правового забезпечення інформаційної безпеки дуже поширене використання правових заборон. Прикладами таких заборон є: заборона зловживання свободою масової інформації; заборона розповсюдження протиправної інформації;заборона недобросовісної та недостовірної реклами; заборона обігу інформаційної продукції, що містить інформацію, заборонену для поширення серед дітей тощо.

Фундаментальне значення у механізмі правового забезпечення інформаційної безпеки має закріплена у ст. 28 Закону України «Про інформацію» заборона поширення протиправної інформації [37]. У ньому проявляється міжгалузева природа аналізованого правового інституту та простежуються галузеві взаємозв'язки інформаційного, адміністративного та кримінального права.

Ця правова заборона сформульована двояко: спочатку через перерахування кількох конкретних видів негативного контенту (інформації, спрямованої на пропаганду війни, розпалювання національної, расової чи релігійної ненависті та ворожнечі), поширення якого забороняється, та через вказівку щодо інформації, за поширення якої передбачена кримінальна чи адміністративна відповідальність.

Законодавець пішов шляхом закріплення відкритого переліку протиправної інформації, який постійно коригується шляхом внесення змін до Кримінального кодексу України (Закон України «Про внесення змін до статті 114^{-2} Кримінального кодексу України щодо удосконалення відповідальності за несанкціоноване розповсюдження інформації про засоби протидії збройній агресії Російської Федерації» [157; 158]).

У проєкті Закону України «Про засади інформаційної безпеки України» (2014 рік) використано дещо інший підхід до формулювання заборони, що розглядається [57]. Встановлено правову заборону на поширення деструктивної інформації: інформації, що порушує права та законні інтереси фізичних та юридичних осіб; інформації, що має деструктивний вплив на індивідуальну,

групову чи суспільну свідомість, що підриває національну безпеку.

Авторами законопроєкту зроблено спробу визначити вичерпний перелік такої інформації. До інформації, що порушує права та законні інтереси фізичних та юридичних осіб, віднесено: неправдиву, таку, що принижує честь та гідність особи, інформацію; відомості, що дискредитують ділову репутацію суб'єкта господарювання; хибні відомості про товари та послуги; інформація, що містить загрози заподіяння шкоди правам та інтересам особи.

Як інформація, що надає деструктивний вплив на індивідуальну, групову або суспільну свідомість, ідентифіковані: інформація порнографічного характеру; інформація, що пропагує культ насильства та жорстокості, що містить заклики до насильницького повалення конституційного ладу, організації або проведення масових заворушень; інформація, що пропагує війни, соціальну, національну, релігійну та расову ворожнечу; інформація, що охоплює загрозу вчинення акту тероризму; відомості про способи, методи розробки, виготовлення та використання, місця придбання наркотичних засобів, психотропних речовин, їх прекурсорів та аналогів, вибухових речовин та вогнепальної зброї. Вони багато в чому збігаються з виділеним у дослідженні переліком основних загроз інформаційній безпеці.

В основі зазначених у проєкті закону видів деструктивної інформації лежить механізм надання деструктивного інформаційного впливу, але його типи різняться. Формування закритого (вичерпного) переліку шкідливої інформації є недоцільним. Якщо для проєкту закону таке рішення може бути виправдане, то в національному законодавстві краще дотримуватися формули, використаної в Законі України «Про інформацію» та інших нормативно-правових актах. Це передбачає вказівку конкретних видів забороненого негативного контенту (прямий спосіб викладу) та заборону поширення інформації, за яку встановлено кримінальну чи адміністративну відповідальність (бланкетний спосіб викладу). Це дозволяє забезпечити певну стабільність правової норми, інакше до неї довелося б постійно вносити доповнення.

Будь-який варіант правової регламентації переліку негативної інформації, забороненої для розповсюдження, вимагає подальшої синхронізації з механізмами обмеження доступу до такої інформації.

В Україні з моменту запровадження Закону України «Про санкції» використано досить цікаву схему [159]. Законодавець встановлює процедури блокування таких ресурсів, які містять певні види забороненої інформації у позасудовому порядку. Перелік видів такої інформації поповнюється. Санкції вводяться у дію указами Президента України на підставі рішення Ради національної безпеки і оборони [160; 161].

Для решти видів протиправного контенту передбачено процедуру обмеження доступу на підставі судового рішення [162].

У 2019 році було затверджено спільний наказ Державної служби спеціального зв'язку та захисту інформації України та Служби безпеки України про затвердження технічних вимог до технічних засобів для блокування доступу до визначених інформаційних ресурсів [163, с. 18]. За даними аналітичного звіту «Санкції та блокування вебсайтів в Україні», станом на 2021 рік заблоковано 633 інтернет-ресурси [163].

У поточному році (2022) за допомогою телеграм-ботів кіберполіції вдалося заблокувати понад 3 тисячі ворожих інтернет-ресурсів. Загальна аудиторія заблокованих ресурсів становила понад 23 млн осіб [164].

Такий алгоритм роботи правового механізму блокування можна вважати прийнятним. Однак очевидна відсутність системності та чітких методологічних принципів функціонування.

Правовим способом забезпечення інформаційної безпеки у межах імперативного методу регулювання є зобов'язання. Воно виявляється у закріпленні обов'язків певних суб'єктів інформаційної сфери відповідно до регламентації їх правового статусу. Такі обов'язки Законом України «Про електронні комунікації» встановлено для оператора електронних комунікацій (послуг).

Значущими у контексті забезпечення інформаційної безпеки є юридичні

обов’язки:

- не допускати використання сервісу з метою вчинення кримінальних діянь, поширення пропаганди тероризму, матеріалів, що пропагують порнографію, культ насильства та жорстокості;

- перевіряти достовірність поширених суспільно значимих відомостей до поширення;

- не допускати використання сервісу з метою приховування або фальсифікації суспільно значимих відомостей, поширення недостовірної суспільно значущої інформації новин під виглядом достовірних повідомлень;

- не допускати поширення інформації з метою знеславити громадянина або окремі категорії громадян за ознаками статі, віку, расової чи національної приналежності, мови, ставлення до релігії, професії, місця проживання та роботи, у зв’язку з політичними переконаннями.

Частина сформульована за типом пасивних обов’язків, тобто обов’язки не допускати, але реалізація передбачає активну діяльність з вивчення, перевірки та оцінки контенту, що поширюється, вживання заходів щодо припинення обігу недостовірного контенту в певних випадках.

У Законі України «Про друковані засоби масової інформації (пресу) в Україні» правову заборону на поширення певних видів інформації встановлено не лише для засобів масової інформації, а й стосовно інформаційно-комунікаційних мереж. Водночас використання засобами масової інформації з метою поширення фейкової (fakenews) інформації не знайшло відображення серед форм зловживання правом на інформації у Законі України «Про інформації» [37].

О. А. Невельська-Гордєєва та В. О. Нечитайло, досліджуючи «Феномен «fakenews» у контексті забезпечення інформаційної безпеки держави», зазначають, що неправдива інформація – «fakenews» – існує в усіх сферах суспільства. Завдяки розвитку інформаційних технологій вони стали поширюватися ще швидше та охоплюють більшу аудиторію. Загроза пропаганди, дезінформації, бажання похитнути авторитет та викликати агресію

приносять величезну кількість проблем у сучасному світі. Інформаційні війна є однією з таких проблем, з якими зіштовхнулися багато країн, у тому числі й Україна. Психологічні операції є надзвичайно інтерактивними та застосовуються з однією метою – знизити можливі ризики з боку населення та здобути його довіру. Тому першим кроком у бік запобігання дезінформації є медіаобізнаність, власна усвідомленість та глибокий аналіз новин, що поширюються [165, с. 131].

На думку В. В. Володовської, в умовах відсутності розвинутого саморегулювання медіа в Україні та зважаючи на російську агресію, що супроводжуються інформаційними кампаніями, які загрожують національній безпеці, пропозиція впровадження більш чіткого регулювання діяльності онлайн-медіа, виглядає виправданою [166].

Популярні блогери мають велику аудиторію, що за впливом можна порівняти з деякими засобами масової інформації, а тому виступають потужними потенційними джерелами деструктивного інформаційного впливу. Проєкт закріплював обов’язок блогерів дотримуватись приписів законів, зокрема: не допускати зловживання свободою масової інформації; перевіряти достовірність загальнодоступної розміщеної інформації до розміщення та видаляти розміщену недостовірну інформацію; не допускати публікацію відомостей про приватне життя громадянина та інше [167].

Низку конкретних обов’язків, зокрема перевірка достовірності інформації, що публікується, видалення фейків, ніде більше не закріплено.

Авторка не наполягає на «реставрації» проєкта закону, проте вважає за необхідне визначити правову регламентацію статусу такої категорії учасників інформаційної сфери, як блогери.

Третім правовим методом регулювання забезпечення інформаційної безпеки є дозвіл, що уособлює диспозитивний спосіб регулювання. Дозвіл переважно використовується в інформаційному праві під час регламентації правового статусу фізичних осіб.

Введення у дію у 2022 році Закону України «Про електронні комунікації»

надає громадянину право у разі виявлення в Інтернеті недостовірних зневажливих відомостей, пов'язаних із звинуваченням у скоєнні злочину, направити оператору звернення про вжиття заходів щодо видалення зазначеної інформації або блокування Інтернет-ресурсів, що їх розповсюджують. Проте дозволи можуть стосуватися інших суб'єктів інформаційних правових відносин.

Наприклад, Закон України «Про захист суспільної моралі» наділяє правом здійснювати громадський контроль за дотриманням вимог закону не лише громадян, а й громадські об'єднання, у тому числі через формування гарячих ліній.

Дозвіл є важливим методом правового забезпечення інформаційної безпеки і його застосування має розширюватися. Вектором такого розширення має стати правова регламентація прав фізичних та юридичних осіб щодо участі у забезпеченні інформаційної безпеки.

Надзвичайно перспективним є завершення реалізації правової ініціативи Міністерства інформаційної політики України щодо залучення інститутів громадянського суспільства до протидії деструктивним інформаційним впливам, яка була реалізована протягом 2018-2020 років [168; 169].

Що стосується додаткових способів правового регулювання, до яких належать заохочення та рекомендації, то вони знаходять необґрунтовано мале застосування у механізмі правового забезпечення інформаційної безпеки. Це стосується законодавчого рівня, де таких норм практично немає. Розвиток таких способів регулювання, як пільги та стимули, можна віднести до трансформації правового регулювання інформаційної безпеки.

У нормативних документах Європейського Союзу активно застосовуються заохочувальні та рекомендаційні норми, присвячені забезпеченню інформаційної безпеки. Наприклад, Директива Європейського Парламенту і Ради (ЄС) 2016/1148 від 06 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу, Regulation (EU) 2019/881 of the European Parliament and of the

Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)[170; 171].

Досвід участі авторки у щорічних міжнародних конференціях з проблем інформаційного права та інших подібних конференціях, де були присутні представники провідних засобів масової інформації та компаній інтернет-галузі, показав, що зі сторони зазначених суб'єктів у добровільному порядку реалізовано ряд позитивних ініціатив, спрямованих на протидію інформаційним загрозам [172-175]. Проте держава недостатньо чітко сформулювала зацікавленість у реалізації таких ініціатив громадянського суспільства та інтернет-галузі. Зробити це можна було б за допомогою заохочувальних та рекомендаційних правових норм. Позитивним у цьому плані є розробка проєкту Концепції та плану заходів з розвитку цифрових прав дітей [176].

У Концепції закріплено комплекс заохочувальних та рекомендаційних норм, спрямованих на стимулювання участі інститутів громадянського суспільства у забезпеченні інформаційної безпеки дітей та поширення наявного позитивного досвіду в цій сфері.

Доцільно зауважити, що появі проєкту Концепції передували наукові дослідження. О. В. Топічий у дисертації «Адміністративно-правове забезпечення інформаційної безпеки неповнолітніх в Україні» (2019 рік), у своїй роботі зазначала, що аналіз чинного законодавства дозволив констатувати, що нині не існує єдиного консолідованого акту, яким би врегульовувався комплекс питань, пов'язаних із забезпеченням інформаційної безпеки. Окремі норми розпорошені в десятках не узгоджених між собою законів. Значна частина актів, які містять деякі проєкції проблеми, морально застаріла й не відповідає вимогам сьогодення. Більшість законів слабко вписується в сучасну парадигму епохи інформаційних війн, спеціальних психологічних операцій, не відображають протиріччя глобалізаційної доби в контексті негативного впливу на неповнолітніх. Обмежувальні та заборонні заходи адміністративного впливу переважають порівняно із засобами

переконання й організації просвіти. Увага законодавця здебільшого сконцентрована на телерадіосфері, пресі, а не на врегулюванні інформаційних правовідносин у медіапросторі [177, с. 29].

Зокрема, Концепція передбачає: надання державної підтримки соціально значимим проєктам у галузі друкованих та електронних мас-медіа для дітей та молоді, узагальнення кращих форм з підтримки регіональних виробників інформаційної продукції для дітей з подальшим виробленням рекомендацій для органів місцевого самоврядування; організацію та проведення конкурсу соціальної реклами пропаганди здорового способу життя, спрямованого на формування у підлітків та молоді негативного ставлення до незаконного споживання наркотиків та ін.

Такі механізми охоплюють певні правові засоби та методи чи їх комплекс. Проведений аналіз інформаційного законодавства дозволив вирізнити такі:

1. Встановлення правових заборон та інших обмежень поширення певних видів негативної інформації – означає правове закріплення заборон поширення негативного контенту, обмежень інших видів.

Правові обмеження можуть виражатися у зменшенні кількості можливих форм здійснення права чи свободи, у фіксації чи звуженні просторових та тимчасових кордонів реалізації права чи свободи, кола осіб, які мають можливість користуватися правом (свободою), у виключенні юридичної можливості здійснення права чи свободи у певних випадках, в ускладненні порядку здійснення права або свободи, а також у знищенні, вилученні або применшенні блага, що лежить в основі конституційного права або свободи.

Основне значення має норма ст. 28 Закону України «Про інформацію», яка встановлює заборону розповсюдження протиправної інформації.

Нормами кримінального та адміністративно-деліктного права може встановлюватися заборона не лише на розповсюдження, а й на виготовлення певних видів негативного контенту, наприклад дитячої порнографії (ст. 301^{-1} «Одержання доступу до дитячої порнографії, її придбання, зберігання,

ввезення, перевезення чи інше переміщення, виготовлення, збут і розповсюдження КК України [178]). Критерії віднесення продукції до такої, що має порнографічний характер, визначені наказом Міністерства культури України [179].

Складніший механізм регламентований ст. 7 «Захист дітей від негативного впливу продукції сексуального чи еротичного характеру» Закону України «Про захист суспільної моралі» [50].

А. О. Нестеренко в дисертаційному дослідженні «Адміністративно-правове забезпечення прав дітей в інформаційному середовищі» пропонує внесення доповнень до Закону України «Про охорону дитинства» щодо визначення терміну «інформаційна безпека дітей» – стан захищеності дітей, при якому нема ризику, пов'язаного із заподіянням інформацією шкоди їх здоров'ю та (або) фізичного, психічного, духовного, морального розвитку [180, с. 84].

Н. В. Лесько в дослідженні «Правові засади попередження медіанасильства щодо дітей» зазначає, що медіанасильство – форма психологічного насильства, що охоплює пропагування через засоби масової комунікації насильницьких дій, якщо це викликає у постраждалої особи емоційну невпевненість, нездатність захистити себе або завдає шкоду психічному здоров'ю [181, с. 103].

2. Закріплення спеціальних правил обігу інформаційної продукції певних видів – означає встановлення правовими нормами спеціальних умов виробництва та поширення негативної інформації. Такі умови можуть охоплювати просторові та тимчасові обмеження розповсюдження контенту, додаткові вимоги до обігу інформаційної продукції. Усі вони знайшли відображення у Законі України «Про захист суспільної моралі».

У законодавстві встановлено низку додаткових вимог поширення певних видів інформаційної продукції. Наприклад, продукція сексуального чи еротичного характеру може розповсюджуватися лише за умови герметичної упаковки, спеціального маркування і за наявності повідомлення «продукція

сексуального характеру, продаж дітям заборонено». Це передбачено Законом України «Про внесення змін до Закону України «Про захист суспільної моралі» щодо захисту прав та найкращих інтересів дитини» [182].

3. Закріплення обов'язків суб'єктів інформаційних правовідносин щодо забезпечення інформаційної безпеки означає встановлення правовими нормами зобов'язань учасників правовідносин щодо забезпечення інформаційної безпеки. Такий правовий механізм використовує законодавець стосовно ключових інформаційних посередників у мережі Інтернет. Важливим стало закріплення обов'язків соціальних мереж здійснювати моніторинг з метою виявлення протиправного контенту та вживати заходів щодо обмеження доступу [183, с. 26, 45].

4. Вікова класифікація та маркування інформаційної продукції – передбачає проведення класифікації інформаційної продукції щодо прийнятності інформації для людей певних вікових категорій з наступним нанесенням на таку продукцію присвоєного знака вікової категорії [184].

Сам правовий механізм вікової класифікації та маркування використовується подвійним чином. З одного боку, вона є основою для встановлення правових режимів обігу інформаційної продукції певних вікових категорій, а з іншого – має самостійну значущість як спосіб оповіщення дорослих про вікові обмеження інформаційної продукції для прийняття рішення про доцільність та допустимість показу дітям.

5. Експертиза інформаційної продукції означає проведення досліджень інформаційної продукції із залученням спеціальних знань. Основним нормативно-правовим актом, що регламентує експертну діяльність, є Закон України «Про судову експертизу» [185]. Закон регламентує провадження експертизи у межах кримінального, цивільного та адміністративного судочинства. Експертизи проводяться у справах про злочини, адміністративні правопорушення або цивільно-правові делікти, пов'язані з наданням деструктивного інформаційного впливу (наприклад, справи про порушення ненависті або ворожнечі, приниження людської гідності).

Однак у правозастосовній практиці проводяться експертизи поза межами судочинства за завданнями правоохоронних органів, організацій, приватних фізичних та юридичних осіб. Це здійснюють відповідні підрозділи кіберполіції України [186]. Основним видом експертиз у сфері інформаційної безпеки є лінгвістична експертиза тексту. Однак можуть проводитися інші види експертиз, наприклад, психофізіологічна, комп'ютерно-технічна та інші експертизи з метою дослідження наявності прихованих вставок, що впливають на підсвідомість людей або надають шкідливий вплив на їх здоров'я.

6. Ідентифікація особи абонентів, користувачів мережі Інтернет та цифрових сервісів – означає систему заходів, спрямовану встановлення та перевірку справжності особи користувачів інформаційних сервісів і послуг. Ідентифікація – це інформаційний процес, спрямований на встановлення суб'єктного та об'єктного складу правовідносин на основі ідентифікаторів або їхньої сукупності.

Ідентифікація особи – процедура використання ідентифікаційних даних особи з документів, створених на матеріальних носіях та/або електронних даних, у результаті виконання якої забезпечується однозначне встановлення фізичної, юридичної особи або представника юридичної особи [187].

Значимість ідентифікації в механізмі забезпечення інформаційної безпеки обумовлюється тим, що спрямована на усунення анонімності як одного з важливих факторів, що утворюють загрозу в цифровому середовищі. Анонімністю користуються іноземні спецслужби та злочинці для здійснення шкідливої діяльності в цифровому середовищі, пов'язаному з негативним інформаційним впливом на окремих індивідів або соціальні групи. Фактор анонімності найбільш активно проявляється при використанні мобільного зв'язку та інформаційно-комунікаційних мереж. Останніми роками законодавець вніс до чинного інформаційного законодавства низку норм, спрямованих на усунення чи зниження впливу анонімності в електронних комунікаціях [188].

Реалізація різних методів ідентифікації за умов цифрової трансформації

сприяє вирішенню важливого завдання забезпечення довіри до цифрових комунікацій.

7. Видалення чи обмеження доступу до протиправного контенту – охоплює правові методи та засоби обмеження доступу до забороненої інформації або її видалення.

8. Встановлення юридичної відповідальності за правопорушення, що посягають на інформаційну безпеку – означає правове закріплення складів правопорушень та заходів відповідальності за вчинення. Ключове значення тут мають норми кримінального та адміністративно-деліктного законодавства. Безперервне розширення спектра загроз інформаційній безпеці особи, суспільству та державі диктує потребу постійного доповнення складів правопорушень. Формою юридичної відповідальності за правопорушення, що посягають на інформаційну безпеку, є цивільно-правова відповідальність, що регламентується Цивільним кодексом України.

9. Правове регулювання заходів контрпропаганди – означає правову регламентацію заходів контрпропаганди, змістом якої є надання зустрічного інформаційного впливу з метою нейтралізації деструктивної інформаційної активності противника (джерела загрози). В інформаційному законодавстві брак норм, які комплексно регулюють цей напрям діяльності. Фрагментарне правове регулювання з цього питання є у Законі України «Про боротьбу з тероризмом» та в інших законодавчих актах, які стосуються сфери адміністративного права.

10. Правове стимулювання розвитку цифрової грамотності та формування культури інформаційної безпеки – охоплює правові засоби, спрямовані на стимулювання підвищення поінформованості громадян про наявні загрози інформаційній безпеці,джерела та форми прояву, правила безпечної поведінки в інформаційному середовищі.

Проєкт Концепції виховання дітей та молоді в цифровому просторі серед пріоритетних завдань забезпечення інформаційної безпеки закріпив формування у дітей навичок самостійного та відповідального споживання

інформаційної продукції та підвищення рівня медіаграмотності [189].

Оскільки основна роль у підвищенні цифрової грамотності та формуванні культури інформаційної безпеки відводиться системі освіти та інститутам громадянського суспільства, головними завданнями держави є стимулювання та підтримка таких ініціатив.

Заходи щодо формування культури інформаційної безпеки знайшли відображення у Пріоритетних напрямах та завданнях (проєктах) цифрової трансформації на період до 2023 року [190].

У дисертаційному дослідженні «Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні» (2019 рік) Т. С. Перун зазначає, що механізм правового регулювання – це система спеціально-юридичних засобів, організованих послідовним чином, спрямованих на регулювання суспільних відносин певного виду. Конструювання механізму правового регулювання забезпечення інформаційної безпеки має здійснюватися відповідно до цілі правового регулювання. Ціль правового регулювання, будучи частиною управлінського процесу та результатом правової політики, передбачає об’єднання певних правових засобів для досягнення правового результату, визначаючи при цьому природу механізму правого регулювання [3,с. 201].

В умовах цифрової трансформації зміни зазнає сфера правового регулювання, у якій формуються відносини, що охоплює безпосередню участь громадян, у тому числі у сфері інформаційної безпеки. Багато нових відносин не можуть бути врегульовані своєчасно через відсутність відповідних цифрових технологій та можливостей здійснення контролю реалізації. Правова практика потребує оптимального поєднання юридичних та цифрових технологій величезного спектра відносин, які підпадають під сферу правового регулювання, що визначаються об’єктивними умовами життя.

У національній правовій системі формуються суспільні відносини, які раніше не вимагали правової регламентації. Їх учасниками є анонімні цифрові суб’єкти у віртуальному просторі. Регулювання подібних відносин передбачає

заміну багатьох юридичних процедур у чинному праві, пов’язаних, перш за все, з ідентифікацією особи як суб’єкта права, з реалізацією прав людини у цифровому просторі, з використанням баз даних, що впливає на забезпечення інформаційної безпеки.

Проаналізувавши адміністративно-правові засоби та механізми забезпечення інформаційної безпеки, ми зробили такі висновки.

Дослідження сучасних адміністративно-правових засобів та механізмів забезпечення інформаційної безпеки в умовах цифровізації передбачає детальний розгляд специфіки правового та організаційного регулювання у попередні історичні періоди.

В інформаційному праві та на практиці склався комплекс юридичних засобів, які при системному застосуванні дозволяють забезпечувати інформаційну безпеку. Системне та впорядковане застосування юридичних засобів дозволяє виявити існування забезпечувального механізму. Як основний підхід до аналізу сутності названого механізму використовувався інституціоналізм, що передбачає охоплення названим механізмом та вивчення окремих адміністративно-правових норм або інститутів адміністративного та інформаційного права та практику застосування за допомогою діяльності держави, органів публічної адміністрації, інститутів громадянського суспільства, судових та квазісудових органів. За такого підходу інституційний механізм забезпечення інформаційної безпеки є комплексним правовим явищем. Забезпечення інформаційної безпеки потребує активного впровадження інновацій, поступового переходу до механізмів, передбачених нормативними актами НАТО та Європейського Союзу.

Наразі триває подальший розвиток законодавства щодо удосконалення адміністративно-правових засобів та механізмів забезпечення інформаційної безпеки. Передбачувані зміни можуть торкнутися спектру питань, важливими з яких в аспекті проблем адміністративно-правового регулювання є посилення державного контролю за раціональним використанням ресурсів та вдосконалення взаємодії органів публічної влади та інститутів громадянського

суспільства в досліджуваній сфері. Це пов’язано з великим обсягом чинних нормативно-правових актів, що регламентують складову діяльність у сфері інформаційної безпеки. Щодо видання локальних нормативно-правових актів адміністративно-правового регулювання, то вони можуть здійснюватися незалежно один від одного компетентними органами.

Аналіз дозволив зробити висновок про те, що адміністративно-правові засоби та механізми забезпечення інформаційної безпеки в умовах проведення цифровізації в Україні становлять досить складне поєднання політико-правових та адміністративно-правових норм, які відповідають за певну сферу діяльності органів публічної влади та суб’єктів господарювання.

Органи публічної влади у сфері інформаційної безпеки повинні демонструвати систему горизонтально та вертикально взаємно збалансованих та взаємопов’язаних публічно-правових утворень, до завдань яких належить координація з метою недопущення виникнення загроз інформаційній безпеці особи, суспільства та держави.

2.2. Правові обмеження у контексті забезпечення інформаційної безпеки на прикладі засобів масової інформації

Ставлення держави до інформаційної сфери визначається історією та сучасністю, залежить від ступеня розвитку демократичних інститутів у минулому та сьогодні, рівня приватизації засобів масової комунікації, впливу релігійних традицій, стану технічної бази засобів масової інформації та масштабу запровадження нових технологій. Вплив на інформаційний процес надають нові технології, швидкість, масштаб і характер запровадження. З огляду на швидкість запровадження деякі держави частково втрачають можливості контролю. Інші держави, навпаки, завдяки застосуванню таких технологій успішно контролюють внутрішню інформацію і закріплюють своє становище щодо інших держав, які використовують їх інформаційну продукцію. Посилюється позиція тих, хто створює технології.

Технологічні новинки не тільки впливають на можливості держав контролювати інформаційні потоки, а й на міжнародні відносини. Технології мають ще один важливий вимір. Нова технологія здатна транслювати інформацію, що змінює уяву людей про себе і суспільство, запроваджувати нові цінності й орієнтації.

В Україні, як зазначає К. В. Захаренко, не існує системи інформаційної безпеки, що відповідає сучасним цивілізаційним і геополітичним викликам. Тому насправді управління безпекою інформації потрібно посилити у всіх сферах: у нагляді, організації та управлінні й інформаційних технологіях. Окрім новітніх викликів та реалій, що не врегульовані або не передбачені чинним законодавством, не одне десятиріччя існують проблеми інформаційного простору, що потенційно становлять ризики для інформаційної безпеки держави. Серед них можемо виділити: проблеми створення суспільного мовлення та приналежності засобів масової інформації фінансово-промисловим олігархічним групам; проблеми законодавчого регулювання інформаційної діяльності в мережі Інтернет і поширення інформації у соціальних інтернет-мережах [191, с. 372-373].

Адміністративна діяльність органів публічної влади в інформаційній сфері забезпечує соціальну динаміку відтворення суспільних відносин. Тому особливість правомірного обмеження прав громадян органами публічної влади в інформаційній сфері з метою забезпечення інформаційної безпеки полягає не в блокуванні соціальної взаємодії, а в сприянні суспільно-правовій комунікації.

Узгодження публічних та приватних інтересів шляхом поєднання публічно-правового та приватно-правового регулювання, державного регулювання та саморегулювання – усе це в комплексі має забезпечити соціальне спрямування цифровізації у сфері інформаційної безпеки [192, с. 67].

В. Г. Чорна, розглядаючи відносини адміністративно-правових обмежень, пропонує розрізняти суб’єктів відносин адміністративних обмежень, де, з одного боку, суб’єктом є суб’єкт застосування адміністративних обмежень – уповноважений суб’єкт, який має відповідні повноваження, а з іншого – інший

суб'єкт, якого пропонуємо називати суб'єктом-контрагентом, тобто особа, до якої застосовується адміністративне обмеження та на поведінку якої направлено правовий вплив. Перша і друга група суб'єктів є безпосередньо суб'єктами відносин адміністративних обмежень, під якими пропонуємо розуміти уповноважених суб'єктів публічної адміністрації, їх посадових осіб і структурні підрозділи, суд, а також суб'єктів-контрагентів – фізичних і юридичних осіб, на поведінку яких направлений владний управлінський вплив. Суб'єкти застосування можуть бути суб'єктами різного ієрархічного рівня (наприклад, Кабінет Міністрів України й органи місцевого самоврядування), а суб'єкти-контрагенти можуть мати різний адміністративно-правовий статус (наприклад, Президент України, громадяни України, іноземці, особи без громадянства) [193, с. 57-58].

Суб'єкти публічної влади шляхом застосування обмежень здійснюють санкціонування соціально значущої діяльності в інформаційному просторі. Разом із цим обмеження права дозволяють органам публічної влади реалізовувати власні оперативні повноваження в процесі здійснення адміністративної діяльності.

Дослідження з питань правового регулювання обмежень прав, у тому числі в інформаційному просторі, здійснювали відомі представники юридичної науки: В. Б. Авер'янов, І. В. Арістова, О. Ф. Андрійко, О. М. Бандурка, О. А. Баранов, Ю. П. Битяк, В. М. Гаращук, І. П. Голосніченко, С. Т. Гончарук, Є. В. Додін, Ю. М. Дьомін, Р. А. Калюжний, А. Т. Комзюк, Т. О. Коломоєць, В. К. Колпаков, В. Я. Настюк, О. І. Остапенко, В. Г. Перепелюк, О. П. Рябченко, А. О. Селіванов, Ю. М. Тодика, В. К. Шкарупа, М. Г. Шульга та ін.

Обмеження прав громадян органами публічної влади – це регулювальний механізм, а не інструмент державного придушення. Звідси випливає, що правомірне обмеження прав громадян органами публічної влади – це правовий засіб динамічного характеру, що має компенсаційний механізм, застосовуваний владною стороною з власної ініціативи на основі норм адміністративного права, що транслює державну функцію застосування методів адміністративно-

правового впливу на права, свободи та законні інтереси громадян, інших невладних суб'єктів з метою підтримки встановленого порядку управління та забезпечення безпеки.

О. І. Остапенко зазначає, що адміністративно-правові заборони, метою яких є сприяння захисту прав, свобод і законних інтересів людини та громадянина, виявляють в дії (недопущення, обмеження, примус), спрямовані на запобігання протиправним діям та настання суспільно шкідливого і небезпечного за наслідками результату. Передбачені в адміністративно-правових нормах дії, спрямовані на заборону та обмеження, є дозволеними і їх схвалює та підтримує держава [194, с. 54].

Охоплення структурою змістової частини адміністративної діяльності методів адміністративно-правового впливу, правомірних обмежень прав громадян як правового засобу забезпечують умови для сталого застосування методу. Органи публічної влади за допомогою обмежень права домагаються впливу на невладних суб'єктів, досягаючи поставленої мети з дотримання та виконання адміністративно-режимних вимог.

Послідовне застосування методів адміністративно-правового впливу розкриває функціональні сторони обмежень прав громадян органами публічної влади. У процесі формування адміністративної політики виробляються перспективні параметри інтенсивності, функціональності та локалізації застосування обмежень прав громадян органами публічної влади, що в контексті інформаційного простору здійснює Стратегія інформаційної безпеки України.

Проблема методів державно-управлінської діяльності або адміністративно-правового впливу лежить у площині їх розумного поєднання з урахуванням об'єктивних чинників, інших умов. Послідовне розв'язання цього завдання залежить від термінів роботи щодо впорядкування всієї системи державного управління відповідно до мети політичного й економічного реформування суспільного життя [195, с. 350].

У межах статусних адміністративно-правових режимів обмеження права

набуває відповідних форм. Обмеження прав громадян у формі нав'язування з боку публічної адміністрації вводять громадянина в предметну площину адміністративно-правових відносин, наділяючи загальним адміністративно-правовим статусом.

У процесі реалізації методу адміністративного визнання права (легалізації) обмеження прав проявляється у формі перешкод, долаючи які невладний суб'єкт отримує можливість здійснювати спеціальні види суспільно-корисної діяльності.

У ході ліцензійно-дозвільної дії громадянин зіштовхується з обмеженнями прав у формі бар'єрів, дотримання яких дозволяє здійснювати особливо значущу діяльність у межах встановлених адміністративно-правових вимог.

Шляхом створення умов органами публічної влади для здійснення різних видів діяльності та сприяння у забезпеченні життєдіяльності невладних суб'єктів проявляється компенсаційний механізм обмеження прав громадян у межах регулювальних методів адміністративно-правового впливу.

О. В. Ткаля зазначає, що адміністративно-правовий вплив на поведінку осіб спрямовано на забезпечення балансу інтересів особи, суспільства і держави. Це специфічна дія права на адміністративно-правові відносини активного та пасивного характеру правовими, психологічними, ідеологічними, моральними, інформаційними та іншими засобами, що здійснюється спеціально уповноваженими суб'єктами владних повноважень [196, с. 162].

Обмеження прав громадян, окрім задоволення приватного інтересу невладних суб'єктів, можуть забезпечувати виконання оперативно-виконавчих завдань суб'єктів адміністративної діяльності. Найчастіше застосовуване органом публічної влади обмеження права служить інструментом реалізації профілактичної та пошукової функції, функції припинення у межах адміністративно-юрисдикційної діяльності у контексті порушення інформаційної безпеки. Встановлюється оригінальний вид ситуаційного адміністративного режиму, у межах якого органи публічної влади застосовують

обмеження прав громадян за власним (оперативним) інтересом, наприклад, з метою залучення громадянина для надання сприяння представнику влади або реалізації власних публічних функцій, у тому числі у сфері інформаційної безпеки.

Важливість виділення індивідуального режиму пов'язані з тим, що характер застосовуваних обмежень права найчастіше за суворістю можна порівняти з юрисдикційними обмеженнями, але, на відміну від останніх, застосовується за відсутності протиправної поведінки громадянина. У зв'язку з цим обмежене право невладного суб'єкта підлягає компенсації, оскільки в таких ситуаціях органу публічної влади з метою дотримання та гарантування прав громадян слід керуватися правилом: не підлягають компенсації лише ті права, які обмежені у зв'язку з протиправністю поведінки невладної сторони. З позиції інформаційної безпеки – це ліквідація деструктивного інформаційного впливу.

Б. Д. Леонов і О. Г. Семенюк зазначають, що правовий інструментарій, що діє в певному напрямі та забезпечує досягнення поставленої мети у вигляді захисту інформаційних прав особи, суспільства та держави, необхідно об'єднати в однорідні комплекси спеціальних правових режимів інформації. Це дозволить не просто обмежити доступ до різних видів інформації, а визначатиме єдину систему підходів до регулювання однорідних правовідносин, можливі винятки, їх підстави, порядок введення і припинення дії режиму, терміни його дії [197, с. 48].

З метою оптимізації та підвищення ефективності правозастосовної діяльності органів публічної влади необхідно внесення змін до законодавства, спрямованого на виключення низки додаткових адміністративних покарань у сфері інформаційної безпеки та їх заміни на інші галузеві обмеження.

У науковій літературі пропонують використання механізму наростаючої репресії із застосуванням інших галузевих обмежень під час виборів заходу державного примусу за порушення адміністративних вимог у сфері інформаційної безпеки.

Формування інформаційного суспільства та побудова правової держави, інтеграція в європейський правовий простір тісно взаємопов'язані не тільки з суб'єктивними правами та свободами, але й з правовими обмеженнями публічної влади, прав і свобод людини та громадянина в інформаційному просторі, що обумовлено необхідністю забезпечення інформаційної безпеки.

Виникла проблема пошуку балансу в системі прав, свобод, обов'язків та обмежень прав, свобод, законних інтересів та повноважень суб'єктів права з метою підтримки стабільності в країні, забезпечення умов для існування кожного індивіда, поступального розвитку суспільства та держави.

Унаслідок аналізу точок зору щодо поняття та сутності правових обмежень у сфері інформаційної безпеки як центральної категорії, що визначає функціональне призначення інституту правових обмежень в інформаційному праві, можна стверджувати, що перспективами розвитку нормативно-правового закріплення інформаційних прав громадян є утвердження права людини на інформаційну безпеку, зокрема в частині захищеності людини від неповноти, невчасності та невірогідності інформації, що використовується, від негативних інформаційних впливів. Наприклад, ст. 34 Конституції України може бути доповнена ч. 4 такого змісту: «Кожен має право на захист від інформації, яка може зашкодити його здоров'ю та (або) розвитку. Перелік інформації, що завдає шкоди здоров'ю та розвитку особистості, визначається законом» [198, с. 26].

Адміністративно-правові обмеження в інформаційному праві – це закріплені у чинному законодавстві та забезпечені примусовою силою держави межі дозволеної поведінки суб'єктів, виражених у винятках певних можливостей у діяльності та вилученнях з їх правового статусу, що створюють несприятливі умови для задоволення власних інтересів суб'єктів стримування та водночас задоволення інтересів контрагентів чи публічних інтересів, які охороняються державою.

Конституційний Суд України зазначає, що звуження змісту та обсягу прав і свобод є їх обмеженням. У традиційному розумінні діяльності

визначальними поняття змісту прав людини є умови і засоби, які становлять можливості людини, необхідні для задоволення потреб її існування та розвитку. Обсяг прав людини – це їх сутнісна властивість, виражена кількісними показниками можливостей людини, які відображені відповідними правами, що не є однорідним і загальним. Загальновизнаним є правило, згідно з яким сутність змісту основного права в жодному разі не може бути порушена [199].

Щодо інституту адміністративно-правових обмежень в інформаційному праві як комплексного нормативно-правового утворення, додатково виділено такі ознаки: однорідний і системний характер, комплексність, обумовленість предметом і методом правового регулювання відповідних суспільних відносин, тобто специфічним режимом регулювання, що забороняє; універсальний характер, наявність специфічного змісту, що охоплює правові норми (основний компонент), принципи, юридичні конструкції, поняття, загальні положення, терміни.

З урахуванням виділених ознак запропоновано авторське визначення інституту правових обмежень у сфері інформаційної безпеки як специфічного комплексу правових норм, принципів та конструкцій, що утворюють певну систему, відокремленого єдиним правовим режимом, який регулює суспільні відносини, пов’язані зі встановленням меж дозволеної поведінки суб’єктів права. Зміст інституту правових обмежень у сфері інформаційної безпеки складають правові норми, принципи та конструкції, що закріплюють та визначають зміст відповідних правових обмежень, а також поняття та терміни, характерні для конкретного інституту (підгалузі) інформаційного права.

Основною складовою юридичних інститутів є правові норми, але не їх довільне поєднання, а певна сукупність, пов’язана юридичним змістом та безпосереднім ставленням до регульованих суспільних відносин.

Інститут правових обмежень складається з асоціації правових норм – генеральної конституційної норми (ст. 64 Конституції України) та деталізованих або варіантних розпоряджень, закріплених у поточному законодавстві та підзаконних нормативно-правових актах [127].

Під принципами інституту правових обмежень розуміються вихідні ідеї, базові положення, встановлення, що визначають загальну спрямованість правового регулювання у сфері обмеження права і свободи людини та громадянина, а також повноважень інших суб'єктів права, межі і умови встановлення.

Системою принципів інституту правових обмежень у контексті забезпечення інформаційної безпеки охоплено:

- загальні принципи конкретного інституту, що визначають найбільш суттєві риси правового обмежувального регулювання, його зміст та особливості, що поширюються на всі галузі права незалежно від характеру та специфіки регульованих суспільних відносин;

- спеціалізовані принципи інституту правових обмежень (міжгалузеві та галузеві).

Юридичні конструкції інституту правових обмежень у сфері інформаційної безпеки обумовлені предметом та методом правового регулювання відповідних суспільних відносин, тобто специфічним юридичним режимом регулювання, в основі якого лежать загальні заборони та позитивні зобов'язання (як методи правового регулювання), конкретні заборони, обов'язки, заходи покарання та примусу (як засоби правового регулювання).

У межах відповідного режиму, що вказує на заборону, встановленого в інституті правових обмежень, виділено юридичні конструкції: правова заборона; юридичний обов'язок; зупинення; ценз; заходи державного примусу та покарання.

Правова заборона як юридична конструкція інституту правових обмежень полягає в юридично закріпленому обов'язку утриматися від протиправних (або небажаних) діянь під загрозою застосування заходів державного примусу.

Юридичний обов'язок є передбаченою законом (угодою сторін) мірою належної владно приписаної, необхідної поведінки особи, яка перебуває в необхідності особи вчинити певні дії, чи утриматися від вчинення.

Призупинення визначено як тимчасову заборону на здійснення фізичними

і юридичними особами діяльності (повноважень) з метою запобігання вчиненню правопорушень або недопущення інших суспільно небезпечних наслідків під загрозою застосування юридичної відповідальності.

Правові цензи є встановленими законом умовами, що обмежують доступ особи до здійснення певних суб'єктивних прав.

Основні вимоги до юридичних конструкцій щодо інституту правових обмежень у контексті забезпечення інформаційної безпеки можна подати таким чином:

- регулятивна норма має бути забезпечена охоронною нормою, яка встановлює юридичну відповідальність за порушення заборон та невиконання обов'язків;

- матеріальна норма повинна забезпечуватися процесуальною, яка встановлює порядок реалізації та застосування матеріального права;

- елементи юридичних конструкцій правових обмежень мають бути викладені у відповідному правовому розпорядженні послідовно, повно та несуперечливо;

- модель обмеження, представлена певною юридичною конструкцією, повинна найбільш повно відповідати реальності, тобто специфіці суспільних відносин, стосовно яких встановлюється.

Цілі інституту правових обмежень визначені як передбачувана або закріплена державою ідеальна модель меж дозволеної поведінки суб'єктів, що досягається за допомогою реалізації правових засобів, які входять до його (юридичного інституту) складу, і спрямована на стримування протиправної (або небажаної для держави) поведінки суб'єктів права, захист публічних інтересів, задоволення інтересів інших суб'єктів правовідносин.

Основними цілями інституту правових обмежень, що поширюються на всі види, визнаються як: захист публічних та приватних інтересів; стримування протиправної (або небажаної для держави) поведінки суб'єктів права; задоволення інтересів інших суб'єктів правовідносин; регулювання суспільних відносин у специфічних умовах; виявлення негативних правових наслідків

через учинення правопорушення; щодо деяких категорій осіб – встановлення обсягів права та свободи.

Натомість функції інституту правових обмежень у сфері інформаційної безпеки відображають динаміку правового регулювання, тобто функціонування цього інституту безпосередньо пов'язані з цілями та функціями правового регулювання в інформаційному просторі. Вони визначені як основні напрями впливу на суспільні відносини з метою оптимального регулювання, стримування протиправної (чи небажаної державі) поведінки суб'єктів права, захисту публічних інтересів, задоволення інтересів інших суб'єктів правовідносин.

До функцій інституту правових обмежень у сфері інформаційної безпеки належать:

- за характером та метою впливу: регулятивна (статична та динамічна), охоронна, що охоплює превентивну, право-відновлювальну, компенсаційну, каральну та виховну функції;

- у сфері суспільних відносин: економічна, політична, культурна, соціальна функції.

Право є одним із видів соціальної інформації, відповідно, весь механізм правового регулювання – це безперервна поява, рух, переробка соціальної інформації, що циркулює у двох потоках від суб'єкта соціального управління до об'єкта та навпаки.

О. М. Солодка пише, що можливість розгляду суб'єктів суспільних відносин в якості суб'єктів інформаційної сфери зумовлюється їх взаємодією з приводу інформації, причому зміст та обсяг їх прав визначається властивостями інформації, яка, таким чином, є основним елементом інформаційної сфери [200, с. 45].

Факторами, які впливають на інформаційний простір зсередини, є дійсний рівень демократичних відносин, рівень та структура інформаційного захисту від негативних впливів, наявність та чітке окреслення загального суспільного інтересу та об'єднання навколо нього, усвідомлення важливості й

значення системи духовно-ціннісних орієнтирів, ефективність державного управління, поточний стан, обсяги фінансування, підтримки і розвитку сфери науки та освіти, техніко-технологічна база, наявність або відсутність доступу до попередніх пластів наукових напрацювань.

Особливу роль в інформаційному просторі відіграють засоби масової інформацій. Характер і особливості процесу впливу ЗМІ в умовах зміни соціуму є важливою соціальною проблемою, яку має вирішити наука. Інформація, що розповсюджується засобами масової інформації сьогодні може призвести до виникнення небажаних соціальних ефектів, при цьому відбувається постійне удосконалення інформаційних технологій, що спрощують цей процес.

Роль засобів масової інформації проявляється у таких аспектах: проведення аналізу громадської думки визначення найбільш оптимального варіанта регулювання суспільних відносин; оприлюднення законодавчих ініціатив та опублікування прийнятих джерел права; публікація правової інформації, яка провокує виникнення, зміну та припинення правовідносин; формування правосвідомості.

Засоби масової інформації в сучасному цифровому світі є потужним каналом психологічного впливу на масову свідомість, виконують системоутворювальну роль у розвитку інформаційного суспільства. Закон України «Про друковані засоби масової інформації (пресу) в Україні» визначає дефініцію «засоби масової інформації» через перелічення видів засобів масової інформації, виділяє сутнісні ознаки останніх: постійна назва і періодичність поширення масової інформації [121].

В Україні офіційно зареєстровано 3143 друкованих видання сукупним тиражем 607,2 млн. примірників на рік. У соціологічній науці засоби масової інформації визначаються як «соціальні інститути» (преса, книжкові видавництва, агенції друку, радіо, телебачення), що забезпечують збирання, обробку та розповсюдження інформації в масовому масштабі [201].

Британський дослідник засобів масової інформації Д. Мак-Квейл

визначає ЗМІ (massmedia) як види засобів широкомасштабної комунікації, які певною мірою стосуються кожного мешканця, відносячи до них друковані видання, аудіовізуальні матеріали, радіо та телебачення [202, с. 95].

У науковій літературі є термін «засоби масової комунікації». Дискусія щодо співвідношення двох термінів не вщухає досі [203]. Але домінує думка про те, що засоби масової комунікації охоплюють як засоби інформації, так й інші засоби міжособистісного чи групового спілкування.

Але Д. Мак-Квейл наголошує на тому, що відбувається стирання кордонів між публічною та приватною комунікацією щодо дії фактора цифрової конвергенції, який значно посилився за останні десятиліття.

Засоби масової інформації як суб'єкти масової комунікації є потужними джерелами інформаційно-психологічного впливу на суспільство через масовість, повсюдну доступність і психологічну переконливість.

Багаторічні соціологічні дослідження, які проводяться в Україні Фондом О. Разумкова, Центром соціального моніторингу та іншими інститутами, ілюструють переконання домінування засобів масової інформації як джерела отримання новин про країну та світ [204; 205]. Незважаючи на певні проблеми довіри людей до засобів масової інформації щодо новин, вони залишаються абсолютними лідерами та значно перевищують за цим показником особисті канали комунікації. Поряд із традиційними засобами масової інформації дедалі більшу конкуренцію становлять «нові медіа», інтернет-сайти та соціальні медіа.

Необхідність вивчення тенденцій та особливостей правового регулювання медіасфери обумовлена проблематикою не лише наукового, а й практичного характеру: значним зростанням останніми роками кількості засобів масової інформації; розширенням медійного поля через посилення залучення аудиторії до створення медіа контенту, як наслідок, зростанням порушень у цій сфері. Тобто аудиторія стає активним учасником інформаційного поля. А оскільки аудиторія створює більше контенту, то виникає більше порушень у сфері інформаційної безпеки. Ця тенденція щороку посилюється.

Правові обмеження у сфері засобів масової інформації – не самоціль, вони мають на меті дотримуватися балансу інтересів особи, суспільства та держави. Ніхто не скасовує свободу слова як базову, фундаментальну цінність. Ніхто не сумнівається, що інформація – це суспільне благо. Але свобода не є вседозволеністю, а інформація тоді є благом, коли вона правдива, достовірна і не завдає шкоди. Жодна свобода не може бути виправданням пропаганди ненависті та насильства, посягання на територіальну цілісність України. Але відсутність належної відповідальності в деяких випадках може призвести до зловживання свободою інформації. Обмежувальна політика держави спрямована на недопущення цього.

Можна виділити дві різноспрямовані тенденції. Держава ліберально підходить до регулювання норм, що стосуються приватних аспектів життя громадян і відображення у медіасфері. Водночас законодавець постійно посилює обмеження щодо поширення серед громадян недостовірної та шкідливої інформації. Держава на законодавчому рівні вимагає оперативно виконувати рішення щодо видалення небажаної інформації та карає тих, хто таких рішень не виконує [206].

Для розробки методологічних аспектів правового регулювання забезпечення інформаційної безпеки в засобах масової інформації необхідне розуміння особливостей механізму психологічного впливу ЗМІ на аудиторію. Цьому присвячено розділ теорії масових комунікацій, що в науковій літературі отримав назву «ефект впливу засобів масової інформації» (massmediaeffects). Основними аспектами такого ефекту є вивчення викликаних впливом масової комунікації змін у свідомості та поведінці людини [207].

Аналіз тематичної літератури дозволив виділити основні характеристики механізму психологічного впливу мас-медіа на особистість та соціальні групи:

- вплив засобу масової інформації залежить від комплексу факторів: виду засобу масової інформації, змісту матеріалу, характеру аудиторії, умов сприйняття інформації, факторів соціального середовища, змісту контенту;

- аудиторія засобів масової інформації є активною при виборі та

споживанні інформації, що транслюється, може чинити опір засвоєнню думок і оцінок, які нав’язують;

- аудиторія засобів масової інформації дуже неоднорідна, сегментована на певні групи з різними орієнтаціями на певний вид засобу масової інформації, медіаконтенту та здібностями до засвоєння інформації;

- соціальний вплив засобів масової інформації охоплює три основні групи ефектів: когнітивні (вплив на погляди, думки, рішення, ціннісні орієнтації, соціальні уявлення), афективні (вплив на індивідуальні та групові емоції, почуття, настрої) та поведінкові (вплив на індивідуальну та колективну поведінку);

- вплив засобів масової інформації може проявлятися у визначенні предмета суспільної уваги, у змісті та характері суспільних поглядів та оцінок. Мас-медіа здатні успішно розвивати певну точку зору та блокувати альтернативні, сприяючи прогресу «спіралі умовчання» у суспільстві;

- одним з поширених ефектів засобів масової інформації є соціальне навчання моделей поведінки, що транслюються в мас-медіа, які в подальшому можуть відтворюватися в реальному житті;

- засоби масової інформації формують особливе символічне уявлення про реальність з набором образів, моделей сприйняття, ціннісних орієнтацій, норм поведінки, яке зумовлює спосіб мислення, почуттів та поведінки широкого загалу людей.

Таке детальне висвітлення базових теорій ефектів масової комунікації обумовлено необхідністю показати різноманіття підходів до опису механізму впливу засобу масової інформації на особу та соціальні групи, окреслити контури реального змісту.

Авторський досвід вивчення юридичної літератури, участі в науково-практичних конференціях та семінарах показав, що такого чіткого уявлення, за межами вузького кола профільних фахівців, нема [208; 209]. Спостерігаються крайні, полярні погляди, здебільшого «малюються» жахливі образи тотального впливу засобів масової інформації на безпорадну аудиторію або ж, навпаки,

максимально нівелюється вплив ЗМІ на свідомість людини.

Така полярність у поглядах проектується на сферу законотворчості, коли законодавці або взагалі відмовляються вживати заходів щодо захисту суспільства від деструктивного інформаційного впливу засобів масової інформації, посилаючись на недоведеність однозначного негативного характеру такого впливу, або, навпаки, пропонують законодавчі ініціативи у цій сфері, що не відповідають реальній суспільній небезпеці конкретної загрози інформаційній безпеці.

Механізм інформаційного впливу засобів масової інформації на особу, соціальні групи та суспільство має надзвичайно складний, багатоаспектний характер. Територіальний масштаб та кількісне охоплення впливом засобів масової інформації обумовлені комплексом факторів, охоплюючи вид засобу масової інформації, характер контенту, особливості цільової групи аудиторії, фактори зовнішнього мікро- та макросоціального середовища. Наслідком цього для нормотворчої діяльності є вимога максимальної гнучкості правового регулювання з обов'язковим урахуванням конкретної специфіки регламентованого аспекту забезпечення інформаційної безпеки у засобах масової інформації.

Базовим джерелом у сфері є Закони України «Про інформацію» і «Про інформаційні агентства», які декларують базовий конституційний принцип свободи масової інформації та розкривають нормативний зміст. В Україні обіг масової інформації, установи та право власності на засоби масової інформації не піддаються обмеженням. Нормативні акти містить застереження щодо винятків з посиланням на норми законодавства про засоби масової інформації [121-124].

Обмеження свободи масової інформації встановлюються законодавством. Як важлива юридична гарантія свободи масової інформації закріплена неприпустимість цензури. Під цензурою розуміється вимога попереднього узгодження матеріалів із боку державних органів та подальше накладення заборони поширення таких матеріалів. В Україні заборонено створення

спеціальних цензурних органів щодо засобів масової інформації.

Проте заборона цензури зовсім не означає неприпустимість обмеження щодо поширення масової інформації. На неї цілком поширюються загальні правила допустимості обмеження основних прав, встановлені Конституцією України. Важливе значення для забезпечення інформаційної безпеки у діяльності засобів масової інформації є неприпустимість зловживання свободою масової інформації. Нормативно визначено можливі форми зловживання:

- використання засобів масової інформації для скоєння злочинів, пропаганди (виправдання) тероризму, порнографії, жорсткості та насильства;

- застосування спеціальних методів деструктивного інформаційного впливу на підсвідомість людини;

- поширення відомостей про способи виготовлення наркотиків, вибухових речовин та вибухових пристроїв;

- розповсюдження персональних даних неповнолітніх потерпілих;

- розповсюдження іншої протиправної інформації.

До форм зловживання свободою масової інформації віднесено невиконання правил щодо поширення інформації забороненого характеру про діяльність терористичних організацій. Види інформації, поширення яких кваліфікується як зловживання свободою масової інформації, регулюються окремими законодавчими актами.

Окрема стаття Закону України «Про захист суспільної моралі» присвячена такій формі контенту, як еротичні видання, характерною ознакою яких є стимулювання та використання інтересу до сексу. Такі видання не віднесені до протиправних, але для них встановлені деякі обмеження, пов’язані із забороною радіо- та телетрансляції в денний час та спеціальними вимогами щодо роздрібного продажу.

На сьогодні спостерігається постійне збільшення потоку інформації, що вимірюється секундами. Однак якість поширюваного контенту, якою засоби масової інформації намагаються залучити нову або утримати стару аудиторію,

знижується. При цьому в умовах нестабільної економічної ситуації все більше ЗМІ переходять в електронний формат видання. Натомість, перед засобами масової інформації у мережі Інтернет особливо гостро постає проблема залучення надавачів реклами, інтерес яких прямо залежить від чисельності аудиторії каналу доставки інформації. В умовах постійної конкуренції інтернет-видання опинились перед необхідністю регулярного оновлення контенту, що, таким чином спровокувало скорочення часу на перевірку достовірності інформації. У редакціях невеликих регіональних засобів масової інформації з обмеженим штатом, не використовують час на перевірку інформації, яка тиражується на інших інформаційних ресурсах або у великих засобах масової інформації. Це призвело до того, що недостовірні новини стали проблемою медійного простору з постійною прив'язкою до швидкості інформаційного обігу.

Недостовірні новини розповсюджуються так швидко, що знайти першоджерело фактично неможливо. У результаті заходи впливу застосовуються до розповсюджувачів недобросовісної інформації, а не до її авторів. З метою правового регулювання такої проблематики публічна адміністрація може встановити об'єктом контрольних дій користувачів. Чим важче контролювати виробників інформації, тем вище вірогідність прямого впливу на її користувачів. Показником контрольних дій держави є інтенсивність правового обмеження.

Особливе значення мають новітні інформаційно-комунікаційні технології, оскільки дають публічній адміністрації можливість регулювання інформаційної сфери поза офіційними правовими санкціями. Це не завжди узгоджується з формальними нормами контрольної діяльності. Практика застосування органами публічної адміністрації заходів обмеження заслуговує особливої уваги.

Більшість сенсаційних подій у світі супроводжується інформаційним потоком даних, значна частина якого може демонструвати «підроблені новини», засновані на відомостях завідомо неправдивого характеру, що

навмисно спотворюють сприйняття дійсності.

Такий феномен ефективний в умовах інформаційного «голоду», коли політична еліта дає недостатньо інформації або запізнюється з офіційними коментарями щодо певної події. У цей момент «фейкові новини» заповнюють інформаційні «білими плямами» у свідомості людей недостовірною або спотвореною інформацією. Вірусним способом «фейкові новини» здатні протягом короткого терміну спровокувати громадський резонанс. Вирішення проблеми вимагає уваги до інших зон інформаційного поля, де контроль ускладнено, наприклад, угоди між користувачами та інтернет-операторами (провайдерами).

Як інструмент інформаційної війни «фейкові новини» представляють загрозу інформаційній безпеці. Необхідно розробити основні рекомендації щодо формування в Україні державної системи протидії розповсюдженню «фейкових новин» та їх впливу на суспільство, охоплюючи відповідні форми, методи та технології. Система дозволить у співробітництві зі структурами громадянського суспільства забезпечити захист особи та суспільства від деструктивного інформаційного впливу та обмежити канали розповсюдження недостовірної інформації.

Медіаповедінка учасників інформаційних процесів та сама логіка розвитку цих процесів приводять до висновку, що політика застосування адміністративних засобів обмеження держави у сфері засобів масової інформації активізуватиметься в умовах війни Російської Федерації з Україною. Можна констатувати дві тенденції реалізації державою регулювання медіасфери. Влада більш ліберально підходять до реалізації норм, які стосуються приватного життя та відображення у медіасфері. Посилюється регулювання в медійному полі інформації щодо недостовірної діяльності влади, забезпечується оперативне виконання рішень щодо видалення небажаної інформації та посилення покарання за невиконання таких рішень.

Журналістська спільнота має розвивати та посилювати інститути саморегулювання, запроваджувати в медіапростір редакційні стандарти, які

стали б реальним механізмом боротьби з недостовірними новинами, зловживанням свободою слова журналістами. Запровадження редакційних стандартів є важливим, оскільки за дотриманням положень стежать не представники правоохоронних чи наглядових органів, а працівники засобів масової інформації. Для кореспондентів та редакторів специфіка та особливості роботи в медіа більш зрозумілі, керівники редакцій зацікавлені не в покаранні порушника закону, а в профілактиці порушень. Відповідно, дотримання редакційних стандартів може запобігти не тільки проникненню в медіа фейків, але й загрозі появи самоцензури.

2.3. Правове регулювання забезпечення інформаційної безпеки в мережі Інтернет

Інформаційно-комунікаційна мережа Інтернет – це децентралізована глобальна система, яка поєднує на основі IP-протоколів різні пристрої. Структура мережі ніяк не прив’язана до кордонів держав і юрисдикцій. Вона з’єднує не тільки комп’ютери та мобільні телефони, але й інші засоби комунікації, здатні за IP-протоколом отримати доступ до мережі.

Інтернет (англ. internet від лат. лат. inter – між і англ. нет – мережа): всесвітня система взаємосполучених комп’ютерних мереж, побудована на використанні протоколу IP і маршрутизації пакетів даних. Інтернет утворює глобальний інформаційний простір, слугує фізичною основою для Всесвітньої павутини (World Wide Web, WWW) і великої кількості інших систем передачі даних [210].

Вивчення Інтернету дозволяє виділити матеріальні та нематеріальні види об’єктів правового та технічного регулювання. До перших відносяться технічні пристрої, що дозволяють абоненту отримати доступ до мережі, до другого – нематеріальні об’єкти, під якими розуміється інформація, що отримується та розповсюджується в мережі.

Необхідність регулювання мережі зі сторони держави має дві складові. З

одного боку, технічну систему, яка регулюється «Злагодою з основних питань», документованою в RFC. Request for comments (запити коментарів) – документи із серії пронумерованих інформаційних документів, що містять технічні специфікації та стандарти, які широко застосовуються в мережі Інтернет. Їхнє число наближається до чотирьох тисяч, і більшість цих документів має суто технічний характер [211].

З іншого боку, вміст і більшість процесів, що відбуваються в мережі, – це явище соціальне. Питання, пов'язані з регулюванням, вирішуються суспільством самостійно.

Інформаційно-комунікаційна мережа Інтернет є прикладом того, як при мінімальному державному регулюванні може ефективно розвиватися складна технічна система, ґрунтуючись переважно на встановлених правилах всередині мережі. Виникають питання, пов'язані з часом, який буде потрібний для розробки та застосування основ правового регулювання мережі, беручи до уваги рівень розвитку соціальних відносин у ній, наскільки ефективним буде це регулювання для розвитку технічної системи.

Т. В. Глуха визначає типи регуляторів правовідносин у мережі Інтернет: безпосередньо законом; технічними нормами, що регулюють доступ; соціальними та корпоративними нормами, що використовуються учасниками мережі; законами ринку та конкуренції, пов'язаними з наданням товарів і послуг [212, с. 162].

Виходячи з цього, норми, що регулюють поведінку учасників мережі, можна згрупувати: по-перше, це ділові звичаї (звичайне право), тобто практика, що склалася в результаті дій соціальних норм і правил відповідно до умов конкуренції; по-друге, це міжнародне право у зв'язку з тим, що мережа Інтернет має міжнародний характер згідно з технічними умовами свого існування, по-третє, це національне законодавство, оскільки умови існування мережі Інтернет у різних країнах мають правові особливості. Правове регулювання Інтернет-відносин – це комплексна проблема не тільки юридичної науки, а й практики [213, с. 152].

Регулювання мережі в країнах із англосаксонською системою права відбувається з допомогою судових прецедентів. Рішення, що ухвалюються, ґрунтуючись на чинних законах і традиційних нормах права, беручи до уваги відсутність прямого регулювання, підтверджувалися застосуванням до суперечливих питань немережевого законодавства, пов'язаних з мережею.

Нині пріоритетними галузями законодавчої діяльності є інформаційна безпека, захист персональних даних та інтелектуальної власності, регулювання електронної комерції та протидія кіберзлочинності. З огляду на багатогранність соціальних відносин, слід зазначити, що вони можуть регулюватися лише законодавством.

Технологічний розвиток змінює соціальну реальність набагато швидше, аніж законодавці можуть відреагувати на ці зміни. У процесі регулювання інформаційно-комунікаційної мережі Інтернет необхідно пам'ятати про небезпеку старіння правових норм. Оскільки законодавець не завжди встигає закріплювати норми, що регулюють відносини в Інтернеті через законодавчі акти, більшого значення набувають діловий звичай та мережевий етикет, на яких побудовано регулювання більшої частини відносин [214].

Використання самоврядування в інформаційно-комунікаційній мережі Інтернет потребує мінімального ступеня самоорганізації, інакше подібні організаційні механізми виконавчі органи влади будуть приймати та запроваджувати. Розглядаючи український сегмент мережі, слід зазначити розвиток елементів самоорганізації користувачів.

Сьогодні ознаки самоорганізації високого рівня вже існують. Наприклад, це Правила безпечної поведінки в Інтернеті, підготовлений Інтернет Асоціацією України [215; 216]. Цей документ сприятиме формуванню цивілізованого ринку інформаційних, комунікаційних та інтернет-технологій в Україні.

Документ покликаний «закрити» наявні прогалини в законодавстві, які створюють складнощі в правозастосовній діяльності та роботі судів під час вирішення суперечливих ситуацій. Механізм вирішення суперечок вирішується

з використанням ODR-платформ [217, с. 117].

Бажано, щоб аналогічні об’єднання були створені операторами доступу до мережі, постачальниками інформації, мережевими інформаційними агентствами, представленими в Інтернеті засобами масової інформації, правозахисними організаціями. Досі нормативне регулювання мережевих відносин не має спеціального правового характеру.

Крім численних регламентів і стандартів технічного характеру, до мережі Інтернет застосовні норми, які належать до звичайних корпоративних або навіть етичних відносин з відповідною специфікою. Це є історією виникнення та розвитку цієї мережі. Протягом багатьох років вона об’єднувала порівняно обмежене коло користувачів університетських дослідницьких центрів США. Їхні мережеві відносини характеризувалися високим ступенем довіри, повагою до думки співрозмовника, певними правилами ввічливості, використанням наукової термінології, добре відомої співрозмовникам, але мало зрозумілої нефахівцям.

З розвитком мережі Інтернет стихійно вироблені, не зафіксовані правила мережевого етикету (netiquette) ставали стандартом поведінки нових користувачів мережі [218]. Наразі ці правила можна знайти в Інтернеті в детальному викладі з коментарями. Не йдеться про їхнє примусове застосування. У кращому разі при відхиленні від зазначених правил інші користувачі не звернуть на це уваги або, навпаки, надішлють зауваження, у гіршому випадку порушник буде частково позбавлений можливості продовжувати спілкування з іншими користувачами.

Можна виділити два підходи до питань взаємодії права та мережі Інтернет: перший – за аналогією до конструкції теорії держави і права, можна назвати природно-мережевим; другий – нормативним [213]. Сенс природно-мережевого підходу у проголошенні принципової нерегульованості мережі. Вже існує декларація віртуального незалежного простору, етика, система одноголосного ухвалення рішень, відповідно, право тут марне, можливо, навіть шкідливе.

Нормативний підхід передбачає створення правових норм з метою впорядкування відносин, що складаються в Інтернеті. Тому прихильники цього підходу стверджують, що необхідно видати певну кількість актів, щоб врегулювати це питання, аби надалі ця проблема жодним чином не виходила з-під контролю організацій, держав та світової спільноти.

Що стосується природно-мережевого підходу, то нині він є найбільш популярним і полягає у підтримці та розвитку саморегулювання Інтернету. Саморегулювання передбачає наявність певних правил, які приймаються на основі загальної згоди між учасниками спільноти, соціальної групи, колективу.

Механізми контролю над дотриманням таких правил розробляються і застосовуються учасниками спільноти без залучення методів впливу «ззовні». Запровадження в таку динамічну та комплексну сферу, як мережа Інтернет, механізмів саморегулювання з урахуванням положень законодавства є пріоритетним.

У такій динамічній та комплексній сфері, як мережа Інтернет, та похідних мережевих технологіях запровадження в рамках чинного законодавства механізмів саморегулювання, що є запорукою реалізації вищезгаданих конституційних прав та свобод, є пріоритетним, оскільки ці механізми відповідають інтересам суб'єктів відповідних відносин, ліквідують частину наявних прогалин у сфері регулювання використання мережі Інтернет та сприяють оперативному розв'язанню конфліктів між організаціями, громадянами та державними органами у зв'язку з використанням інформаційних та комунікаційних технологій [219, с. 333].

Це повною мірою відповідає інтересам суб'єктів відповідних відносин, ліквідують частину наявних прогалин у сфері законодавчого регулювання використання мережі Інтернет та сприяють оперативному вирішенню конфліктів між юридичними та фізичними особами та державними органами у зв'язку з використанням мережі Інтернет.

З метою удосконалення законодавства треба виходити з того, що Інтернет є громадським середовищем, громадським простором, що використовують для

економічної діяльності та для збору інформації. Інтернет змінює наш простір, роблячи його віртуальним.

О. Г. Данильян та О. П. Дзьобань зазначають, що віртуальна реальність є результатом взаємодії об'єктивного й суб'єктивного, вона має статус випадкового буття, яке не фіксоване чи не вкорінене повністю у соціальному. Віртуальна реальність, сформована новими інформаційними технологіями, сприяла створенню мережевого суспільства, а існування кіберпростору є його основою, яка впливає на всі сфери суспільного життя [220, с. 19-20].

Але у віртуальному просторі мають діяти не віртуальні закони, а нормативні акти, яким підпорядковується реальний простір. Інформаційному суспільству необхідне правове закріплення основних елементів. Інтернет є базисом для розвитку й закріплення основних напрямів. Будь-яке втручання з боку держави у мережу сприймається інтернет-спільнотою як порушення її прав, оскільки сьогодні регулювання відбувається за допомогою громадського контролю.

Для того, щоб регулювати мережу, необхідно проаналізувати ті тенденції, які виникають в Інтернет-спільноті, закріплюючи аспекти, які вона визнала. Важливим елементом формування громадянського суспільства в Україні є прийняття законодавчого рішення на основі проведення об'єктивного аналізу ставлення населення до тих чи інших запроваджуваних нормативно-правових положень. Тому прийняття закону про Інтернет повинно базуватися на основі об'єктивних побажання співтовариства, на яке спрямовується воля законодавця.

Можливі такі перспективи розвитку регулювання мережі Інтернет: інформатизація суспільства призведе до збільшення та якісного покращення інтернет-аудиторії; подальше опрацювання та закріплення в законодавстві окремих норм функціонування мережі; вироблення мережевого етикету, ділових звичаїв регулювання відносин усередині мережі Інтернет; значне поширення практики судових суперечок щодо мережі Інтернет; створення закону про інформаційно-комунікаційну мережу Інтернет.

Відносини у межах мережі формуються значно швидше, ніж формування належної законодавчої бази. Регулювання відносин в Інтернеті ґрунтується на ділових звичаях. Висловлюючи волю учасників, ділові звичаї, які є у мережі Інтернет, регулюють їх поведінку. Встановлюючи певні правила, учасники передбачають можливість настання негативних наслідків, як-от: тимчасова чи постійна заборона доступу до мережного ресурсу.

Особливість таких мережевих звичаїв полягає в тому, що вони, ґрунтуючись на чинній законодавчій базі, мають час та простір дії, зафіксовані таким чином, що без повідомлення про їх прочитання учасник інтернет-спільноти не може потрапити на певний ресурс мережі.

У певних випадках мережеві звичаї входять у конфлікт із чинними нормами права. Пріоритетними є норми чинного законодавства. Ідеї саморегулювання відносин в Інтернеті, розвиваючись паралельно із законодавством, починають служити основним механізмом стимулювання розробки нормативно-правових актів у сфері правового регулювання відносин у мережі Інтернет.

Слід зазначити, що нині не потрібно створення нових структур у сфері розробки та впровадження ініціатив у сфері саморегулювання, необхідна активізація вже наявних організацій.

Доцільно, в перспективі, на державному рівні вводити інститут саморегулювальних організацій інформаційної сфери, основною метою яких буде забезпечення сумлінного регулювання діяльності в Інтернеті. Реалізація цього інституту буде неможливою без стимулювання та пропаганди державою у суспільстві саморегулювання мережевих відносин. Проблема екстериторіальності та глобальності мережі Інтернет, обумовлена поширеністю у світі та територіальною компетенцією окремих держав, має вирішуватись шляхом міжнародного співробітництва у даній галузі через уніфікацію законодавства про правове регулювання та функціонування мережі Інтернет різними країнами.

Розробка єдиних правил призведе до впорядкування та уніфікації взаємин

між суб'єктами мережевих відносин. Оскільки нині подібна уніфікація неможлива, питаннями регулювання Інтернету займуться законодавчі органи, що призведе до зближення національно-правових систем.

Сучасний стан законодавчої бази в українському сегменті мережі Інтернет та необхідність зміни та розвитку позначають три основні напрями розвитку національного законодавства у галузі регулювання відносин, що виникають у мережі Інтернет: розробка принципово нових законодавчих та інших нормативних актів, що беруть до уваги специфіку функціонування та розвиткок мережі; часткова трансформація наявної в Україні нормативно-правової бази для її пристосування до чинних правовідносин; створення (або роз'яснення) механізмів прямого використання стосовно Інтернету частини чинних законодавчих актів без зміни змісту; адаптація нормативної бази до вимог директив і стандартів Європейського Союзу, яка охоплює усі три напрями.

З розвитком комп'ютерних технологій та інформаційно-комунікаційної мережі Інтернет виникає нове покоління мас-медіа, узагальнено іменованих «новими медіа» (newmedia). До них належать Інтернет-ресурси, мультимедійні матеріали, комп'ютерні ігри, цифрові аудіовізуальні матеріали, віртуальну реальність, цифрові інтерфейси «людина – комп'ютер».

З. В. Григорова, О. А. Сухорукова, А. В. Кваско та Л. П. Шендерівська виокремили основні засади нових медіа: цифрова репрезентація; модульність; автоматизація; варіативність; транскодінг. Основними ознаками, що відрізняють нові медіа від традиційних, є:

- дігітальність – цифровий характер контенту;

- інтерактивність – наявність зворотного зв'язку, можливість користувача одночасно бути автором і споживачем контенту;

- персоналізація інформації – автоматична фільтрація контенту, що відображається відповідно до інтересів певного користувача;

- гнучкість форми, змісту і використання – цифрові технології дають можливість транслювати і об'єднувати різні види інформації – текст, аудіо,

зображення і відео, розміщувати їх на різних платформах;

- потоковість споживання контенту і необмеженість у його обсягах, просторі, формі комунікації;

- можливість редагувати і вилучати інформацію після розміщення; оперативність надання і оновлення інформації – інформація може передаватися в режимі реального часу або оновлюватися в будь-який час за потреби;

- відсутність цензури і модерації [221, с. 138-139].

Ключову роль серед нових медіа відіграють численні інтернет-ресурси. У юридичному плані мережа Інтернет є каналом поширення масової інформації, але засобом масової інформації вона не є. Під останню категорію підпадають лише мережеві видання.

В еволюції інтернет-технологій масової комунікації прийнято виділяти два основні покоління. Перше покоління вебтехнологій (Web 1.0) було спрямоване на передачу та розповсюдження інформації. Основним типом інтернет-ресурсів були інтернет-сайти.

У 2021 році у світі налічувалося понад 127 млн. веб-сайтів [222]. Друге покоління вебтехнологій (Web 2.0) має на меті забезпечення інтерактивної комунікації інтернет-користувачів за допомогою соціальних мережевих ресурсів. Завдяки їм різко зросла інтенсивність спілкування та взаємодії людей. Технології Web 2.0 сприяли зростанню популярності Інтернету.

Закон України «Про авторське право і суміжні права» визначає веб-сайт у мережі Інтернет як сукупність даних, електронної (цифрової) інформації, інших об’єктів авторського права і (або) суміжних прав тощо, пов’язаних між собою і структурованих у межах адреси вебсайту і (або) облікового запису власника цього веб-сайту, доступ до яких здійснюється через адресу мережі Інтернет, що може складатися з доменного імені, записів про каталоги або виклики і (або) числової адреси за інтернет-протоколом [223].

В Україні динамічно розвивається сектор інформації, комунікацій та інформаційних технологій. Усі види засобів масової інформації значною мірою доступні для більшості українців, хоча регіональні та місцеві розподілені

нерівномірно по всій країні.

За даними dataportel.com станом, на січень 2021 року: населення України становить 43,60 млн. осіб. 69,7% населення проживає в міських центрах і 30,3% – у сільській місцевості. Кількість користувачів Інтернету становить 29,47 мільйона, рівень проникнення в Інтернет становить 67,6%. Кількість користувачів соціальних мереж становить 25,70 мільйона, що еквівалентно 58,9% від загальної кількості населення [201, с. 11].

Мобільні пристрої є головним способом для виходу в Інтернет серед громадян різного віку. Дослідники все частіше говорять про підключення, яке відповідає високому рівню активності користувача та максимальним показникам «екранного часу», проведеного у смартфоні, комп'ютері або планшеті.

Ключову роль у розвитку Web 2.0 відіграли соціальні мережі (socialnetworksservices) – інтерактивні вебплатформи, призначені для спілкування користувачів і розміщення контенту.

Найбільш популярною соціальною мережею у світі є Facebook (2,9 млрд. користувачів), друге місце посідає YouTube (2 млрд. користувачів). В Україні трійку лідерів серед соціальних мереж складають мережа Facebook, Instagram і YouTube [224].

Крім соціальних мереж як основного каналу інтернет-комунікації, у другому десятилітті XXI століття широкого розвитку набули Інтернет месенджери (Instant messaging) – програми для миттєвого обміну повідомленнями через Інтернет. Найпопулярнішим серед них в Україні є Telegram, Viber та інші месенджери [224]. Вони стали значним каналом поширення контенту та комунікації.

Наслідком розвитку технологій Web 2.0 є те, що інтернет-ресурси на відміну від традиційних засобів масової інформації, є джерелом не тільки контентних, а й комунікаційних загроз інформаційній безпеці. Небезпекою для інтернет-користувачів є не тільки інформація, яка розповсюджується в мережі, а й деструктивна комунікація між користувачами.

Ю. В. Половинчак підкреслює, що за численних перевах Інтернету і можливостях, що надаються, мережа несе небезпеки, пов’язані з деструктивною комунікацією між людьми. По-перше, відбувається збільшення розриву між активними та пасивними індивідами через нерівномірність доступу до інформаційних технологій. По-друге, індивідуалістичний характер цифрових технологій може бути небезпечним для громадянського суспільства через можливе ослаблення і розмивання колективних дій та зв’язків усередині реальної спільноти, через декларативно-віртуальну участь у громадському житті тощо. По-третє, непрофесійний характер масових комунікацій у соціальних медіа може призводити до профанації обговорюваних проблем як умисної, так і неумисної, наслідком чого є викривлення інформації та некоректне формування громадської думки [225, с. 189-190].

Соціологічні дослідження показують, що нові медіа в особі Інтернет-сайтів, соціальних мереж, месенджерів і вебдодатків витісняють традиційні засоби масової інформації щодо часу споживання та впливу. Ця тенденція продовжиться, а тому нові медіа стають основними джерелами інформаційного впливу на суспільство, а отже, основними джерелами загроз інформаційній безпеці. Цьому також сприяють деякі ознаки нових медіа.

На основі аналізу наукової літератури та власних досліджень виділено ключові характеристики інтернет-ресурсів, які мають значення у контексті правового регулювання забезпечення інформаційної безпеки:

1. Транскордонність та глобальний характер. Інтернет є глобальною інформаційно-комунікаційною мережею, що забезпечує транскордонний миттєвий доступ до інформації, що зберігається у будь-якій точці земної кулі. Це викликає складнощі щодо національного правового регулювання та здійснення державного управління у сфері інтернет-відносин, розширює географію джерел інформаційних загроз та ускладнює можливості нейтралізації.

2. Чинник відносної анонімності віртуального спілкування. Реєстрація громадян у соціальних мережах та інших інтерактивних ресурсах переважно

здійснюється самостійно за обмеженої верифікації зазначених персональних даних. Це створює можливість використання фейкових облікових записів. ІТ-компанії та спецслужби мають інструментарій, що дозволяє у низці випадків встановити особистість власника або користувача інтернет-ресурсу. Для більшості користувачів спеціальні засоби приховування справжньої особи недоступні через складність. Незалежно від об'єктивної наявності анонімності, її суб'єктивне сприйняття користувачем сприяє формуванню мережевої активності та прояву її деструктивних форм.

3. Надання можливості розміщення контенту користувачам. Це означає наявність у користувачів соціальних мереж та інших інтернет-ресурсів можливості самостійного розповсюдження контенту на масову аудиторію. У цьому полягає головна відмінність нових медіа від традиційних засобів. Традиційна схема односпрямованої трансляції відомостей від засобу масової інформації до аудиторії трансформується на нову модель транзактної медійної комунікації, у якій кожна людина стає потенційним джерелом масової інформації. Контент, що генерується користувачами, складає основну частину інформації в глобальній мережі. Цей тренд з кожним роком посилюється. Такий фактор означає мультиплікативне зростання кількості джерел інформаційних загроз. Щодо правового регулювання, то є складність здійснення контролю за контентом, що розміщується, через велику кількість авторів.

4. Надання інформації на запит користувача. На противагу колишнім аудіовізуальним засобам масової інформації, що передбачають централізовану модель мовлення, коли межі розсуду аудиторії обмежуються єдиним інформаційним розкладом, Інтернет дає користувачам свободу вибору інформації, причому у глобальному масштабі. Разом з трансфертом селекції від редакції засобів до самого користувача частково відбувається перенесення відповідальності за результати. У соціальних мережах ключову роль у вибудовуванні інформаційної стрічки для користувача відіграють рекомендаційні алгоритми, що працюють за непрозорою схемою.

5. Важлива роль пошукових систем. Ці системи забезпечують

відшукування необхідної інформації серед гігантського масиву даних. Найбільш відомими є Google, Bing, DuckDuckGo, Yahoo [226]. Змінюючи порядок відображення інформації в результатах пошукової видачі можна проводити перегляд контенту. Цей фактор береться до уваги при забезпеченні інформаційної безпеки. Однак роль пошукових систем знижується внаслідок підвищення ролі соціальних мереж та зростання кількості мобільних додатків.

Пошукова система здійснює за запитом користувача пошук у мережі Інтернет інформації певного змісту та надає користувачеві відомості про покажчик сторінки вебсайту для доступу до інформації, що запитується, розташованої на вебсайтах, що належать іншим особам.

Механізми інформаційного впливу масової комунікації прийнятні до нових медіа та передбачають вивчення механізмів соціально-психологічного впливу у галузі психології, соціології та теорія комунікацій.

Суспільні відносини, пов’язані з використанням Інтернету, є предметом правового регулювання різних галузей права. Інформаційне право в даному аспекті відіграє ключову роль.

Беручи до уваги відсутність окремого закону про Інтернет, регулювальні правові норми знаходять відбиток у Законі України «Про захист інформації в інформаційно-комунікаційних системах» та в Законі України «Про електронні комунікації». Слід зважати на поширення дії загальних принципів права та норм інших правових актів, не присвячених спеціально Інтернету, але застосовних до інтернет-відносин з урахуванням специфіки.

Проблеми поширення деструктивного інформаційного впливу в мережі Інтернет та захисту суспільної моралі були одним із чинників щодо розширення сфери правового регулювання Інтернет-відносин. У практичному плані це виявилося у закріпленні у Законах України «Про захист суспільної моралі» та «Про санкції» [50;159].

Надалі законодавець запроваджує нові механізми обмеження доступу до протиправного контенту. В основному йшлося про контент, що чинить негативний інформаційний вплив, хоча траплялися й приклади протиправної

інформації іншого виду. У більшості випадків процедура обмеження доступу до інформації передбачає ініціативне реагування на виявлений протиправний контент державних органів та направлення інформації до відповідних структур.

Законодавством передбачено переважно позасудовий порядок обмеження доступу до протиправної інформації, коли рішення про блокування ухвалюються органами виконавчої влади (Національна поліція, Міністерство культури і інформаційної політики, Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації України) чи Радою національної безпеки і оборони України.

У судовому порядку ухвалюється рішення про визнання забороненою для розповсюдження будь-якої іншої інформації, передбаченої нормами Кримінального кодексу України та Кодексу України про адміністративні правопорушення.

Т. В. Авдєєва у дослідженні «Відповідність блокування соціальних мереж європейським стандартам свободи вираження поглядів» пише, що національне законодавство має чітко передбачати можливість блокування вебсайтів на певний період часу, забезпечуючи застосування такого заходу виключно за рішенням суду. Окрім наявності підстави для обмеження в національному законодавстві, держави повинні забезпечити процесуальні гарантії та гарантії проти зловживань. Запроваджуючи обмеження, держави повинні звернути увагу на те, що обґрунтування цільового та масового блокування соціальних мереж не може бути однаковим для цілей оцінки законної мети. ЄСПЛ не перейшов до оцінки критерію необхідності, тому комплексний підхід розроблений не був, проте ця вимога була частково врахована в національних юрисдикціях та практиці Суду справедливості ЄС. Необхідність вимагає більш складного та всебічного балансування інтересів, врахування обсягу та тривалості обмеження, а також готовності платформи до співпраці, ефективності наявних альтернатив та впливу застосованих заходів на функціонування сервісу [227].

Особливістю функціонування механізмів обмеження доступу до

інформації є те, що за схожістю роботи (механізм позасудового та судового обмеження) законодавцем встановлені різні процедури блокування.

Під процесуальним провадженням в юридичній діяльності пропонується розуміти встановлений процесуальним законом порядок здійснення юридичної діяльності, а також комплекс процедурно-процесуальних дій та операцій спеціально уповноважених суб'єктів та інших учасників процесуального провадження, спрямований на розгляд та вирішення юридичних справ з метою досягнення соціально значущих результатів. Системою видів процесуальних проваджень охоплюються дві групи, як-от: юрисдикційні; не юрисдикційні (позитивні).

До першої групи належать: конституційне процесуальне провадження; кримінальне процесуальне провадження; цивільне процесуальне провадження; господарське процесуальне провадження; адміністративне провадження; виконавче виробництво. До другої групи входять: контрольне провадження; наглядове провадження; податкове провадження; установче провадження; виборче провадження та низка інших.

Важливими напрямами (умовами) оптимізації процесуальних проваджень з метою підвищення ефективності є вдосконалення нормативно-правової бази, що регламентує юридичну процедуру здійснення всіх різновидів процесуальних проваджень у юридичній діяльності, точне та неухильне, відповідно до закону виконання процесуальних дій суб'єктами та учасниками процесуального провадження виключно на основі всіх принципів здійснення такого.

Потрібно брати до уваги рівень професійного професіоналізму суб'єктного складу процесуальних проваджень. Оптимальне процесуальне законодавство, процесуальні дії, засоби, способи та умови реалізації поставлених завдань тоді будуть ефективними, коли буде забезпечено процесуально правильне, законне та обґрунтоване на належному професійному рівні їх здійснення.

Детально розглядати кожен такий алгоритм ми не будемо, виділимо лише

спільні риси та позначимо ключові відмінності. Спільним для всіх механізмів є організація взаємодії між органом, який ініціює процедуру обмеження доступу, та Державною службою спеціального зв'язку та захисту інформації України, а також учасниками в ланцюжку Державна служба спеціального зв'язку та захисту інформації України – оператор хостингу – власник інформаційного ресурсу – оператор електронної комунікації.

Тобто після звернення компетентного органу або прийнятого рішення Державна служба спеціального зв'язку та захисту інформації України починає взаємодіяти з інформаційними посередниками, насамперед з оператором хостингу та оператором електронних комунікацій.

Статистика щодо обмеження доступу до інформації відображає показники блокувань на рівні операторів електронних комунікацій. Тоді як не менш значущими є перші два етапи роботи алгоритму, перший передбачає фізичне видалення шкідливого контенту з інформаційного ресурсу, а другий – блокування лише на рівні хостингу.

Обидва чинники методу дозволяють повністю вимкнути доступ до негативної інформації, тоді як блокування на рівні оператора електронних комунікацій – лише частково. Вона може бути подолана через використання анонімайзерів та інших інструментів [228].

Основна відмінність у механізмах обмеження доступу до інформації від блокування полягає у тому, що при застосованні блокування на рівні операторів електронних комунікацій всі попредні кроки користувача не дають результату, встановлюється попереджувальне блокування ресурсу оператором електронних комунікацій, після чого розпчинається взаємодія з оператором хостингу та власником ресурсу.

Слід зазначити, що тривалий час проблемою залишалося обмеження доступу до протиправного контенту соціальних мереж. Це пов'язано з тим, що передбачені механізми блокування важко застосувати до окремих сторінок соціальних мереж, не поставивши під загрозу блокування всього ресурсу. У зв'язку з цим видалення контенту або обмеження доступу забезпечувалося

через взаємодію державних органів та адміністрації соціальних мереж.

Інтернет є принципово відмінним від традиційного політичного комунікаційного простору, у якому використання традиційних офлайн-технологій масової комунікації значно менш ефективне стосовно можливостей політичного управління за умов інформаційного суспільства. Результати застосування класичних моделей комунікації в інтернет-просторі відрізняються від результатів застосування такого роду моделей у традиційному медіапросторі. Йдеться про принципово нові ефекти, які породжують необхідність перегляду наявних та розробки нових концептуальних парадигм та моделей масової політичної комунікації.

Сучасне політичне управління здійснюється за допомогою використання комунікаційних інструментів, що забезпечують формування та трансляцію смислів, символів та цінностей у суспільну свідомість. Щодо інтернет-простору такого роду комунікаційні інструменти мають яскраво виражену специфіку. Вони відрізняються від класичних інструментів комунікації мультимедійністю, екстериторіальністю, високим рівнем довіри до горизонтальних комунікацій, наявністю можливостей широкомасштабного застосування віртуальних симулякрів, падінням значення безпосередньо контенту повідомлень і зростанням значущості оцінок користувача контенту.

В інтернет-просторі формуються принципово нові форми впливу на суспільну свідомість. Вони засновані на моделях залучення мережевих користувачів до розподіленої комунікаційної взаємодії з подальшим формуванням мережевих співтовариств, що існують як нові громадські інститути.

Поняття маси в інтернет-просторі стосовно можливостей та особливостей комунікативного впливу у межах політичного управління набуває принципово нового звучання завдяки структуризації мережевих спільнот. Йдеться про появу ефекту «розумного натовпу», пов’язаним з використанням багатофункціональних високотехнологічних гаджетів, створенням нового феномену «віртуальної маси», що відрізняється наявністю в мережевих

спільнотах значної кількості віртуальних лідерів громадської думки [229].

Розвиток інтернет-технологій масової політичної комунікації створює нові соціально-політичні ефекти. Ці ефекти раніше не існували в традиційному публічному політичному просторі і безпосередньо пов'язані з мобілізаційними можливостями соціальних медіа. Йдеться про ставлення до представників громадянського суспільства, інтерактивну взаємодію між представниками суспільства та влади, організацію структурованого тиску на владу мережевих спільнот, радикалізацію настроїв інтернет-користувачів, перенесення на мережеві спільноти частини функцій традиційних соціально-політичних інститутів.

Сьогодні уявлення про Інтернет як відкритий простір політичних комунікацій, що має потенціал демократизації суспільства, потребує перегляду. Різноспрямовані тенденції глобалізації та універсалізації інтернет-простору та фрагментація закритість окремих мережевих сегментів, які в перспективі можуть змінити наявний комунікативний простір, призводять до необхідності переосмислення чинних концепцій та моделей комунікаційної діяльності в управлінні.

Інтернет-простір характеризується значно більшим деструктивним та пропагандистським потенціалом у порівнянні з традиційним простором публічних комунікацій. Інтернет-ресурси та технології трансформуються з прозорого та незалежного інструменту демократизації суспільства на інструмент формування спотвореної віртуальної псевдореальності.

Нині значну роль в інформаційно-комунікаційному впливі в Інтернеті відіграють симулякри – віртуальні псевдоособистості, що функціонують в мережевому просторі, які симулюють репрезентацію реальних Інтернет-користувачів, забезпечуючи трансляцію пропагандистського контенту для здійснення деструктивного впливу. Це зумовлює віртуалізацію Інтернет-простору та викликає суттєві спотворення у відображенні політичної реальності.

Вищезазначене актуалізує проблему національної інформаційної безпеки

щодо політичної стабільності на поточному етапі суспільно-політичного розвитку в умовах війни Російської Федерації з Україною. Канали інтернет-комунікації використовуються для віртуального перекодування ціннісно-смислового простору України. Йдеться про підрив стабільності чинного національного режиму із подальшим впровадженням у суспільну свідомість проросійської моделі поведінки. Кіберполіція опублікувала список сторінок, які користувач може заблокувати [230].

Одним із наслідків нових викликів у сфері інформаційної безпеки тоталітарних держав є тенденція фрагментації наявного мережного простору масових комунікацій. Йдеться про формування специфічних і відокремлених національних сегментів Інтернету. Це дозволяє здійснювати політичне управління у межах держави та блокувати інформацію зовні.

О. Е. Радутний зазначає, що держава, яка не є технологічним або економічним лідером, крім заходів щодо охорони суверенітету та національної безпеки, має не припиняти зусиль щодо захисту власного інформаційного суверенітету, у тому числі конкретним способом підтримувати національну освіту та науку, вітчизняного виробника програмного забезпечення та технологічного обладнання, запровадити постійне навчання та тренування на рівні кожної особи як найменшої одиниці суспільства та народу, дієво заохочувати до саморозвитку, сформулювати об’єднавчу національну ідею, здійснювати заходи щодо збереження та розвитку досвіду і традицій (як горизонтально – створення нових інформаційних масивів, так і вертикально – передача знань від одних поколінь до інших, як передбачено преамбулою Конституції України («усвідомлюючи відповідальність перед Богом, власною совістю, попередніми, нинішнім та прийдешніми поколіннями»), популяризувати зразки бажаної поведінки, підтримувати позбавлення відчуття меншовартості у порівнянні з іншими країнами або спільнотами, які нещодавно були такі самі тощо [231, с. 35-36].

Розглянувши правове регулювання забезпечення інформаційної безпеки в мережі Інтернет, робимо висновки.

Правове забезпечення інформаційної безпеки в мережі Інтернет передбачає комплексне та гнучке використання різних моделей правового регулювання відносин в аналізованій сфері, охоплюючи державне регулювання та саморегулювання. Пріоритет у правовому регулюванні має бути за державою. Галузеве саморегулювання має доповнювати законодавче, щоб запобігти надмірному втручанню держави в діяльність суб'єктів інтернет-індустрії. При гарантуванні свободи вираження поглядів та масової інформації застосовуються обмеження прав та інші правові заходи, спрямовані на забезпечення інформаційної безпеки громадян. Інструментарій, що застосовується, досить універсальний, охоплює регламентацію статусу розповсюджувачів інформації в Інтернеті, встановлення правових заборон і обмежень на поширення контенту та комунікацію користувачів, моніторинг інтернет-активності, застосування блокування Інтернет-ресурсів, притягнення до відповідальності конкретних користувачів. Правові підстави, процесуальний порядок та гарантії дотримання прав громадян при застосуванні таких заходів, відповідно до правової позиції Європейського Суду з прав людини, мають бути визначені на законодавчому рівні з урахування гарантів дотримання прав людини та недопущення зловживань посадових осіб органів, які здійснюють інформаційні обмеження.

Пріоритетним рівнем правового регулювання забезпечення інформаційної безпеки має бути національний рівень, що передбачає законодавчу регламентацію мети, завдань і напрямів забезпечення інформаційної безпеки, а також системи забезпечення інформаційної безпеки та правового статусу складових її суб'єктів, форм, методів і засобів діяльності.

2.4. Юридична відповідальність у сфері забезпечення інформаційної безпеки

При формуванні інформаційного суспільства одним із принципів є верховенство права, а відповідно, актуальними є питання юридичної

відповідальності за правопорушення в інформаційній сфері. Уся система правового регулювання відносин інформаційної сфери націлена на забезпечення ефективності відносин, зміцнення гарантій дотримання прав суб'єктів правовідносин.

На сучасному етапі до правових засобів забезпечення інформаційної безпеки України слід віднести необхідність підготовки та прийняття нових нормативно-правових актів, уточнення наявних концептуальних і доктринальних документів, які повинні адекватно відображали національні інтереси України, у тому числі в інформаційній сфері, та сприяти реалізації завдань забезпечення інформаційної безпеки у контексті динаміки загроз інформаційній безпеці країни.

Це комплексне завдання, яке повинно бути реалізовано в межах різних інститутів права. Поряд з іншими інститутами права особливе місце у механізмі правового забезпечення інформаційної безпеки має зайняти юридична відповідальність. Це важливо для формування державної політики у цьому стратегічному напрямі та національної системи заходів забезпечення інформаційної безпеки, що охоплює системи державного обліку та реєстрації інформаційних систем та ресурсів.

Значний внесок у дослідження юридичної відповідальності у системі правового забезпечення інформаційної безпеки в Україні зробили вчені: І. В. Арістова, О. А. Баранов, К. І. Бєляков, О. П. Дзьобань, О. А. Заярний, М. В. Карчевський, В. К. Колпаков, О. В. Кохановська, Н. Б. Новицька, А. М. Новицький, Н. А. Савінова, О. О. Тихомиров, І. М. Шопіна та інші [232-237].

Сьогодні важливо забезпечити інформаційну безпеку державних інформаційних ресурсів, інформаційних систем, критичну інформаційну інфраструктуру та її об'єкти.

Забезпечення інформаційної безпеки особи, суспільства та держави, а також національної безпеки Україні торкається питання інформаційної безпеки, забезпечення захисту персональних даних, недоторканості приватного життя,

розширення застосування безпечних інформаційних і цифрових технологій у системі державного управління та у соціальній сфері – освіті, охороні здоров'я, наданні адміністративних послуг, у соціальній сфері.

В умовах трансформації, що відбувається в суспільстві та у правовій системі при переході у цифрову епоху, питання щодо забезпечення інформаційної безпеки потребують системного правового регулювання, зважаючи на наявний досвід держав Європейського Союзу, правозастосовну практику, що формується.

Спільними пріоритетами можна вважати політику підтримки стратегії інформаційної безпеки Європейським Союзом і Північноатлантичним альянсом (НАТО), що стосується інформаційного тероризму, кібератак, зовнішніх інформаційних впливів деструктивного характеру. Ініціативи щодо вирішення проблем інформаційної та кібербезпеки Європейського Союзу полягають у поглибленні координації дій наднаціональних і національних інститутів та у виробленні спільних підходів до протидії інформаційним загрозам [238, с. 96].

Виявлені у ході дисертаційного дослідження проблеми, пов'язані із забезпеченням інформаційної безпеки, не є вичерпними, оскільки саме поняття забезпечення інформаційної безпеки різноманітне, розвивається в умовах переходу до цифрової економіки, що пронизує всі сторони життя.

Нові суб'єкти та об'єкти інформаційної сфери формально не закріплені у законодавстві, а фактично існують та застосовуються на практиці, що потребує розвитку стратегічних і програмних документів та інформаційного законодавства.

Інформаційна безпека, як і національна безпека, визначається європейською та національною доктриною через розвиток [239].

Одним із важливих напрямів досліджень щодо такого підходу є нові тренди національної політики забезпечення інформаційної безпеки та зміщення у бік комплексного використання різних прийомів та засобів мирного врегулювання суперечок та конфліктів, інструментарію співпраці. Зазначене знайшло відображення у Стратегії інформаційної безпеки України.

На національному рівні важливо забезпечити систему ефективного правового забезпечення. Стан захищеності не є в сучасних умовах статичний, потребує постійного вдосконалення. Варто розглядати поняття «інформаційна безпека», як це пропонує Стратегія інформаційної безпеки України, тобто комплексно [58].

О. І. Остапекно і О. В. Баїк вказують, що, аналізуючи сутність і значення інформаційної безпеки особи, суспільства і держави, варто зазначити, що кожен із наявних видів інформаційної безпеки має відповідну юридичну оцінку інформаційних загроз, що дозволяє вести мову про: адміністративно-санкціоноване забезпечення інформаційної безпеки; адміністративно-юрисдикційне забезпечення інформаційної безпеки; адміністративно-казуальне забезпечення інформаційної безпеки.

Адміністративно-юрисдикційне забезпечення інформаційної безпеки визначається як врегульований процесуальними нормами адміністративного права стан захищеності конституційних та інших інтересів особи, суспільства і держави, порядок провадження в справах про адміністративні правопорушення та визначення міри адміністративної відповідальності за вчинене правопорушення [240, с. 174].

Одним із важливих механізмів правового забезпечення інформаційної безпеки є заходи юридичної відповідальності за вчинення правопорушень у галузі, що розглядається. За допомогою заходів державно-примусового впливу гарантується реалізація правових норм, що регламентують підтримку стану захищеності особи, соціальних груп і суспільства від деструктивного інформаційного впливу. Юридичну відповідальність визначають як застосування заходів державного примусу до правопорушників для відновлення порушеного правопорядку та покарання особи, яка вчинила правопорушення. Вона є основним способом реалізації регулятивно-охоронної функції права, змістом якої є попередження.

С. В. Пєтков підкреслює, що відповідальність – правова та державно-адміністративна категорія, що відображає ціннісно-правовий аспект суспільних

відносин, які побудовано за принципом «людина – суспільство – держава» [241, с. 120]. Інститут відповідальності є загальним правовим інститутом, але щодо сфери інформаційних правовідносин він базується на спеціальних методах та засобах Це система норм і процедур, що реалізуються з метою припинення правопорушень, встановлення виду, форми та заходів покарання за скоєні та доведені кримінальні чи інші правопорушення з урахуванням соціальної шкоди та вини правопорушника.

З погляду на дослідження О. С. Бакумова, інститут юридичної відповідальності за правопорушення у сфері інформаційної безпеки має міжгалузевий характер і складну внутрішню структуру, що охоплює адміністративно-правові, цивільно-правові, кримінально-правові елементи та взаємозв'язки між ними, і перебуває в динамічному розвитку. Взаємопов'язаними вимірами правового регулювання юридичної відповідальності у сфері інформаційної безпеки є ціннісний, нормативно-правовий, функціональний та інституційний [242, с. 28].

Ціннісний вимір правового регулювання юридичної відповідальності вказує, що інформаційна безпека перебуває в системних зв'язках із конституційними цінностями та сприяє забезпеченню суспільно корисної мети – гарантії захищеності прав, свобод, законних інтересів людини в інформаційному просторі.

Нормативно-правовий вимір означає фіксацію принципів юридичної відповідальності у сфері інформаційної безпеки, основних видів, підстав і особливостей застосування юридичної відповідальності.

Функціональний вимір вказує на те, що нормативне закріплення відповідальності у сфері інформаційної безпеки забезпечує реалізацію низки суспільно важливих функцій відповідальності – правоохоронної, каральної, правовиховної, поновлення права.

В інституційному вимірі юридична відповідальність за правопорушення у сфері інформаційної безпеки означає створення певного механізму, що охоплює сукупність інституцій, основу якого складає адміністративно-

правовий механізм, які здатні притягнути фізичну і юридичну особу до юридичної відповідальності у межах, визначених законом, з метою покарання за вчинені протиправні діяння щодо зловживання.

Основне значення для визначення юридичної відповідальності в інформаційній сфері має ст. 27 «Відповідальність за порушення законодавства про інформацію» Закону України «Про інформацію». Відповідно до цієї статті, порушення вимог закону тягне дисциплінарну, цивільно-правову, адміністративну чи кримінальну відповідальність згідно із законодавством України [37]. Законом України «Про інформацію» встановлено чотири види юридичної відповідальності. Хоча галузь інформаційного законодавства не вичерпується одним Законом України «Про інформацію», це правило поширюється на систему інформаційного законодавства.

З огляду на специфіку правових відносин у сфері забезпечення інформаційної безпеки, які виражають переважно громадські інтереси, основну роль у механізмі правової охорони відіграють норми кримінального й адміністративно-деліктного законодавства. В умовах активного розвитку інформаційного суспільства саме цифрове середовище є одним із ключових драйверів змін та доповнень Кримінального кодексу України та Кодексу України про адміністративні правопорушення.

Інформаційна безпека, з одного боку, є частиною національної безпеки, а з іншого боку, є відносно самостійним видом безпеки, що має системний характер. В Україні нема кримінальної політики у сфері протидії злочинам проти інформаційної безпеки. Чинне кримінальне законодавство вже вичерпало свій профілактичний і каральний потенціал у цій сфері.

Норми перебувають у різних розділах Особливої частини Кримінального кодексу України, створені задля забезпечення інформаційної безпеки, позбавлені інституційних зв’язків, мають суттєві юридично-технічні відмінності, тому навряд чи можуть бути здатними ефективно реагувати на реалії, що стрімко змінюються. Тому сьогодні одним із актуальних питань у науці кримінального права є дослідження проблеми кримінально-правової

охорони інформаційної безпеки.

Злочинами проти інформаційної безпеки слід вважати винно вчинені суспільно небезпечні діяння, які посягають на суспільні відносини, що забезпечують реалізацію інтересів особи, суспільства та держави в інформаційній сфері.

Кримінальна відповідальність встановлюється за скоєння злочинів у сфері інформаційної безпеки, тобто суспільно небезпечних діянь з надання деструктивного інформаційного впливу, заборонених Кримінальним кодексом України (далі – КК України) під загрозою покарання. Останніми роками кількість злочинів, скоєних із використанням інформаційно-комунікаційних технологій, неухильно зростає [243].

Виходячи із структури інформаційної безпеки як об’єкта кримінально-правової охорони, систему інформаційних злочинів утворюють:

- злочини проти права на інформацію та охорони інформації від неправомірного доступу;

- злочини проти безпеки інформаційних ресурсів;

- злочини проти безпеки інформаційно-телекомунікаційних технологій. Кожна із запропонованих підсистем будується за ознакою наявності єдиного видового об’єкта. Їх об’єднує єдиний родовий об’єкт – інформаційна безпека.

До злочинів проти права на інформацію та захисту інформації від неправомірного доступу належать заборонені кримінальним законом суспільно небезпечні діяння, які посягають на суспільні відносини, що забезпечують реалізацію права шукати, отримувати, передавати, виробляти та поширювати інформацію законним способом, а також дозволяти або обмежувати доступ до інформації власниками такої інформації.

До злочинів проти безпеки інформаційного ресурсу слід відносити заборонені кримінальним законом суспільно небезпечні діяння, що посягають на суспільні відносини, що забезпечують безпеку, доступність, достовірність інформації у формі документів на електронних чи паперових носіях.

Злочинами проти безпеки інформаційно-комунікаційних технологій є

заборонені кримінальним законом суспільно небезпечні дії, які посягають на суспільні відносини, що забезпечують безпеку процесів та методів пошуку, збору, зберігання, обробки, надання, розповсюдження інформації за допомогою засобів обчислювальної техніки та інформаційно-комунікаційних мереж.

Аналіз норм Особливої частини КК України показав, що закріплено певну кількість складів злочинів, змістом яких виступають різні види деструктивного інформаційного впливу, інформаційного та комунікаційного характеру. Найчастіше описане у диспозиції статей КК України діяння може виявляти одночасно у обох сферах, тобто здійснюватися у вигляді поширення інформації, і шляхом комунікації (пропаганда тероризму, громадські заклики до скоєння злочинів тощо).

Значно рідше склади злочинів охоплюють одну форму прояву загроз інформаційної безпеки (виготовлення та обіг матеріалів або предметів з порнографічними зображеннями неповнолітніх як приклад інформаційної форми та залучення неповнолітнього до скоєння злочину як приклад комунікаційної форми).

Надання деструктивного інформаційного впливу переважно закріплено як злочинне діяння (поширення матеріалів, публічні заклики щодо порушення територіальної цілісності країни, вербування до складу незаконних озброєних формувань тощо), хоча в деяких випадках є способом скоєння злочинів (обман чи зловживання довірою як спосіб розкрадання у шахрайстві). Варто звернути увагу на правову категорію «психічне насильство», яка охоплює комплекс кримінально-караних видів деструктивного інформаційного впливу.

Г. В. Собко визначає кримінально-каране психічне насильство як протиправний суспільно небезпечне вплив на психіку іншої особи, проти її волі, що чиниться з прямим наміром і здатне заподіяти або завдає психічну, фізичну чи матеріальну шкоду [244, с. 27]. Учена вказує, що психічне насильство в закріплених кримінальним законодавством складах злочинів може бути як спосіб скоєння злочину та, з огляду на харак еристику обставин скоєного, як наслідок злочину. Г. М. Собко вказує на прогалини у КК України

щодо криміналізації реальних проявів небезпечного психічного насильства, зокрема нав'язливого переслідування.

У редакції КК України, що діє, немає спеціальних статей про відповідальність за надання деструктивного інформаційного впливу у формі сигналів від технічних пристроїв. Однак такі форми деструктивного інформаційного впливу можна побачити як способи скоєння злочинів, пов'язаних із заподіянням шкоди життю та здоров'ю людини.

Протягом останнього десятиліття законодавець активно вдавався до кримінально-правових інструментів для протидії різним формам деструктивного інформаційного впливу. На порядку денному питання встановлення кримінальної відповідальності за нові форми деструктивного інформаційного впливу – «треш-стріми» та глибокі фейки [245; 246].

Одна з проблем у сфері забезпечення інформаційної безпеки пов'язана із застосуванням технології фішингу – створення підроблених сайтів, порталів, інформаційних систем або їх частин, які імітують сайти органів публічної влади прибуткових та неприбуткових організацій з метою крадіжки конфіденційних. даних з пристроїв користувачів та подальшим використанням цих даних для незаконного збагачення. Фішинг поширений у сфері дистанційного банківського обслуговування і навіть сприяв появі інших нових видів злочинів в інформаційній сфері [247].

На думку О. І. Остапенко і О. В. Баїк, сучасною правовою основою забезпечення інформаційної безпеки в Україні є реалізація положень, закріплених у Стратегії воєнної безпеки України «Воєнна безпека – всеохоплююча оборона», що позитивно вплине на соціально-економічний розвиток країни, захищеність її суверенітету, територіальної цілісності, прав, свобод і законних інтересів особи, суспільства і держави [240, с. 174].

В умовах збройної агресії Російської Федерації проти України з метою посилення інформаційної безпеки Кримінальний кодекс України доповнено новими нормами, визначеними у законах:

- від 3 березня 2022 року № 2110-IX «Про внесення змін до деяких

законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції» [100];

- від 24 березня 2022 року № 2160-IX «Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану» [248];

- від 1 квітня 2022 року № 2178-IX «Про внесення змін до статті 114-2 Кримінального кодексу України щодо удосконалення відповідальності за несанкціоноване розповсюдження інформації про засоби протидії збройній агресії Російської Федерації» [249];

- від 22 травня 2022 року № 2265-IX «Про заборону пропаганди російського нацистського тоталітарного режиму, збройної агресії Російської Федерації як держави-терориста проти України, символіки воєнного вторгнення російського нацистського тоталітарного режиму в Україну» [206].

В. С. Батиргареєва у дослідженні «Правова платформа для забезпечення в Україні ефективного захисту цифрових трансформацій суспільства» зазначає, що стосується науки і галузі кримінального права, то тут принаймні необхідно розв’язати низку завдань, як-от: переосмислити теоретичні підходи до предмета злочину; взяти за основу класифікації злочинів ту ідею, що відбиватиме логіку цифрових трансформацій та забезпечуватиме надійний захист цих процесів засобами кримінального права; переглянути шляхи реалізації деяких інститутів кримінального права, насамперед пов’язаних із кваліфікацією вчиненого та реалізацією кримінальних покарань [250, с. 31].

Іншим видом юридичної відповідальності за скоєння правопорушень у сфері інформаційної безпеки є адміністративна відповідальність. На відміну від кримінальної відповідальності, її підставою можуть бути не тільки вчинення протиправних діянь, пов’язаних з наданням деструктивного інформаційного

впливу, але й з порушенням встановлених правил у галузі, що розглядається. Ця ознака визначає галузеву специфіку. Остання категорія складів адміністративних правопорушень закріплена переважно у главі 10 «Адміністративні правопорушення на транспорті, в галузі шляхового господарства і зв'язку» Кодексу України про адміністративні правопорушення (КУпАП).

Незважаючи на меншу суспільну небезпеку в порівнянні зі злочинами, адміністративні правопорушення у сфері, що розглядається, заслуговують на серйозну увагу. С. В. Пєтков, Н. О. Армаш, Є. Ю. Соболь Є. Ю. підкреслюють неприпустимість не дооцінок та небезпеки адміністративних правопорушень, що залишаються поширеними видами протиправної поведінки [251, с. 16].

Незважаючи на наявність у чинному КУпАП досить значної кількості складів адміністративних правопорушень, вони не утворюють системи і в основному спрямовані на захист окремих, часто не пов'язаних між собою аспектів діяльності забезпечення інформаційної безпеки, у низці випадків належним чином не солідаризуються з правовідносинами, що регулюються нормами матеріального та процесуального права, для охорони яких вони призначені. У конструюванні чинних норм є істотні недоліки юридично-технічного плану, що знижують ефективність застосування на практиці.

Норми, що містяться в КУпАП, охоплюють відносини у галузі забезпечення інформаційної безпеки, їх можливо класифікувати за основними напрямами такої важливої для держави діяльності: забезпечення доступу громадян та юридичних осіб до достовірної інформації; необхідності превентивного оповіщення громадян та юридичних осіб про факти та події, що створюють загрозу безпеці; забезпечення обмеження у доступі до певних категорій відомостей, поширення яких може завдати шкоди правам і свободам осіб, законної діяльності юридичних осіб або безпеки України.

При складанні переліків протиправного контенту та комунікації відзначено основні статті КУпАП, які встановлюють покарання за скоєння адміністративних правопорушень, пов'язаних із наданням деструктивного

інформаційного впливу. Серед них – низка статей, об'єктом порушень яких є медіапростір:

- ст. 146 КУпАП – порушення правил реалізації, експлуатації радіоелектронних засобів та випромінювальних пристроїв, а також користування радіочастотним ресурсом України;

- ст. 147 КУпАП – порушення правил охорони ліній і споруд зв'язку;

- ст. 148–1 КУпАП – порушення Правил надання та отримання комунікаційних послуг;

- ст. 148–3 КУпАП – використання засобів зв'язку з метою, що суперечить інтересам держави, з метою порушення громадського порядку та посягання на честь і гідність громадян;

- ст. 164–7 КУпАП – порушення умов розповсюдження і демонстрування фільмів, передбачених державним посвідченням на право розповсюдження і демонстрування фільмів;

- ст. 173–1 КУпАП – поширювання неправдивих чуток;

- ст. 188–7 КУпАП – невиконання законних вимог Національної комісії, що здійснює державне регулювання у сфері зв'язку й інформатизації; та інші, окрім тих, що нині стали актуальними, які мають вплив на формування ставлення до держави чи суспільних процесів, – це встановлення відповідальності за зміст та якість медіаконтенту радіо та телеорганізацій [252, с. 67].

Ні один із зазначених вище напрямів забезпечення інформаційної безпеки не захищається за допомогою адміністративних санкцій з належним рівнем комплексності, а ціла низка норм взагалі є окремими фрагментами зазначеної діяльності, системно між собою не пов'язані.

КУпАП не закріплює склад адміністративного правопорушення щодо надання деструктивного інформаційного впливу на підсвідомість людини. Джерелом погроз тут виступають відомості (наприклад, текстова інформація при її підпороговому пред'явленні) та інші види інформації (наприклад, акустичні сигнали певної частоти), що впливають на підсвідомість людини.

Оскільки самі засоби впливу на несвідоме не тільки існують, а й удосконалюються, необхідне опрацювання питання про механізм моніторингу щодо виявлення прихованих вставок в інформаційній продукції, охоплюючи інтернет-контент.

У нормах чинного КУпАП нема системного підходу в регулюванні відносин, пов'язаних із захистом у вигляді адміністративно-правових санкцій права громадян та їх об'єднань на отримання інформації, а також забезпечення поінформованості суспільства про соціально значущі події та факти. Не повною мірою забезпечуються у цій сфері інтереси органів державної влади і органів місцевого самоврядування.

Роль цивільно-правової відповідальності у правовому механізмі забезпечення інформаційної безпеки є незначною. Тут застосовані норми Цивільного кодексу України про компенсацію моральної шкоди, захист честі, гідності та ділової репутації та зобов'язання внаслідок заподіяння шкоди [253].

Зростає значення питання про відповідальність у сфері критичної інформаційної інфраструктури. Закон України «Про критичну інфраструктуру» встановлює основні засади забезпечення безпеки критичної інформаційної інфраструктури, повноваження державних органів у цій галузі, права, обов'язки, відповідальність осіб, які володіють на праві власності або іншій законній підставі об'єктами такої інфраструктури [254].

Пункт 11 Прикінцевих та перехідних положень Закону передбачає, що уповноваженому органу у сфері захисту критичної інфраструктури України протягом року з дня початку ним діяльності підготувати зміни до Закону України «Про критичну інфраструктуру» в частині визначення форм та розмірів штрафних санкцій до операторів об'єктів критичної інфраструктури, до Кримінального кодексу України та Кодексу України про адміністративні правопорушення [254].

Безпека критичної інформаційної інфраструктури та її об'єктів забезпечується, зокрема, за рахунок цілей: розроблення критеріїв категорування об'єктів критичної інформаційної інфраструктури, показників критеріїв

порядку категорування об’єктів; ведення реєстру об’єктів критичної інформаційної інфраструктури; встановлення вимог щодо забезпечення безпеки об’єктів критичної інформаційної інфраструктури з урахуванням категорій; створення систем безпеки об’єктів критичної інформаційної інфраструктури та забезпечення функціонування; забезпечення взаємодії систем безпеки з державною системою виявлення, попередження та ліквідації наслідків комп’ютерних атак на інформаційні ресурси; державного контролю у сфері безпеки критичної інформаційної інфраструктури.

Спеціальна кримінально-правова охорона інформаційно-комунікаційного комплексу, що забезпечує нормальне функціонування особливо важливих для суспільства та держави об’єктів, не є винаходом законодавця та трапляються у багатьох правових режимах. Положення про кримінальну відповідальність за посягання на публічні інформаційні ресурси, що мають виняткову значимість, є в законодавстві країн Європейського Союзу.

До таких дій можна віднести створення та поширення комп’ютерних програм чи іншої інформації, свідомо призначених для неправомірного впливу на критичну інформаційну інфраструктуру; неправомірний доступ до інформації, що охороняється законом, що міститься в критичній інформаційній інфраструктурі; порушення правил експлуатації та засобів зберігання, обробки або передачі охоронної інформації в цій інфраструктурі залежно від спрямованості на публічні електронні інформаційні ресурси та інформаційні системи державних органів.

У постанові Кабінету Міністрів України «Деякі питання об’єктів критичної інформаційної інфраструктури» відображено питання відповідальності іншого роду, відповідальності органу державного контролю та його посадових осіб під час здійснення перевірки [255]. Слід зазначити, що ця норма аналогічно до норми, закріпленої у Законі України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності» [256].

У статті 166-21 «Порушення порядку здійснення державного нагляду (контролю) у сфері господарської діяльності» КУпАП встановлено

відповідальність за недотримання посадовими особами органів державного контролю (нагляду). У разі неналежного виконання ними функцій, службових обов'язків та вчинення протиправних дій (бездіяльності)) після проведення перевірки можуть притягуватися до адміністративної відповідальності [257].

Інститут відповідальності за інформаційні правопорушення як комплекс охоронних норм системи права є міжгалузевим структурним утворенням, що забезпечує безпеку суспільних відносин в інформаційному просторі та спрямований на захист інтересів особи, суспільства та держави в інформаційній сфері.

Аналіз механізмів юридичної відповідальності в інформаційній сфері дає можливість розглянути інформаційно-правову відповідальність як самостійний вид юридичної відповідальності. Низку заходів державного примусу, закріплених безпосередньо інформаційним законодавством, можна вважати за заходи інформаційно-правової відповідальності. Такі заходи мають важливе значення у механізмі правового забезпечення інформаційної безпеки.

Як приклад можна навести комплекс правових санкцій щодо засобів масової інформації за порушення заборони про зловживання свободою масової інформації, передбачених законодавством про засоби масової інформації: відмову в реєстрації засобу масової інформації; призупинення та припинення діяльності засобу масової інформації; зупинення, анулювання чи припинення дії ліцензії на телевізійне мовлення чи радіомовлення [121-124].

Як міру інформаційно-правової відповідальності щодо інтернет-ресурсів, що допускають поширення протиправного контенту та не реагують на повідомлення регулятора, можна розглядати обмеження доступу до них. Хоча такі заходи більш правильно оцінювати як запобіжні заходи.

Юридична відповідальність у сфері забезпечення інформаційної безпеки в умовах розвитку цифрової економіки має міжгалузевий, комплексний характер. Серед примусових заходів у межах інституту юридичної відповідальності за правопорушення у сфері інформаційної безпеки необхідно виділити заходи публічного припинення, які застосовує орган виконавчої влади

або його посадова особа у позасудовому порядку. Заходи публічного припинення застосовуються за невиконання суб'єктом мережі Інтернет обов'язків перед органом виконавчої влади. Наприклад, перед Міністерством цифрової трансформації України, Міністерством культури та інформаційної політики України, Служби безпеки України, Державної служби спеціального зв'язку та захисту інформації України, Національної комісії, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку, їх посадових осіб [258].

До заходів публічного запобіжного заходу в інформаційній сфері можна віднести обмеження прав у вигляді: встановлення обов'язків блокування персональних даних; обмеження доступу до заблокованого веб-сайту; зупинення діяльності мережевого видання.

Заходи інформаційного примусу, передусім, заходи публічного запобіжного заходу, відрізняються від інших заходів відповідальності, встановлених адміністративним, кримінальним, іншим публічним законодавством, особливостями юридичної формалізації: нормативно-правове регулювання здійснюється на підставі правил, встановлених Кабінетом Міністрів України або відомчим нормативним актом органу спеціальної компетенції у сфері інформаційної безпеки, що деталізуються в нормативно-правових та правозастосовних актах органів публічної адміністрації; застосування заходів публічного запобіжного заходу проводиться відразу після ухвалення відповідного рішення, у терміни визначені чинним законодавством. Рішення щодо застосування заходів публічного припинення можуть бути оскаржені в судовому порядку.

Аналіз показує, що одним із найбільш актуальних організаційно-правових механізмів та примусових заходів в інституті юридичної відповідальності в інформаційній сфері є блокування (обмеження роботи) вебсайту або іншого мережевого ресурсу.

Блокування вебсайту в Інтернеті має складну юридичну природу, являючи собою превентивний засіб, який доцільно віднести до

забезпечувальних заходів, міру захисту від неправомірних дій інформації, що завдає шкоди або є протиправною санкцією за правопорушення. Зазначені заходи здійснюються відповідно до Законів України «Про санкції», «Про захист суспільної моралі в Україні», законів, направлених на забезпечення інформаційної безпеки в умовах військової агресії Російської Федерації проти України» [50; 100; 159; 247; 248].

Правова природа блокування (обмеження доступу до вебсайтів), ресурсів або інформації неоднорідна. З одного боку, таке обмеження може бути мірою превентивного характеру (наприклад, тимчасове блокування), з іншого боку, санкцією за порушення встановлених правил і норм, виконувати функцію захисту особи від шкідливої інформації.

У Законі України «Про захист інформації в інформаційно-комунікаційних системах» та в інших нормативно-правових актах не розкривається, що слід розуміти під обмеженням доступу до вебсайту. Визначення необхідно закріпити нормативно. Обмеження доступу до вебсайту є здійсненням на підставі рішення уповноваженого органу або суду комплексу заходів з метою унеможливлення використання інформації, вебсайту або сервісу.

Питання обмеження доступу до веб-сайтів є важливими для розвитку системи інформаційної безпеки. Нині блокування є універсальним механізмом (засобом), який активно застосовується у країнах Європейського Союзу та країнах Північноатлантичного альянсу (НАТО) у контексті Директиви Європейського Парламенту і Ради (ЄС) 2018/1972 від 11 грудня 2018 року про запровадження Європейського кодексу електронних комунікацій [259].

Особливої уваги заслуговує співпраця з країнами НАТО у сфері профілактики тероризму, російського експансіонізму, «русского мира», «исторического единства русского и украинского народов» в Інтернеті, в інформаційному середовищі та цифровому просторі, оскільки такі інформаційні ресурси мають потенційну небезпеку, можуть бути джерелом для поширення протиправних ідей [260].

Дослідження дозволило сформулювати висновок про те, що в системі

забезпечення інформаційної безпеки інформаційні правопорушення становлять особливу правову конструкцію, виражену в застосуванні спеціальних примусових заходів в інформаційній сфері, як-от: блокування інформаційного ресурсу, вебсайту та інформації; встановлення обов'язків блокування персональних даних; призупинення діяльності мережевого видання.

Обмеження доступу до інформаційних ресурсів розглядається як захід, що реалізує превентивну, каральну, охоронну та інші функції юридичної відповідальності.

Закономірності розвитку суспільних відносин у сфері інформаційної безпеки в умовах розвитку цифрових технологій визначають появу в майбутньому нових примусових заходів щодо окремих видів інформації та інформаційних об'єктів, дій суб'єктів тощо.

У Національній економічній стратегії на період до 2030 року та розвитку інформаційного суспільства в Україні стверджується, що формування цифрової економіки та забезпечення національних інтересів у галузі цифрової економіки є стратегічним національним пріоритетом, що реалізується у тому числі забезпеченням інформаційної безпеки.

Стратегія інформаційної безпеки України є основою для формування державної політики та розвитку суспільних відносин у галузі забезпечення інформаційної безпеки, для вироблення заходів вдосконалення системи забезпечення інформаційної безпеки. Таких як, забезпечення єдності, стійкості та безпеки інформаційно-комунікаційної інфраструктури на всіх рівнях інформаційного простору; забезпечення організаційного та правового захисту особи, бізнесу та державних інтересів при взаємодії в умовах цифрової економіки; створення умов для провідних позицій у галузі експорту послуг та технологій інформаційної безпеки, врахування національних інтересів у міжнародних документах з питань інформаційної безпеки.

На думку авторів наукової статті «Розвиток цифрової економіки в контексті забезпечення інформаційної безпеки в Україні», до числа основних принципів, які формують інформаційну безпеку в умовах цифрової економіки,

належать: необхідність заміщення технологій, розроблених у Російській Федерації, незалежно від сфери застосування в економіці, забезпечення цілісності, автентифікації та конфіденційності, доступності інформації, що передається, процесів обробки, використання національних технологій, розроблених за стандартами Європейського Союзу або які застосовуються в Європейському Союзі та НАТО, а також відповідного програмного забезпечення і технічних засобів з використанням криптографічних стандартів і методів шифрування НАТО [261, с. 2026].

Формування нових суспільних відносин, пов'язаних з розвитком цифрової економіки, потребує наукового осмислення питань організаційно-правового забезпечення інформаційної безпеки з позиції інформаційного права, удосконалення механізмів юридичної відповідальності і правового регулювання, вирішення низки правових організаційних питань з метою розвитку системи цифрової економіки, передбаченої у стратегічних документах.

Одним з основних компонентів цифрової економіки є значне зміщення в Інтернеті операцій продажу продуктів, надання послуг господарюючими суб'єктами. Розширення застосування нових форм отримання товарів та послуг споживачами спричинить збільшення обсягу безготівкових розрахунків та зростання ризиків, пов'язаних із такими розрахунками. Це потребує створення надійної системи безпеки, яка гарантуватиме захищеність безготівкових коштів населення. Це вимагає нових теоретико-правових підходів, у тому числі спрямованих на вироблення міжгалузевих механізмів для розвитку нових інститутів, класифікації нових суб'єктів відносин, принципів, внесення змін до нормативно-правових актів, у тому числі галузевих, що також підкреслює міжгалузевий характер інституту відповідальності щодо забезпечення інформаційної безпеки.

Як приклад можна навести використання Інтернету для різноманітних атак на інформаційний простір, хоча розвиток Інтернету є одним із напрямів цифрової економіки, всесвітнім трендом та перспективним напрямом для сфери

інформаційних технологій, з погляду розвитку технологій і користі для економіки, що підкреслювалося у програмних документах та документах стратегічного планування [262].

Під час використання різних сервісів, соціальних мереж і медіа-продуктів існує ризик обмеження відповідальності компаній, мають місце складності, пов'язані з транскордонною юрисдикцією при судовому розгляді та обмеження користувачів у захисті прав та законних інтересів.

Це питання може бути вирішене шляхом охоплення користувацькими угодами (між користувачами та власниками сервісів і послуг в мережі Інтернет) надання можливості вибору користувачем (фізичною або юридичною особою) юрисдикції з метою захисту прав у сфері забезпечення інформаційної безпеки застосування, відповідних норм про юридичну відповідальність за правопорушення у цій сфері.

Питання юрисдикції національних ІТ-компаній у користувацьких угодах вирішене шляхом застосування у разі виникнення спорів національного законодавства та юрисдикції на основі норм юридичної відповідальності за правопорушення у сфері забезпечення інформаційної безпеки [263].

Юридична відповідальність у сфері забезпечення інформаційної відповідальності охоплює дисциплінарну відповідальність, що регулюється чинним законодавством і корпоративними нормами.

Дослідження інституту юридичної відповідальності у системі правового забезпечення інформаційної безпеки в Україні дозволяють зробити висновки.

Юридична відповідальність у сфері забезпечення інформаційної відповідальності має міжгалузевий характер правового інституту. Найбільш показовою в цьому плані є одна зостанніх важливих законодавчих ініціатив у сфері, що розглядається, пов'язана з протидією поширенню інформації воєнного значення.

Застосування міжгалузевого пакетного принципу регламентації правових механізмів протидії загрозам інформаційній безпеці є першочерговим. Особливо важливо продумувати питання правового методу обмеження доступу

до протиправного контенту за криміналізації чи запровадження адміністративної відповідальності.

Для посилення кримінально-правової охорони інформаційної безпеки в Україні доцільно доповнити Кримінальний кодекс України розділом «Злочини проти інформаційної безпеки», внесення якого до нової редакції Кримінального кодексу України послужить ефективним механізмом досягнення цієї мети.

Юридична відповідальність в системі забезпечення інформаційної безпеки спрямована на забезпечення реальних умов для розвитку та захисту всіх сфер власності на інформаційні ресурси; створення та вдосконалення державних та регіональних інформаційних систем та мереж, забезпечення сумісності та взаємодії в єдиному європейському віртуальному просторі; створення умов для ефективного інформаційного забезпечення громадян та інших споживачів на основі публічних інформаційних ресурсів, забезпечення безпеки у галузі інформації та інформатизації.

Для ефективного реагування на наявні проблеми у сфері забезпечення інформаційної безпеки, що перебувають у площині правового регулювання інформаційних відносин, можна виділити кілька способів, що полягають у підвищенні ефективності чинних норм права шляхом диференціювання складів правопорушень з урахуванням збитків, заподіяних порушником; суттєвого збільшення розмірів штрафних санкцій, у площині адміністративної відповідальності та кримінальних покарань; наділенням органів публічної влади додатковими повноваженнями щодо адміністративного провадження обмеження доступу до протиправної інформації та інформації деструктивного впливу.

Необхідно продовжувати наукові дослідження інформаційного права, спрямовані на вивчення спільних питань інформаційної відповідальності щодо безпеки, суб’єктів та об’єктів дослідження. Необхідне активне залучення органів державної влади щодо зарovадження та розробки нових навчальних програм на всіх рівнях освітньої системи, що сприятиме формуванню правового фундаменту для подальших практичних кроків у напрямі

забезпечення інформаційної безпеки.

Висновки до розділу 2

Рівень інформаційної безпеки залежить не лише від цифровізації суспільних відносин та спроможності держави, але й від правової урегульованості зазначених процесів. Забезпечення інформаційної безпеки здійснюється у процесі функціонування спеціально створеного механізму публічно-правового впливу, спрямованого на досягнення поставленої мети та практичної реалізації національних інформаційних інтересів за допомогою реалізації комплексу відповідних взаємопов'язаних заходів політичного, правового, організаційного та технічного характеру. Механізм правового впливу в інформаційній сфері ґрунтується на механізмі правового регулювання суспільних відносин адміністративно-правовими засобами. Основне місце у системі механізму адміністративно-правового регулювання посідають адміністративно-правові норми та адміністративні правовідносини, методи правового регулювання, суть яких зводиться до встановлення певного порядку дій у вигляді встановлення заборон, передбачених адміністративно-правовою нормою.

Адміністративно-правові засоби забезпечення інформаційної безпеки – це система адміністративно-правових норм та адміністративних процедур, що реалізуються уповноваженими суб'єктами та надають регулювальний вплив на поведінку фізичних і юридичних осіб громадян в інформаційній сфері з метою недопущення деструктивних інформаційних впливів та пов'язаних з ними наслідків і охоплюють різні методи і способи правового регулювання.

Концептуальна модель адміністративно-правового механізму забезпечення інформаційної безпеки має такі елементи: зміст інформаційної безпеки як об'єкта адміністративно-правового забезпечення, що охоплює форми антисоціальної поведінки, що трансформуються з інформаційної сфери у сферу суспільної та особистої безпеки; загрози інформаційній безпеці, що

виходять від суб'єктів інформаційної діяльності у межах держави та з-за кордону; система суб'єктів, які здійснюють функції адміністративно-правового забезпечення інформаційної безпеки; уніфіковані норми, що регламентують підстави та порядок застосування заходів адміністративно-правового забезпечення; моніторинг та ідентифікація видів загроз інформаційній безпеці. Адміністративно-правовий механізм забезпечення інформаційної безпеки забезпечує нейтралізацію загроз в аналізованій сфері.

Адміністративно-правові обмеження у контексті забезпечення інформаційної безпеки встановлюються органами публічної влади для підтримки встановленого порядку управління в інформаційному просторі. Нормативно-правове регулювання діяльності засобів масової інформації продукує різні типи правових режимів, у яких головними регулювальними впливами є дозволи, зобов'язання та заборони. Специфічний зміст правового регулювання засобів масової інформації зумовлює застосування спеціальних правових методів, таких, як: реєстрація, ліцензування, акредитація, укладання контрактів.

Можливість надання впливу засобів масової інформації на невизначене коло осіб змусила законодавця в межах інформаційного законодавства сформувати низки обмежень та заборон щодо доступу до протиправної інформації. Для досягнення необхідного стану соціальної стабільності єдиним придатним засобом є правомірні обмеження прав фізичних і юридичних осіб в інформаційній сфері.

Головним критерієм є соціально значуща користь. Основним елементом адміністративно-правового обмеження є правова заборона – юридична конструкція, що представляє характеристику правової поведінки як утримання від вчинку на підставі адміністративних засобів. Адміністративно-правові обмеження щодо забезпечення інформаційної безпеки – це сукупність положень виражених у нормах адміністративного права у формі індивідуального правового акта управління, які обмежують права фізичних і юридичних осіб з метою забезпечення належного балансу інтересів фізичних і

юридичних осіб, суспільства та держави в інформаційній сфері.

Системне балансування відповідних адміністративно-правових обмежень у контексті забезпечення інформаційної безпеки у засобах масової інформації здатне забезпечити підвищення ефективності застосування. Однак належного системного підходу до норм про юридичну відповідальність за недотримання заборон нині немає, що зумовлює наявну у правозастосовній практиці різну правову оцінку вчинених порушень.

Інформаційна безпека в мережі Інтернет – складна теоретична конструкція, яка поєднує правовий стан та правове становище суб'єктів інформаційної діяльності, що охоплює природно-правові та позитивно-нормативні елементи. До природно-правових елементів належать законні інтереси, правові ризики, потенційні можливості реалізації прав, що визначають правовий стан суб'єкта інформаційних правовідносин; до позитивно-нормативних елементів – права, обов'язки, відповідальність та юридичні гарантії, що характеризують правове становище.

Правове забезпечення інформаційної безпеки у мережі Інтернет характеризується двоїстістю, що передбачає законодавчі та договірні засади регулювання. Це пов'язано з установками на саморегулювання в Інтернеті, оскільки віртуальний простір і комунікація побудована інакше, ніж у реальному просторі, а також з обмеженими можливостями державних правових механізмів забезпечення гарантій реалізації прав і свобод у віртуальному просторі, у тому числі інформаційну безпеку особи. Виходячи із загальних принципів правового регулювання відносин у мережі Інтернет, можна стверджувати, що такі відносини мають бути обмеженими, що зумовлено необхідністю захисту прав і свобод людини та громадянина, суспільної моралі, безпеки держави. Також сприяти забезпеченню інформаційної безпеки у межах правовідносин, що виникають у мережі Інтернет, регульованих різними галузями права, у тому числі: захищати гідність особи, право на недоторканість приватного життя, особисту та сімейну таємницю, честь та добре ім'я, права на захист від деструктивного інформаційного впливу, неправдивої інформації, заборони

пропаганди держави-агресора. Забезпечення інформаційної безпеки в Інтернеті має свою специфіку, що вимагає обліку в юридичній науці та практиці через вплив великої кількості зовнішніх соціальних і технологічних чинників, а також внутрішніх спонукальних мотивів суб'єкта інформаційної діяльності.

Правове забезпечення інформаційної безпеки в Інтернеті за умов невизначеності правового регулювання та природи інтернет-процесів сприяє розвитку судової та правозастосовної практики. Це вимагає накопичення інформації про реальні правові наслідки, на підставі яких можна робити висновок про необхідність запровадження певного правового інструменту або залучення суб'єкта до сфери юридичної відповідальності.

У юридичній науці не сформульовано наукове поняття юридична відповідальність об'єктом якої є інформаційна безпека. Для визначення поняття юридична відповідальність щодо забезпечення інформаційної безпеки має бути сформована належна методологічна основа, що охоплює визначення родового поняття, щодо якого видовим поняттям має бути інформаційна безпека особи, суспільства і держави. У контексті розуміння, згідно з яким інформаційна безпека розглядається як процес необхідності, юридична відповідальність є способом вираження в правових актах юридичних норм, що визнані як необхідні державною владою для забезпечення національних інтересів в інформаційному просторі.

Зміст юридичної відповідальності щодо забезпечення інформаційної безпеки визначається системою юридичних норм кримінального, адміністративного, цивільного, інформаційного права, як ієрархічно організована сукупність нормативно-правових актів публічної влади, у яких має виражатися нормативна визначеність вимог, визначених законом.

Інститут юридичної відповідальності щодо забезпечення інформаційної безпеки характеризує кількісною та якісною визначеність норм кримінального, адміністративного, цивільного та інформаційного права. Кількісна визначеність законодавства характеризується оптимальною кількістю нормативно-правових актів з однаковою предметністю на різних рівнях законодавства. Якість

нормативно-правової бази пов’язується зі ступенем придатності законодавства для врегулювання суспільних відносин в інформаційному просторі згідно з визначеною метою правового регулювання в контексті забезпечення національних інтересів України.

Систематичне та послідовне удосконалення юридичної відповідальності у сфері забезпечення інформаційної безпеки потребує вироблення та реалізації державної правової політики розвитку інформаційного, кримінального та адміністративного законодавства відповідно до Стратегії інформаційної безпеки України як самостійного постійного напряму забезпечення інформаційної безпеки. В умовах правового режиму воєнного стану у сфері забезпечення інформаційної безпеки виникають додаткові правові зобов’язання, невиконання яких має зумовлювати додаткову юридичну відповідальність одночасно з відповідальністю, яку несуть органи публічної адміністрації за умов функціонуванняв межах воєнного стану.

РОЗДІЛ 3
ШЛЯХИ УДОСКОНАЛЕННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

3.1. Пріоритетні напрями удосконалення законодавства у сфері забезпечення інформаційної безпеки в умовах цифрової трансформації

Формування принципово нового технологічного середовища з урахуванням цифрових технологій істотно впливає на економіку, політику та соціальні процеси сучасного світу. Вплив цифрової революції поширився на систему права на національному та на міжнародному рівні. Передові цифрові технології, що застосовуються в різноманітних галузях діяльності, які охоплюють Інтернет речей (Internet of things), штучний інтелект і машинне навчання (Artificial intelligence & Deep learning), технології на принципах розподіленого реєстру (Blockchain), хмарні комп'ютерні сервіси та обчислення (Cloud mputing), розумні комплекси та пристрої (Smart everything), великі дані (Big Data), віртуальна та доповнена реальність (Augmented & additive reality), сучасні біоінженерні технології (Biotech), системи кібербезпеки (Cybersecurity), соціальні мережі (Facebook, *Instagram,* Twitter), цифрові двійники (Digital twins), цифрові технологічні платформи (агрегатори) та пов'язані з ними інші технології, створили технологічний базис для формування принципово нового середовища адміністративно-правового та інформаційно-правового регулювання.

Застосування цифрових технологій у зв'язку зі стратегічною спрямованістю європейського та національного розвитку цифрової економіки, цифровізації різноманітних сфер діяльності зумовили зростаючий науковий інтерес до теоретичних та науково-практичних досліджень, у тому числі в галузі правового регулювання забезпечення інформаційної безпеки. Перспективи розвитку інформаційного права багато в чому пов'язані з

використанням цифрових технологій у сфері забезпечення інформаційної безпеки.

Питання про значення інформаційної безпеки в житті суспільства та кожного з нас не потребує додаткового обґрунтування, але, безсумнівно, потребує пильної уваги. В інформаційному суспільстві, заснованому на знаннях, роль інформаційної безпеки визначається потребою реалізації права людини на інформацію, позбавлення деструктивного інформаційного впливу, необхідністю забезпечення системи стратегічного планування та розвитку національного інформаційного середовища.

Розробка методологічних, організаційних і нормативно-правових засад побудови системи інформаційної безпеки розпочалася у 90-ті роки минулого століття, але не втратила актуальності сьогодні для забезпечення інтересів особи, суспільства та держави.

Сукупність національних документів стратегічного планування, охоплюючи ухвалені стратегії та доктрини, сьогодні значною мірою характеризує основні цілі, завдання та напрями розвитку інформаційної безпеки. Серед інших важливих завдань Стратегія інформаційної безпеки України передбачає розвиток механізмів електронної взаємодії між органами державного управління України, місцевими органами державної влади з державними позабюджетними фондами, фізичними та юридичними особами в межах концепції електронного уряду.

Доцільно відзначити, що в умовах збройної агресії Росії набуває суттєвого значення виконання вимоги Стратегії воєнної безпеки України щодо інформаційної безпеки, відображеної у Законах України: «Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану»; «Про внесення змін до статті 114-2

Кримінального кодексу України щодо удосконалення відповідальності за несанкціоноване розповсюдження інформації про засоби протидії збройній агресії Російської Федерації» та інших [248: 249].

В умовах динаміки інформаційного суспільства інформаційна безпека набуває характеру стратегічного ресурсу в системі цифровізації управління, оскільки цифрові технології, перебуваючи у постійному розвитку та розширюючи доступ до інформації на основі електронної взаємодії різних суб'єктів, створюють умови для переходу державного управління на новий рівень та підвищення якості життя населення, що потребує наукового осмислення з позиції інформаційного права та подальшого вдосконалення правового регулювання відносин в інформаційній сфері.

Велику роль в умовах цифровізації мають питання реалізації конституційного права на інформацію, забезпечення права на достовірну інформацію, що охоплює інформаційна безпеки.

Юридичні ознаки забезпечення інформаційної безпеки вказують на первинну публічно-правову природу та самостійність, що дозволило визначити зазначений інститут у двох аспектах: вузькому та широкому. У широкому аспекті забезпечення інформаційної безпеки – правовий елемент інформаційної діяльності держави, спрямований на реалізацію державної політики у соціально-інформаційній та економічній сфері шляхом створення умов захисту інформації, інформаційних систем і ресурсів та захисту від деструктивного інформаційного впливу. У вузькому аспекті забезпечення інформаційної безпеки є самостійним елементом в структурі інформаційного права, створеним та регульованим спеціальними нормативно-правовими актами.

У документальному аспекті інформаційна безпека охоплює сукупність нормативно-правових актів та ненормативно-правових актів, довідкові, нормативно-технічні документи, документи стратегічного планування, програмно-цільові документи, ненормативні правові акти, правові знання, правова статистика, акти правозастосовної практики, акти тлумачення законодавства, правові коментарі тощо.

Нормативно-правові документи, інформаційні ресурси є складовою інформаційної системи і належать до інформаційної інфраструктури, входять до системи забезпечення інформаційної безпеки України.

Право на достовірну інформацію багато в чому пов'язане з тим, що Стратегія інформаційної безпеки Україні закріплює поступовий перехід від інформаційного суспільства до суспільства знань, у якому переважне значення з урахуванням національних пріоритетів мають отримання, збереження, виробництво та розповсюдження. достовірної інформації, що забезпечується заходами та засобами інформаційної безпеки [58].

Під нормативною базою інформаційної безпеки у широкому сенсі слід розуміти всю сукупність правових знань, що охоплюють не лише нормативно-правові акти, а й документи стратегічного планування, програмно-цільові документи, акти правозастосовної практики, акти тлумачення законодавства, коментарі до законів.

У вузькому значенні під нормативною базою інформаційної безпеки слід розуміти масив нормативно-правових актів та тісно пов'язаних з ними актів та документів правового змісту – акти тлумачення, довідкові матеріали, нормативно-технічні документи тощо.

Важливими властивостями інформаційної безпеки є її актуальність, що забезпечується системною єдністю її цінності та корисності, що набуло достатнього наукового обґрунтування у працях учених [250; 261].

Оскільки у формуванні системи нормативно-правових актів беруть участь місцеві органи влади та органи місцевого самоврядування, необхідно на основі досягнень цифровізації та системного підходу виявити однорідні та суттєво взаємопов'язані компоненти наявної нормативної бази інформаційної безпеки для об'єднання їх у систему нормативного забезпечення інформаційної безпеки.

Зазначена система є впорядкованою багаторівневою сукупністю інформаційних ресурсів нормативно-правового характеру на базі сучасних інформаційних технологій, єдиного програмно-апаратного середовища, що надає функціонально повний набір інформаційно-технологічних сервісів, які

забезпечують збирання, обробку, зберігання, надання та передачу інформації з метою підвищення інформаційної безпеки та безпеки критичної інформаційної інфраструктури.

Охоплення інформаційних технологій системою інформаційної безпеки, формування, розвиток та подальше вдосконалення державної системи інформаційної безпеки є важливими складовими національної безпеки держави що має суттєве значення в умовах збройної агресії Російської Федерації щодо України.

Управління процесами забезпечення інформаційної безпеки має перебувати у підпорядкуванні держави, яка згідно з Конституцією України зобов'язана забезпечити права, свободи та законні інтереси фізичних і юридичних осіб на основі достовірної та актуальної інформації, захисту від інформаційного деструктивного впливу. Для цього потрібний науково-технічний потенціал та використання цифрових технологій для забезпечення інформаційної безпеки, що відповідає всім необхідним сучасним параметрам безпеки.

На основі розвитку правової культури інформаційного суспільства та правосвідомості вимагають уваги такі визнані інститути правового регулювання у сфері забезпечення інформаційної безпеки, як юридична техніка, експертиза нормативно-правових актів, застосування цифрових технологій у юридичній діяльності, правового моніторингу, використання різноманітних форм контролю та оцінки якості законодавства та ефективності застосування права.

Аналіз чинного законодавства показав наявність розвиненої системи правового забезпечення інформаційної безпеки. Водночас є прогалини у правовому регулюванні. У зв'язку з надзвичайно високою динамічністю розвитку інформаційної сфери в умовах цифрової трансформації необхідно виробляти правові рішення, що дозволяють успішно підготуватися до появи нових інформаційних загроз.

Одна з прогалин у чинному інформаційному законодавстві полягає в

тому, що за наявності широкого переліку правових механізмів забезпечення інформаційної безпеки у базових джерелах інформаційного права є брак основоположних положень та засад інформаційної безпеки.

Для іншого ключового елемента інформаційної безпеки – захисту інформації такі основні норми закріплені у Законі України «Про захист інформації у інформаційно-комунікаційних системах».

Стаття 1 «Визначення термінів» і 9 «Забезпечення захисту інформації в системі» закону закріплює правову дефініцію захисту інформації, визначає методи та зміст державного регулювання відносин у цій сфері, встановлює низку правових обов'язків та вимог щодо захисту інформації.

Причина очевидна – назва цього закону адекватно відображає його предмет регулювання, але блок інформаційної безпеки виходить за межі захисту інформації.

Має місце, коли передові вітчизняні розробки у сфері правового регулювання отримують підтримку, але не знаходять втілення у законодавстві. Закріплення блоку норм про поняття, правові принципи та засоби забезпечення інформаційної безпеки дуже важливе.

Надання інформаційної безпеки статусу стратегічного національного пріоритету у Стратегії інформаційної безпеки України вимагає зміни ситуації, що склалася, та повноцінної правової регламентації основ забезпечення інформаційної безпеки на рівні закону.

Тому доцільною є пропозиції про доповнення змісту Закону України «Про інформацію» нормами щодо забезпечення інформаційної безпеки. Пропозиція полягає у внесенні до закону окремої статті щодо забезпечення інформаційної безпеки (Додаток Б).

Таке рішення забезпечить побудову логічної та цілісної системи правового регулювання інформаційної безпеки, що охоплює спочатку базові відправні засади забезпечення, а потім правові норми щодо двох фундаментальних напрямів забезпечення – захисту інформації та інформаційної безпеки.

Як зазначалося вище, у 2014 році такий законопроєкт розроблявся групою вчених та депутатів Верховної Ради України, проте не був ухвалений парламентом. Аналіз положень цього законопроєкту показав, що він переважно регламентує цілі, завдання, принципи та напрями забезпечення інформаційної безпеки, організацію державної системи забезпечення інформаційної безпеки та міжнародного співробітництва.

Однак таке широке коло питань забезпечення інформаційної безпеки доцільно нормативно закріпити в документі стратегічного планування. Механізм практичного використання може бути різним – як використання основи для розробки офіційного документа стратегічного планування з такою назвою, так і застосування під час оновлення Стратегії інформаційної безпеки України. Кожне з рішень має переваги та недоліки.

Наприклад, основним аргументом на користь варіанта єдиного документа є тісний взаємозв’язок інформаційно-психологічних та інформаційно-технічних загроз, так само як діяльність державних органів щодо протидії. Щодо законодавства у сфері забезпечення інформаційної безпеки, то оптимальною стратегією розвитку є закріплення правових засад забезпечення інформаційної безпеки у Законі України «Про інформацію» у поєднанні з регламентацією окремих напрямів та аспектів забезпечення інформаційної безпеки у самостійних законодавчих актах.

У цифровій сфері важливе значення мають інформаційні системи та офіційні сайти органів публічного управління, надання адміністративних послуг органами публічного управління, що здійснюється на основі інформаційних систем.

А. Є. Краковська та М. К. Бабик вказують, що цифровізація адміністративних послуг повинна у повному обсязі забезпечити користувачів безпечними сервісами, метою яких буде надання доступу до детальної інформації про послугу, можливість заповнювати та завантажувати необхідні для отримання послуги зразки та форми документів, механізмом інформування користувача про стан розгляду, а також здатністю онлайн оплати послуги. Нині

такий механізм в Україні працює недосконало, що викликає певні труднощі під час отримання адміністративних послуг за допомогою сучасних технологій [264, с. 332]. Учені в загальному аспекті пропонують внесення змін до нормативних актів, але не конкретизують вимоги.

Доцільно доповнити Закон України «Про адміністративні послуги» частиною 3 до статті 5 вимогою щодо організації інформаційної безпеки (Додаток В*)* [265].

Інформаційні системи, що містять правову інформацію, яка застосовується у сфері публічного управління та судової системи, є базою інформаційно-правового забезпечення організаційно-управлінської діяльності органів публічної влади, судової діяльності у сфері інформаційної безпеки, що дозволяє розвивати державні інформаційні системи у різних галузях діяльності із забезпеченням вимог інформаційної безпеки.

У базовому нормативному акті щодо державних інформаційних ресурсів Закон України «Про публічні електронні реєстри» безпосередньо не згадується інформаційна безпека. Водночас зазначений закон доцільно доповнити словами: «Вимоги про захист інформації, які містяться в реєстрах, встановлюються центральним органом виконавчої влади зі спеціальним статусом у сферах електронних комунікацій, радіочастотного спектру та надання послуг поштового зв’язку» (Додаток Д) [266].

Аналіз європейського досвіду свідчить про успішність переведення органів публічної влади на сервісні моделі споживання хмарних сервісів, центрів обробки даних з метою підвищення стабільності роботи інформаційно-комунікаційних систем, підвищення безпеки інформації, що міститься в інформаційних ресурсах, зменшення витрат на розвиток інформаційно-комунікаційної інфраструктури, охоплюючи хмарні сервіси.

12 березня поточного року Кабінет Міністрів України дозволив українським державним установам у воєнний час користуватися хмарними технологіями з розміщенням даних у закордонних дата-центрах [267]. Реалізація розміщення даних у закордонних дата-центрах вимагає внесення

доповнень до закону України, що регулює надання хмарних послуг.

Доцільно доповнити статтю 14 «Захист інформації при наданні хмарних послуг та/або послуг центру обробки даних» Закону України «Про хмарні послуги» частиною 3 у редакції:

«Державний нагляд за дотриманням вимог з інформаційної безпеки хмарних послуг здійснюється центральним органом виконавчої влади зі спеціальним статусом у сферах електронних комунікацій, радіочастотного спектру та надання послуг поштового зв'язку. Предметом державного нагляду за дотриманням вимог з інформаційної безпеки є дотримання фізичними особами-підприємцями та юридичними особами обов'язкових вимог, встановлених цим законом, іншими законами та прийнятими відповідно до нормативно-правових актів у сфері інформаційної безпеки» (Додаток Е) [268].

З метою підвищення ефективності інфраструктури електронного уряду в Україні впроваджується єдина платформа цифрової взаємодії, що охоплює єдине програмно-апаратне середовище та методологію, яке підтримує взаємовідносини громадян, державних органів та юридичних осіб на базі сучасних інформаційних технологій. Розроблена концептуальна модель єдиної платформи цифрової взаємодії передбачає поетапний перехід державних інформаційних систем на вказану платформу та впровадження сервісної моделі надання інформаційних послуг в електронній формі, що посилить інформаційну безпеку у певному секторі інформаційного простору країни [269].

В опрацюванні правових актів у сфері інформаційної безпеки беруть участь державні органи та органи місцевого самоврядування. В умовах інформаційного суспільства та цифровізації ключове значення набуває трансформація зазначеної системи в загальнонаціональну систему інформаційної безпеки відповідно до принципів державно-приватного партнерства, що дозволить перейти на наступний рівень правової інформатизації на основі цифрових технологій з метою формування єдиного цифрового інформаційно-правового простору України.

Запровадження нових цифрових технологій, цифрової взаємодії потребує

пошуку нових концептуальних підходів і правових методів, механізмів публічного управління за обов'язкового дотримання вимог забезпечення інформаційної безпеки.

Цифрова трансформація впливає на механізми інформаційно-правової та електронної взаємодії між державою та суспільством, іншими суб'єктами інформаційного обміну, що відповідно вимагає адекватного забезпечення інформаційної безпеки.

Запит на розвиток інформаційної інфраструктури національної системи забезпечення інформаційної безпеки виходить із підвищення правової поінформованості та культури фізичних і юридичних осіб, а також необхідності забезпечення інформаційних потоків різних рівнів лінгвістичними, інформаційними засобами та інструментами, що забезпечують взаємодію громадян із державними інформаційними ресурсами.

Створення єдиного цифрового простору на платформній основі є перспективним, і в рамках реалізації зазначеного підходу можливий розвиток національної системи інформаційної безпеки на основі платформних рішень.

Водночас потрібні відповідні зміни у законодавстві та інтеграція сукупності публічних інформаційних ресурсів та сучасних цифрових технологій, спрямованих на забезпечення взаємодії всіх суб'єктів інформаційного обміну, інтеграція нормативного масиву інформаційної безпеки, що забезпечить її актуальний стан.

У сучасних умовах інформаційна безпека в інформаційному суспільстві набуває характеру стратегічного ресурсу; трансформуючись у систему цифровізації та публічного управління, вона дозволить публічним інформаційним системам перейти на платформне забезпечення та запровадити сучасні сервісні моделі інформаційних послуг на підставі нових правових і технологічних рішень у сфері забезпечення інформаційної безпеки.

Національна система інформаційної безпеки має розвиватися та набути офіційного статусу, бути інтегрованою, багаторівневою та відкритою для взаємодії з іншими інформаційними системами, а її інформаційно-правове

забезпечення будуватися на базі конвергентних інформаційних технологій та платформних рішень.

У зазначеному контексті важливо виділити необхідність забезпечення інформаційної безпеки особи та суспільства від деструктивного інформаційного впливу. Провідну роль у структурі цього інституту мають норми інформаційного права. Водночас усталені правові механізми безпеки вимагають подальшого розвитку та адаптації до нових загроз та викликів в умовах цифрової трансформації.

Аналіз інформаційного та іншого галузевого законодавства дозволив виділити такі основні правові механізми забезпечення інформаційної безпеки від деструктивного інформаційного впливу:

- встановлення правових заборон та інших обмежень на поширення певних видів негативної інформації;

- встановлення спеціальних правил обороту інформаційної продукції певних видів;

- закріплення обов'язків суб'єктів інформаційних правовідносин щодо забезпечення інформаційно-психологічної безпеки;

- вікова класифікація та маркування інформаційної продукції;

- експертиза інформаційної продукції;

- ідентифікація особи абонентів, користувачів мережі Інтернет та цифрових сервісів;

- видалення чи обмеження доступу до протиправного контенту;

- встановлення юридичної відповідальності за правопорушення, що посягають на інформаційно-психологічну безпеку;

- правове закріплення заходів контрпропаганди;

- правове стимулювання розвитку цифрової грамотності та формування культури інформаційної безпеки.

Важливу роль у механізмі правового забезпечення інформаційної безпеки відіграють заходи юридичної відповідальності за скоєння правопорушень у цій галузі, які закріплені кримінальним, адміністративно-деліктним і цивільним

законодавством. Водночас розширено практику нормативного закріплення санкцій за правопорушення у сфері захисту від деструктивного інформаційного впливу безпосередньо інформаційним законодавством.

Зазначені правові механізми демонструють доцільність розробки та прийняття окремого Закону України «Про захист від деструктивного інформаційного впливу на населення України».

3.2. Формування культури інформаційної безпеки

З кожним роком зростає потреба у забезпеченні інформаційної безпеки особи, держави та суспільства. Збільшення обсягів використання мережі Інтернет розширює масштаби інформаційних загроз, пов'язаних із діяльністю представників кіберзлочинності, розв'язуванням інформаційних воєн, комп'ютерними атаками хакерів на державні та приватні інформаційні ресурси, які є критично важливими для існування держави та суспільства.

Інша важлива небезпека використання мережі Інтернет у тому, що потужність формованого інформаційного потоку значно перевищує можливості освоєння та застосування інформації людьми. У сприйнятті світу зміщується акцент із наукового, освітнього та культурного на розважально-довідковий. Це формує кліпове мислення, що характеризується поверхневим сприйняттям інформації, падінням здібностей до аналізу, спрощенням поглядів та переваг людей, що сприяє формуванню нав'язаних моделей поведінки [270, с. 43].

Необхідно брати до уваги, що при сучасних темпах розвитку інформаційних технологій та інформаційного простору жоден управлінський апарат не в силах вчасно встановлювати необхідні механізми та адаптувати державне регулювання зазначеної сфери до обставин, що постійно змінюються. Цей факт призводить до необхідності забезпечення інформаційної безпеки.

При розгляді основних напрямів забезпечення інформаційної безпеки у різних галузях переважає необхідність забезпечення безпеки держави та суспільства. Інтереси особи та забезпечення інформаційної безпеки окремих

громадян розглядаються локально, причому як напрям забезпечення інформаційної безпеки в галузі науки, технологій та освіти, фігурує забезпечення захищеності громадян від інформаційних загроз, у тому числі шляхом формування культури особистої інформаційної безпеки.

В умовах посилення цифрової трансформації зростає значення адаптації громадян до нових реалій в умовах цифрового середовища, підвищення поінформованості та набуття навичок протистояння інформаційним загрозам та ризикам. Водночас в умовах інформаційної війни, яку проводить Російська Федерація, основна увага в державній політиці надається боротьбі з загрозами інформаційної безпеки. Це правильно, оскільки завдання держави полягає в тому, щоб максимально захистити особу та соціум від деструктивного впливу інформаційних ризиків.

Однак донині в експертній спільноті склалося розуміння того, що в інформаційному середовищі не можна уникнути будь-яких факторів, що утворюють загрози. Це зумовлено багатьма причинами: складністю виявлення загроз інформаційній безпеці, латентним характером дії, чисельністю джерел загроз інформаційній безпеці, обмеженою ефективністю методів припинення поширення деструктивної інформації.

Не можна забувати про те, що в правовій демократичній державі ступінь втручання в суспільне життя, у тому числі в духовну сферу, має бути лімітованим.

Спроби державного директивного нав’язування поглядів та цінностей, припинення будь-якого інакомислення несумісні з принципами демократичного устрою. Ці ідеї знайшли відображення в Конституції України, що закріплює принципи ідеологічного та політичного плюралізму, свободу думки, слова та інформації, гарантованість свободи масової інформації та допускає суворо лімітоване обмеження прав та свобод.

Слід наголосити, що поняття «культура особистої інформаційної безпеки» може мати широке тлумачення, яке не несе певної конкретики, оскільки його розшифрування в нормативних документах не відображено.

Культура особистої інформаційної безпеки – одна із складових загальної культури людини та її інформаційної культури. Культура охоплює сукупність інформаційного світогляду та системи спеціальних знань, що забезпечують самостійну діяльність із задоволення індивідуальних інформаційних потреб з використанням інформаційно-комунікаційних технологій та автоматизованих систем на принципах захищеності особистої інформації та підтримувальної інфраструктури від випадкових чи навмисних впливів природного чи штучного характеру, які можуть завдати збитків особі.

А. Ю. Геворкян зазначає, що спеціальні знання, вміння та навички – це здатність чітко усвідомлювати інформаційні потреби, з'ясовувати та проводити оцінку джерел інформації (мається на увазі процес виявлення найбільш достовірних, повних та оперативних джерел інформації), знаходити, аналізувати, організовувати, інтерпретувати, синтезувати інформацію, контролювати ефективність процесу задоволення інформаційних потреб [271, с. 172].

Для того, щоб сформувати культуру особистої інформаційної безпеки, необхідно коригувати систему формування світогляду, знань та умінь, пов'язаних із виробництвом, перетворенням, використанням та зберіганням інформації. Для формування культури особистої інформаційної безпеки доцільно:

- проводити заходи у галузі духовно-морального виховання громадян;

- формувати та розвивати правосвідомість громадян та відповідальне ставлення до використання інформаційних технологій, у тому числі споживчу та користувальницьку культуру;

- забезпечити створення та розвиток систем нормативно-правової, інформаційно-консультативної, технологічної та технічної допомоги у виявленні, попередженні, запобіганні та відображенні загроз інформаційній безпеці громадян та ліквідації наслідків прояву;

- удосконалювати механізми обмеження доступу до інформації, поширення якої в Україні заборонено законом, та її видалення;

- удосконалювати механізми законодавчого регулювання діяльності традиційних і нових засобів масової інформації (Інтернет,телебачення, соціальні мережі, вебсайти в мережі Інтернет, месенджери);

- забезпечити використання сучасних інформаційних платформ для поширення достовірної та якісної інформації, наповнення національного інформаційного простору доступними, якісними та легальними медіапродуктами та сервісами.

Зазначені заходи, які проводяться за допомогою апарату публічного управління, можуть допомогти сформувати культуру особистої інформаційної безпеки. Робота з її формування має вестися на всіх рівнях.

У зв'язку з цим потрібне посилення іншого магістрального спрямування забезпечення інформаційної безпеки – підвищення життєстійкості об'єктів інформаційної безпеки, їх здатність самостійно блокувати або знижувати до прийнятних значень деструктивний вплив загроз інформаційної безпеки. Це завдання можна позначити як формування інформаційного імунітету особистості та суспільства.

А. Ю. Геворкян запропонував комплексний проєкт формування сталої культури інформаційної безпеки українського суспільства, у якому зібрані всі основні аспекти та елементи системи інформаційної безпеки та наведено їх взаємозв'язок із головним завданням держави – зміцненням національної безпеки. Це три взаємопов'язані блоки для досягнення максимального ефекту від запровадження та реалізації: 1) теоретико-правові основи формування культури інформаційної безпеки суспільства; 2) визначення основних викликів і загроз інформаційній безпеці; 3) визначення короткострокових і стратегічних завдань державної політики в галузі формування культури інформаційної безпеки суспільства [271, с. 176].

У правових актах та науковій літературі цей напрям забезпечення безпеки зазвичай позначається як формування інформаційної грамотності та цифрової компетентності, культури інформаційної безпеки.

Проведення політики держави щодо підвищення цифрової та

інформаційної грамотності населення є важливим інструментом формування довіри суспільства до цифрових технологій. Це видно з соціологічного опитування науково-педагогічних працівників юридичних кафедр вищих навчальних закладів Львова (Додаток Ж).

Відповідні положення закріплені в документах стратегічного планування. У Стратегії інформаційної безпеки України та Національній економічній стратегії на період до 2030 року окреслено завдання формування культури особистої інформаційної безпеки.

Національна економічна стратегія на період до 2030 року закріплює, що для створення інформаційного простору знань потрібні розвиток правосвідомості громадян та відповідальне використання інформаційно-комунікаційних технологій.

У Концепції виховання дітей та молоді в цифровому просторі як базові засади державної політики названо: необхідність формування в дітей вміння орієнтуватися в сучасному інформаційному середовищі, виховання навичок самостійного та критичного мислення та навчання медіаграмотності [189; 272].

У 2002 році Генеральна асамблея ООН ухвалила резолюцію, присвячену створенню глобальної культури кібербезпеки «Утворення глобальної культури кібербезпеки». У преамбулі зазначається, що забезпечення кібербезпеки залежить не тільки від роботи правоохоронних структур, а й від превентивних заходів, обізнаності та відповідальності власників та користувачів інформаційно-комунікаційних технологій. Останні два аспекти закріплені серед елементів глобальної культури кібербезпеки у додатку до резолюції [273].

Аналіз правових актів Європейського Союзу у сфері забезпечення кібербезпеки, зокрема програми «Безпечний Інтернет», показав, що підвищення поінформованості дітей, батьків і педагогів щодо правил безпечного використання мережі виділялося як один із пріоритетних напрямів [274].

Ще до активного розвитку Інтернету, у європейських країнах за активної підтримки ЮНЕСКО сформувався специфічний напрям «медіа освіта» (media education), покликаний допомогти школярам та студентам краще адаптуватися

у світі медіакультури та спрямований на досягнення медіаграмотності (media literacy).

Медіаграмотність – це комплекс знань, навичок і вмінь, що дозволяють розуміти, аналізувати та критично оцінювати медіа та їхні сюжети та статті, визначається як грамотне використання інструментів, що забезпечують доступ до інформації, розвиток критичного аналізу змісту інформації та прищеплення комунікативних навичок [275].

З появою та зростанням популярності Інтернету дослідники почали говорити про «цифрову грамотність» як здатність критично розуміти та використовувати інформацію, одержувану за допомогою комп'ютера в різних форматах із широкого діапазону джерел. Цифрова грамотність – це наявність навичок, необхідних для життя, навчання і роботи в суспільстві, де спілкування і доступ до інформації здійснюється за допомогою цифрових технологій (інтернет-платформи, соціальні мережі, мобільні пристрої тощо) [276, с. 55].

Істотне зростання можливостей Інтернету та входження у повсякденне життя людини привели дослідників до акцентування уваги на понятті цифрової компетентності. Цифрова компетентність – здатність впевнено, ефективно, критично та безпечно обирати та застосовувати інформаційно-комунікаційні технології у різних сферах життєдіяльності (інформаційне середовище, комунікації, споживання, технічна сфера), готовність до такої діяльності.

За останні десятиліття в країні підготовлено комплекс наукових та методичних праць, присвячених формуванню інформаційної (медійної, цифрової) грамотності та культури інформаційної безпеки.

Виділяють чотири різновиди цифрової компетентності: інформаційна та медіакомпетентність, комунікативна, технічна та споживча компетентність. Методологічним підходом до формування культури інформаційної безпеки є цифрова (кібер) гігієна.

Як зазначається на вебсайті Міністерства та Комітету цифрової трансформації , цифрова гігієна – це грамотне споживання інформації, а також дотримання базових правил кібербезпеки: не використовувати один і той самий

пароль на всіх акаунтах, застосовувати двохфакторну ідентифікацію, регулярно здійснювати резервне копіювання та оновлення [277]. Експерти сформулювали правила кібергігієни, що охоплює безпечне зберігання паролів, використання багатофакторної автентифікації.

Для інформаційної безпеки більше значення мають правила цифрової гігієни: не видавати особистої інформації; не вірити та не довіряти незнайомцям; не викладати нічого важливого у хмару; бути уважним та усвідомленим; пам’ятати та дбати про майбутнє; розпізнавати маніпуляцію та маніпуляторів; дотримуватися розумної помірності; бути джерелом знань.

Аналізуючи зв’язок цифрової компетентності та зіткнення з онлайн ризиками, дослідники дійшли висновку про наявність прямої кореляції між ними. Чим частіше користувач зіштовхувався з онлайнризиками, тим вищий у нього рівень цифрової компетентності. Однак такий спосіб формування цифрової компетентності є небезпечним, оскільки може спричинити неприйнятну шкоду. Головне завдання полягає в навчанні дітей, батьків, вчителів та інших категорій громадян навичок та вмінь, які складають зміст цифрової грамотності (компетентності).

У цьому напрямі в Україні за останнє десятиліття виконано певну роботу. Проводяться виміри рівня цифрової обізнаності, запущено портал цифрової грамотності, у закладах освіти проводяться уроки кібербезпеки [278].

Міністерством цифрової трансформації України відповідно до Концепції розвитку цифрових компетентностей та плану заходів щодо її реалізації розроблені Рамки цифрової компетенції для громадян України [279; 280]. Це інструмент щодо покращення цифрової компетенції українців, спрямованих на підвищення цифрової грамотності та практичного використання сервісів ІТтехнологій конкретними групами населення.

Якщо говорити безпосередньо про Україну, то 53% громадян володіли цифровою грамотністю нижче за базовий рівень, за даними дослідження 2019 року. У 28% громадян вище за базовий рівень. Лише 11% українців можуть розпізнати неправдиву інформацію в Інтернеті [281].

В. Є. Іонан, заступник Міністра цифрової трансформації України з питань євроінтеграції, вказує, що багато хто, як і раніше, має недостатні знання та навички у сфері цифрових технологій. Цифрова грамотність населення у першій половині 2021 року оцінюється: ситуація з комунікацією та взаємодією у цифровому суспільстві: 27% на високому рівні, 69% на середньому рівні; з розв'язанням проблем у цифровій середовищі та навчанням протягом життя: 20% на високому рівні, 77% на середньому рівні. Навички безпеки у цифровій середовищі: лише 14% на високому рівні, 82% на середньому рівні. Ще гірша ситуація зі створенням цифрового контенту: лише 10% на високому рівні, 83% на середньому рівні [282].

Важливим напрямом роботи з формування культури інформаційної безпеки є стимулювання проєктів підвищення медійної та цифрової грамотності громадян. Робота в цій галузі ведеться різними громадськими організаціями національного та місцевого рівнів, причому нерідко з власної ініціативи. Потрібне подальше посилення державної підтримки цього напряму громадської активності.

Наказом Міністерства освіти і науки України затверджено Типову програму підвищення кваліфікації педагогічних працівників із розвитку цифрової компетентності, яка розроблена відповідно до сучасних вимог суспільства [283].

У 2019 році було запущено тематичний інтернет-портал «Цифрова грамотність». На місцевому рівні діють численні проєкти підвищення медійної та цифрової грамотності.

Крім освіти як основної форми підвищення цифрової грамотності та культури інформаційної безпеки, важливе значення має інформаційно-просвітницька робота. Вона спрямована на розвиток критичного мислення, підвищення поінформованості про загрози інформаційній безпеці (хибні новини, маніпуляцію свідомістю, шахрайство та ін.) та правила реагування на них. Формами ведення інформаційно-просвітницької роботи є створення та поширення тематичних інформаційних матеріалів (плакатів, пам'яток, роликів),

інтернет-ресурсів, проведення навчальних занять та інших профілактичних заходів.

Запит на здобуття знань про правила безпеки в цифровому середовищі є в суспільстві. Дослідження аналітичного центру Разумкова показало, що громадяни переймаються власною інформаційною безпекою. Більше половини опитаних хотіли б дізнатися про те, як краще захиститися від цифрових загроз та розвинути навички безпечного використання цифрових пристроїв та технологій, про інструменти особистої цифрової безпеки, люди відчувають інформаційний дефіцит [284]. Потрібна подальша активізація інформаційно-просвітницької роботи інститутів громадянського суспільства в розглянутій сфері за державної підтримки.

На сучасному етапі розвитку України немає можливості повністю позбавити людину інформаційних загроз або зменшити потік новин. Отже, необхідно вживати заходів забезпечення інформаційної безпеки. Використовувати варто не лише технічні методи, а й соціальні технології. Особливу увагу слід звернути на необхідність удосконалення освітньої системи, яка сьогодні не повною мірою відповідає вимогам інформаційного суспільства та захисту від деструктивного інформаційного впливу російського медіасередовища.

Виховання критичного мислення шляхом вивчення питань інформаційної безпеки дозволить уникнути руйнівних психологічних наслідків інформаційних воєн для особистості та дозволить уникнути маніпулятивних технологій російських політичних шахраїв, які активно ведуть діяльність у мережі Інтернет. Грамотний підхід до освіти дітей і молоді з питань інформаційної безпеки дозволить сформувати правильне ставлення до необхідності збереження цілісності, достовірності та доступності інформації, зробить внесок у формування культури особистої інформаційної безпеки, що дозволить успішно посісти своє місце в інформаційному суспільстві.

Висновки до розділу 3

У правовій системі України забезпечення інформаційної безпеки багато в чому забезпечує стабілізацію та ефективний розвиток національного інформаційного простору в умовах цифрової трансформації, що дає змогу забезпечити перехід від інформаційного суспільства до суспільства знань, в основі якого лежить забезпечення безпеки всіх інформаційних процесів.

Щодо цифрових технологій інформаційна безпека набуває особливого значення, є обов'язковою умовою забезпечення стану захищеності в цифровому середовищі, у різних інформаційних просторах, заснованих на цифрових даних; достовірності інформації, пов'язаної з функціонуванням системи органів публічної влади на різних цифрових платформах, наданням на їх основі адміністративних послуг.

Нормативно-правові акти, якими здійснюється регулювання інформаційної безпеки є специфічними техніко-юридичними правовими актами, але ця специфіка не береться до уваги суб'єктами нормотворчості.

Аналіз дозволив виділити низку напрямів розвитку законодавства у сфері забезпечення інформаційної безпеки: закріплення базових положень про інформаційну безпеку, у тому числі принципів інформаційної безпеки, прав та обов'язків, пов'язаних із забезпеченням інформаційної безпеки та інституту юридичної відповідальності; регулювання питань у сфері поширення відомостей, заборонених законодавством, регулювання забезпечення інформаційної безпеки у масових комунікаціях; забезпечення інформаційної безпеки в державних інформаційних системах та реєстрах; регулювання протидії поширенню фейкової інформації та дезінформації.

Удосконалення законодавства у сфері забезпечення інформаційної безпеки є юридичною діяльністю, спрямованою на покращення ефективності засобів і заходів інформаційної безпеки, що здійснюється різними способами в залежності від того аспекту, у якому напрямі інформаційного простору безпека є об'єктом удосконалення.

Для забезпечення інформаційної безпеки людини та суспільства недостатньо соціально-владного, службово-розпорядчого, охоронно-захисного та техніко-технологічного інструменталізму, а необхідне розуміння гуманітарного характеру цієї проблеми, що досягається узгодженням балансу інформаційних інтересів людини як особистості та громадянина, і інформаційних інтересів суспільства та держави, що відображається в культурі інформаційної безпеки. Культура інформаційної безпеки повинна бути зорієнтована на забезпечення інформаційної безпеки, яка становить серцевину державної інформаційної політики, є визначальним фактором забезпечення інформаційного суверенітету України та інформаційної підтримки територіальної цілісності та суверенітету, захисту особи та суспільства від деструктивного інформаційного впливу.

Проблема формування культури інформаційної безпеки особи та суспільства в умовах системних перетворень національної економіки, захисті територіальної цілісності як адекватної відповіді на виклики зовнішнього та внутрішнього інформаційного середовища набула безпосередньо практичного значення та гранично актуалізує суб’єктно-особистісний вимір. Адекватна відповідь на виклик інформаційного середовища залежить від стилю правового мислення громадянина, його ціннісних орієнтацій.

Аналіз динамічного розвитку загроз у сфері деструктивного інформаційно-психологічного впливу на особу та суспільство вимагає нових засобів забезпечення інформаційної безпеки, у зв’язку з чим існує об’єктивна необхідність продовження досліджень різних аспектів формування культури інформаційної безпеки як основного засобу протидії деструктивним впливам.

Планомірне, систематичне та послідовне удосконалення діяльності щодо розвитку культури інформаційної безпеки на засадах національних інтересів потребує упорядкування нормативної бази цього важливого самостійного постійного напряму діяльності, яка сьогодні є хаотичною та суперечливою. Цей процес набув характеру гострої проблеми, яка вимагає невідкладного вирішення.

ВИСНОВКИ

Протягом десятиліття в Україні відбулися масштабні соціальні перетворення, які зумовили розвиток євроатлантичного напряму, що викликало спротив імперських сил на теренах колишньої російської імперії. Це призвело до озброєного втручання у 2014 році та військової агресії Російської Федерації у 2022 році.

Одним з аспектів захисту територіальної цілісності, суверенітету та національної економіки в умовах цифрової трансформації є забезпечення інформаційної безпеки. Діяльність щодо забезпечення інформаційної безпеки громадян, суспільства та держави, будучи формально спрямованою на реалізацію відповідного права осіб, є необхідною складовою механізму державного управління в умовах воєнного стану, бо сприяє збору, аналізу та узагальненню інформації про деструктивний інформаційний вплив агресора та заходи щодо протидії цьому впливу. Це вкрай важливо для ухвалення державних рішень у цій галузі та підготовки відповідних нормативно-правових актів. Результати проведеного дисертаційного дослідження дозволили дійти до таких висновків, направлених на вирішення наукової проблеми адміністративно-правового забезпечення інформаційної безпеки в умовах цифрової трансформації та воєнного стану.

1. Методологічною основою дослідження адміністративно-правового забезпечення інформаційної безпеки є міждисциплінарний підхід, який дає можливість осмислити цілеспрямовану активність особи, суспільства та держави в інформаційному просторі як єдність мети, правових засобів забезпечення, свідомо-вольової активності суб’єктів у процесі реалізації. Це дозволило зібрати окремі положення та висновки, які дають уявлення про забезпечення інформаційної безпеки особи, суспільства та держави в єдину сукупність і сформулювати засновані на емпіричному та теоретичному матеріалі методологічні засади дослідження адміністративно-правового забезпечення інформаційної безпеки в умовах цифрової трансформації.

Засноване на застосуванні методології системно-функціонального підходу з урахуванням розвитку правової науки та інформаційно-комунікаційних технологій адміністративно-правове забезпечення інформаційної безпеки визначається як система теоретичних поглядів і вихідних наукових положень, виражених у категоріально-понятійному апараті теорії права, інформаційного і адміністративного права, розкриваючи сутність, зміст, функції, методи та форми прояву, рівні та види впливу на суспільні відносини за допомогою адміністративно-правових засобів у національному інформаційному просторі, у тому числі у соціальних мережах, Інтернеті тощо.

Побудова теоретичної системи, що цілісно відтворює сутнісні сторони адміністративно-правового забезпечення інформаційної безпеки заснована на емпіричному матеріалі правозастосовної практики та на формуванні загальнотеоретичної та галузевої наукової бази, що сприяє виробленню на підставі міждисциплінарної методології напрямів вирішення проблеми забезпечення інформаційної безпеки в умовах збройної агресії Російської Федерації.

Висунення нових методологічних підходів, що відображають складний процес функціонування адміністративно-правового забезпечення інформаційної безпеки зумовили перехід до аналізу чинників, утворених новітніми інформаційними технологіями у конкретних сферах суспільних відносин в Інтернеті, соціальних мережах, мережевих (нових) засобах масової комунікації.

2. Характеризуючи систему правового забезпечення інформаційної безпеки в умовах цифрової трансформації, доцільно зазначити міжгалузевий характер і складну внутрішню структуру (охоплює конституційно-правові, адміністративно-правові, інформаційно-правові, цивільно-правові, кримінально-правові, міжнародно-правові елементи та взаємозв’язки між ними), що перебуває в динамічному розвитку. Взаємопов’язаними вимірами правового регулювання забезпечення інформаційної безпеки є ціннісний, нормативно-правовий, функціональний та інституційний. Ціннісний вимір забезпечення інформаційної безпеки вказує, що зазначений правовий феномен

перебуває у складних системних зв'язках із конституційними цінностями та слугує забезпеченню суспільно корисних цілей – гарантованості й захищеності людини, суспільства та держави. Нормативно-правовий вимір передбачає фіксацію на законодавчому рівні адміністративно-правових засобів і механізмів, їх основних видів, підстав і особливостей застосування. Функціональний вимір вказує, що нормативне закріплення інформаційної безпеки сприяє реалізації низки суспільно важливих функцій: поновлення права, компенсаторної, правоохоронної, каральної, виховної.

Міжгалузевий характер інституту правового забезпечення інформаційної безпеки охоплює взаємопов'язану сукупність інформаційно-правових та інших галузевих норм, що регулюють відносини у сфері забезпечення інформаційної безпеки. Базове значення у структурі цього інституту мають норми інформаційного та адміністративного права, які закріплені в Законах України «Про інформацію», «Про захист суспільної моралі», «Про санкції», «Про захист інформації в інформаційно-комунікаційних системах», «Про електронні комунікації». Механізм правового забезпечення інформаційної безпеки має низку недоліків. Найажливішим із них є відсутність правового закріплення відправних засад та принципів забезпечення інформаційної безпеки, які не дозволяють набути даному механізму повноцінної системності правового регулювання.

3. Інституціоналізація інформаційної безпеки в інформаційному праві розвивається відповідно до темпів розвитку інформаційно-комунікаційних технологій, підпорядковується водночас логіці інституційної динаміки, закладеної в минулому. Інституціоналізація інформаційної безпеки – це процес виділення, становлення, формування, розвитку та закріплення інститутів і їх коригування, направлених на забезпечення захисту особи, суспільства та держави від деструктивного інформаційного впливу. В інституційному вимірі забезпечення інформаційної безпеки в умовах цифрової трансформації означає створення певного механізму, що складається з сукупності національних і міжнародних інституцій, які здатні захистити особу та суспільство від

деструктивного інформаційного впливу, забезпечити належний захист інформації. Інституціоналізація характеризує систему інформаційної безпеки з реальною та об’єктивною конкретизацією та раціональним співвідношенням статики та динаміки, окремі аспекти забезпечення в оф-лайн та он-лайн-інформаційних середовищах, як-от: засоби масової інформації, інформаційно-комунікаційні мережі, охоплюючи мережу Інтернет, інші форми розповсюдження інформації. Прерогативою інформаційного права є регламентація питань протидії поширенню протиправної інформації у засобах масової інформації та мережі Інтернет. Водночас інформаційно-правове регулювання не вичерпує всієї предметної галузі забезпечення інформаційної безпеки. Тому правову основу інформаційної безпеки становлять норми інших галузей права, охоплюючи конституційне, адміністративне, кримінальне, цивільне.

Основними проблемами інституціоналізації забезпечення інформаційної безпеки в Україні є: відсутність належної конкретизації на рівні спеціальних законів, наприклад, щодо інформаційного забезпечення діяльності збройних сил, правоохоронних і інших державних органів; недостатність адміністративно-правового забезпечення інформаційної безпеки у частині блокування та видалення протиправного контенту відомчими нормативними актами; незабезпеченість матеріально-правових норм належним рівнем процесуального законодавства; відсутність нормативно-правового захисту дітей від деструктивного інформаційного впливу.

4. Адміністративно-правове забезпечення інформаційної безпеки – це врегульована нормами адміністративного права державно-управлінська діяльність публічних органів влади та посадових осіб з виявлення деструктивного інформаційного впливу на інформацію у контексті її захисту, особу, суспільство та державу, запобігання розповсюдженню шляхом блокування або видалення, що здійснюється на основі застосування відповідних адміністративно-правових заходів. Адміністративно-правові засоби запобігання інформаційної безпеки – це способи адміністративно-правового

впливу держави на осіб, які здійснюють інформаційну діяльність щодо запобігання правопорушенням в інформаційному просторі України. Механізм адміністративно-правового регулювання у сфері забезпечення інформаційної безпеки – юридично закріплена, організована система адміністративно-правових засобів, що становить нормативно-правову, інституційну та інструментальну основу для досягнення відповідно до певних юридичних процедур цілей у галузі забезпечення стану захищеності інформації, особи, суспільства та держави та національних інтересів від можливого деструктивного інформаційного впливу їх наслідків.

Аналіз інформаційного та галузевого законодавства дозволив виділити основні адміністративно-правові механізми забезпечення інформаційної безпеки: встановлення правових заборон та інших обмежень на поширення певних видів негативної інформації; встановлення спеціальних правил обігу інформаційної продукції певних видів; закріплення обов'язків суб'єктів інформаційних правовідносин щодо забезпечення інформаційної безпеки; експертиза інформаційної продукції; ідентифікація особи абонентів, користувачів мережі Інтернет та цифрових сервісів; видалення чи обмеження доступу до протиправного контенту; встановлення юридичної відповідальності за правопорушення, що посягають на інформаційно-психологічну безпеку; правове закріплення заходів контрпропаганди; правове стимулювання розвитку цифрової грамотності та формування культури інформаційної безпеки.

Важливу роль у механізмі правового забезпечення інформаційної безпеки відіграють заходи юридичної відповідальності за скоєння правопорушень у цій галузі, які закріплені кримінальним, адміністративно-деліктним і цивільним законодавством. Водночас розширено практику нормативного закріплення санкцій за правопорушення у сфері інформаційної безпеки безпосередньо інформаційним законодавством щодо блокування та видалення.

Закладені в законодавстві правові механізми забезпечення інформаційної безпеки потребують подальшого розвитку та адаптації до нових викликів та загроз в умовах цифрової трансформації та інформаційного протиборства в

умовах правового режиму воєнного стану.

5. Правові обмеження в інформаційному праві у діяльності засобів масової інформації відіграють правоохоронну функцію. Юридична конструкція правових обмежень в інформаційному праві охоплює: регулятивну норму, яка має бути забезпечена охоронною нормою, що встановлює юридичну відповідальність за порушення заборон та невиконання обов'язків; матеріальну норму, яка забезпечується процесуальною, встановлюючи процедуру реалізації та застосування матеріального права; правовий акт, де викладені правові обмеження, що відповідають специфіці суспільних відносин, стосовно яких воно встановлюється. Основними цілями інституту правових обмежень в інформаційному праві є: захист публічних інтересів (забезпечення державної, воєнної та інформаційної безпеки, охорона публічного порядку, здоров'я, моралі); захист приватних інтересів; стримування протиправної або небажаної поведінки суб'єктів інформаційної діяльності; регулювання суспільних відносин в інформаційному просторі у специфічних умовах режимів військового та надзвичайного стану; виявлення негативних правових наслідків щодо обмеження прав громадян у зв'язку із застосуванням заходів процесуального примусу. Застосування правових обмежень у діяльності засобів масової інформації зумовлені механізмом інформаційного впливу. Механізм інформаційного впливу засобів на особу, соціальні групи та суспільство має складний, багатоаспектний характер. Вплив, територіальний масштаб та кількісне охоплення аудиторії засобів масової інформації обумовлені комплексом факторів, охоплюючи вид засобів, характер контенту, особливості цільової групи аудиторії, фактори зовнішнього мікро та макросоціального середовища. Це вимагає максимальної гнучкості правового регулювання з обов'язковим урахуванням конкретної специфіки регламентованого аспекту забезпечення інформаційної безпеки у засобах масової інформації, включаючи «нові медіа» – інтернет-сайти та соціальні медіа. У межах наказового, заборонного режиму, встановленого інститутом правових обмежень в інформаційному праві, виділено: заборону; юридичний обов'язок; зупинення;

ценз; заходи примусу.

6. Специфіка мережі Інтернет зумовлює правове регулювання інформаційної безпеки. В Інтернеті представлено коло осіб, які безпосередньо пов'язані із забезпеченням інформаційної безпеки: громадяни, які є користувачами; технічні суб'єкти, дії яких спрямовані на забезпечення роботи Інтернету; бізнес, громадянське суспільство, зацікавлені в розширенні можливостей; державні суб'єкти до завдань яких належить правове регулювання відносин в Інтернеті; міжнародні організації – координація питань, розробка технічних і правових стандартів, пов'язаних з Інтернетом.

Для забезпечення інформаційної безпеки першої та другої групи осіб необхідно надати правовий вплив на відносини, які пов'язані: зі створенням, функціонуванням та розвитком інфраструктури Інтернету; із забезпеченням безпеки особи, суспільства та держави від деструктивного інформаційного впливу; із забезпеченням реалізації прав громадян під час використання цифрових технологій в Інтернеті. Перелік не може обмежуватися зазначеними відносинами. З розвитком інфраструктури буде розвиватися та доповнюватися. В Інтернеті можемо спостерігати різні суспільні зв'язки, які спрямовані на задоволення інтересів і потреб та мають бути захищені засобами інформаційної безпеки. Забезпечення інформаційної безпеки в Інтернеті в умовах збройної агресії Росії вимагає: забезпечити регулювання інформаційної безпеки в Інтернеті на якісно новому рівні, який спиратиметься на стандарти Європейського Союзу і НАТО, на науково обґрунтовані дані, що дозволить оцінити ефективність захисту національного інформаційного простору. Регулювання таких відносин повинно будуватися на нормах галузевого законодавства, технічно-правових, охоронних, регулятивних, міжнародних засобах, які складуть ефективний механізм правового регулювання інформаційної безпеки в Інтернеті.

7. Правове регулювання юридичної відповідальності за порушення інформаційної безпеки у межах спеціальних законів, що обумовлюють запровадження та дію відповідних правових механізмів, не є завершеним і

системним, що пояснюється концептуальною неопрацьованістю питань покладення юридичної відповідальності у сфері інформаційного права. Залежно від специфіки правового механізму, юридична відповідальність у сфері інформаційної безпеки має бути істотно специфікована. Принциповою особливістю юридичної відповідальності щодо інформаційної безпеки є її підвищений (за обсягом) строковий (обмежений у часі) характер, домінування компенсаторної та охоронної функції.

Стрімкий розвиток процесів цифровізації в Україні потребує переосмислення відповідальності у сфері інформаційної безпеки. Це зумовлено інституційними зрушеннями в процесі європейської інтеграції та суттєвим розширенням деструктивного інформаційного впливу та заходів направлених на знищення державних інформаційних ресурсів країною агресором – Російською Федерацією. Рівень захищеності особи, суспільства та держави від деструктивного інформаційного впливу та інформації залежить не лише від цифровізації суспільних відносин та спроможності держави, але й від правової урегульованості означених процесів.

З метою уникнення використання інформації для підриву територіальної цілісності та суверенітету України, нав’язування ідеології сепаратизму і «єдності російського і українського народів» потребують істотного розширення межі подальшої правової специфікації юридичної відповідальності за порушення у сфері інформаційної безпеки.

8. Правове вдосконалення інституту адміністративно-правового забезпечення інформаційної безпеки в Україні має спиратися на чітку правову основу й новітні доктринально-правові напрацювання; передбачати процесуальне закріплення відповідних матеріальних норм, доповнення їх належними гарантіями та санкціями юридичної відповідальності за порушення; забезпечувати поєднання загальнодержавних, суспільних та індивідуальних інтересів. Належне унормування відповідного кола суспільних відносин покликане сприяти усуненню поширення інформації, яка потенційно може загрожувати державі, суспільству, правам і свободам людини.

Зволікання з вирішенням проблеми належного адміністративно-правового унормування забезпечення інформаційної безпеки не сприятиме оптимальному й ефективному виконанню органами публічної адміністрації зобов'язань із захисту громадян від деструктивного інформаційного впливу.

Важливими напрямами вдосконалення законодавства України щодо адміністративно-правового забезпечення інформаційної безпеки в Україні доцільно вважати: внесення змін до законів України, які регулюють суспільні відносини щодо забезпечення інформаційної безпеки у контексті рішень Європейського Суду з прав людини; законодавчу деталізацію й розмежування порядку виконання рішень щодо блокування або видалення відповідного контенту; запровадження спеціальних процедур ефективного контролю за виконанням рішень уповноважених органів щодо блокування або видалення протиправного контенту.

Важливою складовою правового забезпечення інформаційної безпеки особи та суспільства, які значною мірою визначають інформаційну безпеку держави, є необхідність формування культури інформаційної безпеки. Культура інформаційної безпеки – це сукупність певних знань, умінь, навичок та високий рівень правосвідомості особистості в інформаційній сфері. До знань, умінь та навичок у сфері інформаційної безпеки належать: здатність забезпечувати безпечну реалізацію інтересів в інформаційній сфері, усвідомлення національних інформаційних пріоритетів та інтересів, сформоване вміння визначати загрози інформаційній безпеці, оцінювати ризики, сформовані вміння та навички протистояння можливим загрозам в інформаційній сфері.

З метою формування культури інформаційної безпеки особистості та суспільства за умов цифрової трансформації необхідно розробити документи планування; правове просвітництво, охоплюючи питання відповідальності за правопорушення в інформаційній сфері; визначення викликів і загроз інформаційній безпеці; постановку короткострокових та довгострокових завдань, що охоплють активне залучення до цього процесу установ освіти та культури, інститутів громадянського суспільства; розвиток механізмів

саморегулювання користувачів засобів масової комунікації, соціальних мереж та інших можливостей інформаційних технологій та систем.

Висновки та рекомендації, сформульовані в дисертаційній роботі, доповнюють теоретичні положення інформаційного права у сфері, що розглядається, можуть бути основою для подальших досліджень проблеми забезпечення інформаційної безпеки, сприяти вдосконаленню інформаційного законодавства та обґрунтуванню впливу на інші галузі правового регулювання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Онопрієнко С. Г. Методологічні засади дослідження інформаційної безпеки у науці права національної безпеки та військового права. *Аналітично-порівняльне правознавство*. 2021. № 4. С. 185-188.

2. Молодецька-Гринчук К. В. Методологія побудови системи забезпечення інформаційної безпеки держави у соціальних Інтернет-сервісах: автореф. дис. … д-ра технічних наук: спец.: 21.05.01. Київ, 2018. 42 с.

3. Перун Т. С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні: дис. … канд. юрид. наук: спец.: 12.00.07. Львів, 2019. 268 с.

4. Авер'янов В. Б. Вибрані наукові праці / Упорядники: Андрійко О. Ф., Нагребельний В. П., Кисіль Л. Є. і інші. За заг. ред.: Ю. С. Шемшученка, О. Ф. Андрійко. Київ: Інститут держави і права імені В. М. Корецького НАН України, 2011. 448 с.

5. Арістова В. І., Сулацький Д. В. Інформаційна безпека людини як споживача телекомунікаційних послуг: монографія. Київ: Право України, 2013. 184 с.

6. Архипова Є. О. Інформаційна безпека: соціально-філософський вимір: автореф. дис. ... канд. філософських наук: спец.: 09.00.03. Київ, 2012. 16 с.

7. Баранов О. А. Правове забезпечення інформаційної сфери: теорія, методологія і практика. Київ: Едельвейс, 2014. 497 с.

8. Бурячок В. Л., Толюпа С. В., Семко А. А. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: посібник. Київ: ДУТ-КНУ, 2016. 178 с.

9. Біленська Д. О. Адміністративно-правове регулювання інформаційних відносин в Україні: автореф. дис. … канд. юрид. наук: спец. 12.00.07. Харків, 2016. 23 с.

10. Довгань О. Д., Ткачук Т. Ю. Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс.

Інформація і право. 2018. № 2 (25). С. 73-85.

11. Доронін І. М. Національна безпека України в інформаційну епоху: теоретико-правове дослідження: дис. …д-ра юрид. наук: 12.00.01. Київ, 2020. 539 с.

12. Малашко О. Є., Єсімов С. С. Нормативно-правове забезпечення інформаційної безпеки в Україні. *Міжнародний науковий журнал «Інтернаука»*. 2020. № 14 (94). Т. 2. С. 30–38.

13. Малашко О. Є., Єсімов С. С. Зміст державної діяльності із забезпечення інформаційної безпеки. *Міжнародний науковий журнал «Інтернаука»*. 2020. № 15 (95). Т. 1. С. 46-54.

14. Золотар О. О. Інформаційна безпека людини:теорія і практика: Монографія. Київ: ТОВ «Видавничий дім «АртЕк», 2018. 446 с.

15. Коваленко Л. П. Інформаційне право України: проблеми становлення та розвитку: автореф. дис. ... д-ра юрид. наук: спец.: 12.00.07. Харків, 2014. 37 с.

16. Ковалів М., Єсімов С., Скриньковський Р. і інші. Розвиток цифрової економіки в контексті забезпечення інформаційної безпеки в Україні. *Traektoriâ Nauki = Path of Science*. 2020. Vol. 6. № 5. S. 2023-2032.

17. Ліпкан В. А., Максименко Ю. С., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції. Київ: .КТН, 2006. 280 с.

18. Мукомела І. В. Правові засади інформаційного суспільства: загальнотеоретичний аналіз: автореф. дис. … канд. юрид. наук: спец. 12.00.01. Харків, 2016. 23 с.

19. Рибальський О. В., Хахановський В. Г., Кудінов В. А. Основи інформаційної безпеки та технічного захисту інформації. Київ: Видавництво НАВС, 2012. 104 с.

20. Сопілко І. М. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. *Юридичний вісник. Повітряне і космічне право*. 2021. № 2. С. 110-115.

21. Селезньова О. М. Теоретико-методологічні засади інформаційного права України як інтегрованої категорії: автореф. дис. … д-ра юрид. наук:

спец.: 12.00.07. Київ, 2015. 40 с.

22. Тихомиров О. О. Забезпечення інформаційної безпеки як функція сучасної держави. Київ: Видавництво НА СБ України, 2014. 196 с.

23. Ткаченко В. В. Адаптація інформаційного законодавства України до міжнародних правових стандартів в умовах розвитку інформаційного суспільства : автореф. дис. ... канд. юрид. наук: спец.: 12.00.07. Київ, 2014. 22 с.

24. Ткачук Т. Ю. правове забезпечення інформаційної безпеки в умовах євроінтеграції України: дис. … д-ра юрид. наук: спец.: 12.00.07. Ужгород, 2019. 487 с.

25. Турчак А. В. Механізми забезпечення інформаційної безпеки як складової державної безпеки України: автореф. … канд. наук державного управління, спец.: 25.00.02. Київ, 2020. 23 с.

26. Ситар І. М. Предмет порівняльного правознавства (методологічний плюралізм). *Держава і право. Юридичні і політичні науки*. 2014. Випуск. 64. С. 42-51.

27. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 р. «Про Стратегію національної безпеки України»: Указ Президента України від 14.09.2020 р. № 392/2020. URL. https://zakon.rada.gov.ua/laws/show/392/2020#Text

28. Про національну безпеку України: Закон України від 21.06.2018 р. № 2496-VIII. URL. https://zakon.rada.gov.ua/laws/card/2469-19

29. Богуцький П. П. Концептуальні засади права національної безпеки України. Київ; Одеса: Фенікс, 2020. 374 с.

30. Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 р. «Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України»: Указ Президента України від 06.12.2001 р. № 1193/2001. URL. https://zakon.rada.gov.ua/laws/card/1193/2001

31. Горбенко І, Потій О., Черних С., Прокоф’єв М. Системний аналіз переходу від концепції національної інформаційної політики до доктрини

інформаційної безпеки України. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2002. Випуск 5. С. 12-26.

32. Про рішення Ради національної безпеки і оборони України від 21 березня 2008 р. «Про невідкладні заходи щодо забезпечення інформаційної безпеки України»: Указ Президента України від 23.04.2008 р. № 377/2008. URL. https://zakon.rada.gov.ua/laws/card/377/2008

33. Про Доктрину інформаційної безпеки України: Указ Президента України від 08.07.2009 р. № 514/2009. URL. https://zakon.rada.gov.ua/laws/card/514/2009

34. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. «Про скасування деяких рішень Ради національної безпеки і оборони України» та визнання такими, що втратили чинність, деяких указів Президента України: Указ Президента України від 06.06.2014 р. № 504/2014. URL. https://zakon.rada.gov.ua/laws/show/504/2014#Text

35. Про Заяву Верховної Ради України «Про відсіч збройній агресії Російської Федерації та подолання її наслідків»: Постанова Верховної Ради України від 21.04.2015 р. № 337-VIII. URL. https://zakon.rada.gov.ua/laws/show/337-19#Text

36. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 р. «Про Доктрину інформаційної безпеки України»:Указ Президента України від 25.02.2017 р. № 47/2017. URL. https://zakon.rada.gov.ua/laws/card/47/2017

37. Про інформацію: Закон України від 02.10.1992 р. № 2657. URL. https://zakon.rada.gov.ua/laws/card/2657-12

38. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 р. № 80/94. URL. https://zakon.rada.gov.ua/laws/card/80/94-вр

39. Про внесення змін до деяких законодавчих актів України у зв’язку з прийняттям Закону України «Про інформацію» та Закону України «Про доступ до публічної інформації»: Закон України від 27.03.2014 р. № 1174-VII. URL.

https://zakon.rada.gov.ua/laws/card/1170-18

40. Єсімов С. С. Шляхи удосконалення нормативно-правового регулювання в сфері інформаційної безпеки. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична*. 2013. № 4. С. 144-150.

41. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України: дис. … д-ра юрид. наук: спец. 12.00.07. Одеса, 2004. 427 с.

42. Калюжний Р. А., Цимбалюк В. С. Координація діяльності органів влади у боротьбі з організованою кіберзлочинністю. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2002. № 6. С. 105-111.

43. Інформаційна безпека: навчальний посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник і інші; за заг. ред. Ю. Я. Бобала та І. В. Горбатого. Львів: Видавництво Львівської політехніки, 2019. 580 с.

44. Інформаційна безпека. IT-словник. URL. http://xn--r1a3b.xn--b1amgblet.xn-j1amh/index.php/

45. Розробка проєкту Концепції кодифікації інформаційного законодавства України. *Інформація і право*. 2012. № 1. URL. http://ippi.org.ua/vid-redaktsiinoi-kolegii-rozrobka-proektu-kontseptsii-kodifikatsii-informatsiinogo-zakonodavstva-ukr

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

47. Про схвалення Стратегії розвитку інформаційного суспільства в Україні: Розпорядження Кабінету Міністрів України від 15.05.2013 р. № 386-р. URL. https://www.kmu.gov.ua/npas/246420577

48. Про державну таємницю: Закон України від 21.01.1994 р. № 3855-XII. URL. https://zakon.rada.gov.ua/laws/card/3855-12

49. Деякі питання об’єктів критичної інформаційної інфраструктури: Постанова Кабінету Міністрів України від 09.10.2020 р. № 943. URL.https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text

50. Про захист суспільної моралі: Закон України від 20.11.2003 р. № 1296-IV. URL. https://zakon.rada.gov.ua/laws/card/1296-15

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

52. Брыжко В. М., С. Цимбалюк В. С., Орехов А. А,, Гальченко О. Н. Е-будущее и информационное право. Київ: Интеграл, 2002. 264 с.

53. Основи інформаційного права України. навчальний посібник / В. С. Цимбалюк, В. Д. Гавловський, В. В. Гриценко та ін.; за ред. М. Я. Швеця, Р. А. Калюжного, П. В. Мельника. Київ: Знання, 2004. 274 с.

54. Психологічна безпека особистості: міжнародна колективна монографія / Університет Григорія Сковороди в Переяславі; Брестський державний університет ім. О. С. Пушкіна; за заг. ред. І. В. Волженцевої. Переяслав (Київська обл.): Домбровської Я. М.; Брест: БрДУ, 2021. 890 с.

55. Філіпенко А. С. Міждисциплінарна методологія: базові принципи. *International relations, part «Economic sciences».* 2018. № 13. С. 7-13.

56. Корж І. Безпека: медотологічні підходи до поняття. *National law journal: theory and practice*. 2019. August. P. 68-72.

57. Проєкт Закону України «Про засади інформаційної безпеки України». URL. http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=51123

58. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 р. «Про Стратегію інформаційної безпеки»: Указ Президента України від 28.12.2021 р. № 685/2021. URL. https://zakon.rada.gov.ua/laws/show/685/2021#Text

59. Бойченко В. П. Кримінально-правова охорона суспільної моралі в Україні: антропологічний вимір: дис. … канд. юрид. наук: спец.: 12.00.08. Одеса, 2021. 230 с.

60. Кримінальний кодекс України: Закон України від 05.04.2001 р. № 2341-III. URL. https://zakon.rada.gov.ua/laws/card/2341-14

61. Кодекс України про адміністративні правопорушення: Закон України від 07.12.1984 р. № 8073-X. URL. https://zakon.rada.gov.ua/laws/card/80731-10

62. Кузьменко Т. М. Сутнісні характеристики та класифікація соціальних груп: референтна група: види та функції. *Актуальні проблеми соціології, психології, педагогіки.* 2013. Випуск 18. С. 64-77. URL. https://sociology.knu.ua/sites/default/files/library/elopen/aktprob.18.64.pdf

63. Психіка: поняття, класифікація та система. URL. https://osvita.ua/vnz/reports/psychology/29184/

64. Соціальна психологія: навчальний посібник / Н. Ю. Волянюк, Г. В. Ложкін, О. В. Винославська, І. О. Блохіна, М. О. Кононець, О. В. Москаленко, О. І. Боковець, Б. В. Андрійцев. Київ: КПІ ім. Ігоря Сікорського, 2019. 254 с.

65. Столяренко О. Б. Психологія особистості. Навчальний посібник. Київ: Центр учбової літератури, 2012. 280 с.

66. Основи соціальної психології: підручник / П. П. Горностай, М. М. Слюсаревський, В. О. Татенко, Т. М. Титаренко, Н. В. Хазратова та ін.; за ред. М. М. Слюсаревського. Київ: Талком, 2018. 580 с.

67. Даниленко С., Фурсей О. Деструктивний інформаційний вплив на соціально-політичні процеси (на прикладі Франції). *Вісник Київського національного університету імені Тараса Шевченка.* 2020. № 1 (51). С. 25-30.

68. Національна безпека: світоглядні та теоретико-методологічні засади: монографія / за заг. ред. О. П. Дзьобаня. Харків: Право, 2021. 776 с.

69. Квіткін П., Дятлова І., Петрова Л. Інформаційна безпека особистості: теоретико-методологічний аналіз. *Вісник НЮУ імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія*. 2021. Том 4 (51). С. 46-62.

70. Окінавська хартія глобального інформаційного суспільства. URL. https://zakon.rada.gov.ua/laws/show/998_163#Text

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

72. Гончаров М. В. Тенденції наукових поглядів у сфері нормативно-правового забезпечення інформаційної безпеки України. *Науковий вісник Ужгородського Національного Університету.* 2022. Випуск 70. С. 24-27.

73. Шопіна І. М. Поняття інформаційної безпеки: концептуальні підходи до визначення. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького*. *Серія Право*. 2022. № 13 (25). С. 133-140.

74. Баран М. В. Суб'єкти забезпечення інформаційної безпеки в Україні. *Юридичний науковий електронний журнал.* 2022. № 6. С. 220-223.

75. Про основи національної безпеки: Закон України від 19.06.2003 р. № 964-IV. URL. https://zakon.rada.gov.ua/laws/card/964-15

76. Куц. О. В. Концепція інформаційної екології у дослідженні бібліотек. Матеріали XX ювілейної міжнародної науково-практичної конференції (Київ, 19-20.05.2021 р.). URL. https://repo.knmu.edu.ua/bitstream/123456789/28665/1/%D0%9A%D1%83%D1%86_%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%20%D0%B5%D0%BA%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%8F.pdf

77. Баранов О. А. Правове забезпечення інформаційної сфери: теорія, методологія і практика:монографія. Київ: Едельвейс, 2014. 434 с.

78. Лізинчук В. Інформаційна безпека України: теорія і практика. Львів: ЛНУ, 2017. 728 с.

79. Інформаційна безпека: проблеми приватного права; за ред. Є. О. Харитонова та І. В. Давидової. Одеса: Фенікс, 2020. 194 с.

80. Інформаційна безпека: підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; за ред. В. В. Остроухова. Київ: Видавництво Ліра-К, 2021. 412 с.

81. Ковалів М. В., Єсімов С. С., Хмиз М. В., Кайдрович Х. І., Князь С. В. Проблеми та перспективи забезпечення інформаційної безпеки в органах прокуратури України. *Міжнародний науковий журнал «Інтернаука». Серія: «Юридичні науки».* 2021. № 7. С. 100-106.

82. Сопільник Л., Скриньковський Р, Ковалів М., Заяць Р. і інші Особливості правового забезпечення інформаційної безпеки при використанні хмарних технологій органами державної влади. *Traektoriâ Nauki = Path of*

Science. 2020. Vol. 6. № 6. S. 5006-5013.

83. Тетарчук І., Дяків Т. Теорія держави і права. Навчальний посібник. Київ. Центр навчальної літератури, 2020. 184 с.

84. Баран М. Механізм адміністративно-правового регулювання інформаційної безпеки. *Visegrad journal on human rights*. 2021. № 4. С. 25-30.

85. Заяць Н. Сутнісна характеристика правових засобів у механізмі правового регулювання. *Підприємництво, господарство і право.* 2016. № 12. С. 202-205.

86. Вакарюк Л. В. Правові засоби як складова частина правового режиму з позиції інструментальної теорії права. *Науковий вісник Ужгородського національного університету.* 2018. Випуск 48. Том 1. С. 15-18.

87. Гетьманцева Н., Митрицька Г. Правові засоби в механізмі правового регулювання суспільних відносин у сфері найманої праці. *Підприємництво, господарство і право.* 2021. № 3. С. 132-140.

88. Про Національну стратегію у сфері прав людини: Указ Президента України від 24.03.2021 р. № 119/2021. URL.https://zakon.rada.gov.ua/laws/card/119/2021

89. Про схвалення Довгострокової стратегії розвитку української культури – стратегії реформ: Розпорядження Кабінету Міністрів України від 01.02.2016 р. № 119-р. URL. https://www.kmu.gov.ua/npas/248862610

90. Проєкт Закону України «Про Національну програму інформатизації» від 01.11.2021 р. № 6241. URL. http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=73095

91. Про боротьбу з тероризмом: Закон України від 20.03.2003 р. № 638-IV. URL. https://zakon.rada.gov.ua/laws/card/638-15

92. Про запобігання корупції: Закон України від 14.10.2014 р. № 1700-VII. URL. https://zakon.rada.gov.ua/laws/card/1700-18

93. Риндюк В. І. Системність як властивість змісту законодавства. *Київський часопис права*. 2022. № 1. С. 45-51.

94. Адміністративне право України. Академічний курс: підручник: у 2 т.:

Т. 1. Загальна частина / ред. кол.: В. Б. Авер'янов (голова) та ін. Київ: Юридична думка, 2004. 592 с.

95. Белікова Т. В. Методи виявлення деструктивного інформаційно-психологічного впливу для інформаційних технологій забезпечення безпеки підлітків: дис. … канд. техн. наук: спец.: 05.13.06. Черкаси, 2019. 223 с.

96. Маркова М. В., Марков А. Р. Інформаційно-психологічна війна як нова загроза здоров'ю населення України: реальність небезпеки та напрями протидії. 2016. URL. https://health-ua.com/article/5219-nformatcjnopsihologchna-vjna-yak-nova-zagroza-zdorovyu-naselennya-ukrani-re

97. Бараннік В. В., Сідченко С. О., Белікова Т. В., Олійник Ю. О. Метод виявлення деструктивно інформаційно-психологічного впливу на підсвідомість особового складу та населення України. URL. https://www.researchgate.net/publication/338650565_Metod_viavlenna_destruktivno_informacijnopsihologicnogo_vplivu_na_pidsvidomist_osobovogo_skladu_ta_naselenna_Ukraini

98. Хворост Х. Ю. Інформаційно-психологічний вплив у розрізі безпеки здоров'я. 2016. URL. https://evnuir.vnu.edu.ua/bitstream/123456789/10713/14/33.pdf

99. Деструктивний вплив засобів масової інформації на суспільну і особистісну свідомість та поведінку молоді. 2021. URL. http://il.ippi.org.ua/article/view/254346

100. Про внесення змін до деяких законів України щодо заборони виготовлення та поширення інформаційної продукції, спрямованої на пропагування дій держави-агресора: Закон України від 03.03.2022 р. № 2109-IX. URL. https://zakon.rada.gov.ua/laws/show/2109-20#Text

101. Петренко Л. В. Системний підхід в правовій інформатиці. *Моделювання та інформаційні системи в економіці*. Київ: КНЕУ, 2019. Випуск 97. С. 164-174.

102. Петренко Л. В., Петренко А. В. Психологічні умови формування «цифрових» компетенцій майбутніх фахівців. *Цифрова економіка*. Київ: КНЕУ,

2018. С. 290-293.

103. Про затвердження Указу Президента України «Про введення воєнного стану в Україні»: Закон України від 24.02.2022 р. № 2102-IX. URL. https://zakon.rada.gov.ua/laws/show/2102-20#Text

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

105. Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції: Закон України від 03.03.2022 р. № 2110-IX. URL. https://zakon.rada.gov.ua/laws/show/2110-20#Text

106. Про стимулювання розвитку цифрової економіки в Україні: Закон України від 15.07.2021 р. № 1667-IX. URL. https://zakon.rada.gov.ua/laws/show/1667-20#Text

107. Про затвердження Національної економічної стратегії на період до 2030 року: Постанова Кабінету Міністрів України від 03.03.2021 р. № 179. URL. https://zakon.rada.gov.ua/laws/show/179-2021-%D0%BF#n25

108. Мороз Г. В. Інституціоналізація інтересів у контексті забезпечення екологічної функції держави. *Часопис Київського університету права*. 2020. № 1. С. 270-273.

109. Словник Глосарій із законопроєктування. Центр законопроектних студій. URL. http://lawdrafting.org/glossary/

110. Адамова О. С. Визначення поняття інституту права. URL. http://dspace.onua.edu.ua/bitstream/handle/11300/2595/Adamova%20Viznachennya.pdf?sequence=1&isAllowed=y

111. Теорія держави та права: навчальний посібник / Є. В. Білозьоров, В. П. Власенко, О. Б. Горова, А. М. Завальний, Н. В. Заяць та ін.; за заг. ред. С. Д. Гусарєва, О. Д. Тихомирова. Київ: НАВС, Освіта України, 2017. 320 с.

112. Мироненко І. В. Інститут права сусідства: теоретичні та практичні засади правового регулювання земельних сусідських відносин: автореф. дис. ... д-ра юрид. наук: спец.:12.00.06. Харків, 2020. 46 с.

113. Лавриненко О. О. Міжгалузеві інститути в системі права України. URL. https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/21310/1/%D0%9C%D1%96%D0%%D1%96%20%D0%BF%D1%80%D0%B0%D0%B2%D0%B0.pdf

114. Велика українська юридична енциклопедія. Том 3. Загальна теорія права; за ред. О. В. Петришина. Харків: Право, 2017. 948 с.

115. Драгомерецький М. М. Міжгалузеві інститути права: правова природа та підходи до розуміння. *Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція*. 2021. № 53. С. 21-25.

116. Левицька Н. О. Міжгалузеві нормативно-правові інститути: деякі теоретичні питання. *Науковий вісник міжнародного гуманітарного університету. Серія: юриспруденція*. 2015. № 14. Том. 1. С. 22-24.

117. Правова доктрина України: у 5 т. Т. 2: Публічно-правова доктрина України / Ю. П. Битяк, Ю. Г. Барабаш, М. П. Кучерявенко та ін. ; за заг. ред. Ю. П. Битяка. Харків: Право, 2013. 864 с.

118. Баранов О. А. Інститути інформаційного права. *Правова інформатика*. 2006. № 3 (11). С. 39-45.

119. Ярема О. Г., Єсімов С. С. Предмет правового забезпечення інформаційної безпеки в інформаційному праві. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична.* 2016. Випуск 2. С. 244-252.

120. Енциклопедія соціогуманітарної інформології / координатор проекту та заг. ред. К. І. Бєляков. Одеса: Видавничий дім «Гельветика», 2021. Т. 2. 436 с.

121. Про друковані засоби масової інформації (пресу) в Україні: Закон України від 16.11.1992 р. № 2782-XII. URL. https://zakon.rada.gov.ua/laws/show/2782-12#Text

122. Про телебачення і радіомовлення: Закон України від 21.12.1993 р. № 3759-XII. URL. https://zakon.rada.gov.ua/laws/card/3759-12

123. Про інформаційні агентства: Закон України від 28.02.1995 р. № 74/95-ВР. URL. https://zakon.rada.gov.ua/laws/card/74/95-%D0%B2%D1%80

124. Про Суспільне телебачення: Закон України від 17.04.2014 р. № 1227-

VII. URL. https://zakon.rada.gov.ua/laws/card/1227-18

125. Про затвердження Положення про Національний реєстр електронних інформаційних ресурсів: Постанова Кабінету Міністрів України від 17.03.2004 р. № 326. URL. https://zakon.rada.gov.ua/laws/show/326-2004-%D0%BF#Text

126. Про рекламу: Закон України від 03.07.1996 р. № 270/96-ВР. URL. https://zakon.rada.gov.ua/laws/card/270/96-%D0%B2%D1%80

127. Конституція України: Закон України від 28.06.1996 р. № 254к/96-ВР. URL. https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%Text

128. Державний стандарт України. ДСТУ ISO / IEC27001: 2010 Інформаційна технології. практичні правила управлінні інформаційною безпекою. Вимоги. ISO / IEC27001: 2005 ІДТ. URL. http://online.budstandart.com/ua/catalog/doc-page?id_doc=68935

128. Про комітети Верховної Ради України: Закон України від 04.04.1995 р. № 116/95-ВР. URL. https://zakon.rada.gov.ua/laws/card/116/95-%D0%B2%D1%80

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

130. Про Конституційний Суд України: Закон України від 13.07.2017 р. № 2136-VIII. URL. https://zakon.rada.gov.ua/laws/show/2136-19#Text

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

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

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

134. Питання Міністерства цифрової трансформації: Постанова Кабінету Міністрів України від 18.09.2019 р. № 856. URL.

https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text

135. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 р. № 3475-IV. URL. https://zakon.rada.gov.ua/laws/card/3475-15

136. Про Національну стратегію сприяння розвитку громадянського суспільства в Україні на 2021-2026 роки: Указ Президента України від 27.09.2021 р. № 487/2021. URL. https://zakon.rada.gov.ua/laws/show/487/2021#Text

137. Муравська (Якубівська) Ю. Є. Інформаційна безпека суспільства: концептуальний аналіз. *Економіка та суспільство. Електронне наукове фахове видання.* 2017. № 9. URL. http://dspace.wunu.edu.ua/bitstream/316497/19378/1/%d0%9c%d1%83%d1%80%d0%b0%d0%b2%d1%81%d1%8c%d0%ba%d0%b0%28%d0%af%d0%ba%d1%83%d0%b1%d1%96%d0%b2%d1%81%d1%8c%d0%ba%d0%b0%29_%d0%a1%d1%82%d0%b0%d1%82%d1%82%d1%8f.pdf

138. Ломачинська І., Ломачинський Б. Роль інформаційної культури у регулюванні соціальних інформаційних систем. *Вісник Львівського університету. Серія філософсько-політологічні студії.* 2020. Випуск 29. С. 90-97.

139. Виборчий кодекс України: Закон України від 19.12.2019 р. № 396-IX. URL. https://zakon.rada.gov.ua/laws/card/396-20

140. Про всеукраїнський референдум: Закон України від 19.12.2019 р. № 1135-IX. URL. https://zakon.rada.gov.ua/laws/show/1135-20#Text

141. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 р. № 2135-XII. URL. https://zakon.rada.gov.ua/laws/card/2135-12

142. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 р. № 4651-VI. URL. https://zakon.rada.gov.ua/laws/show/4651-17#Text

143. Цивільний кодекс України: Закон України від 16.01.2003 р. № 435-IV. URL. https://zakon.rada.gov.ua/laws/card/435-15

144. Про основні засади забезпечення кібербезпеки України: Закон

України від 05.10.2017 р. № 2163-VIII. URL. https://zakon.rada.gov.ua/laws/card/2163-19

145. Сопільник Л. І., Сопільник Р. Л., Ковалів М. В., Єсімов С. С., Технічне регулювання в системі права України. *Наукові записки Львівського університету бізнесу і права.* 2020. № 25. С. 149-155.

146. Довгань Б., Міхайліна Т. Цифрові права людини четвертого покоління крізь призму трансгуманізму. *Підприємництво, господарство і право*. 2021. № 1. С. 171-175.

147. Павленко Ж. О. Право в цифровій реальності. *Вісник НЮУ імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія*. 2021. № 2 (49). С. 66-80.

148. Соскін О. Цифровізація як нова реальність України. 2022. URL. https://lexinform.com.ua/dumka-eksperta/tsyfrovizatsiya-yak-nova-realnist-ukrayiny/

149. Андреєв А. Механізм правового регулювання суспільних відносин: окремі аспекти щодо визначення поняття та особливостей. *Підприємництво, господарство і право.* 2019. № 6. С. 125-128.

150. Тарахонич Т. І. Механізм дії права, механізм правового регулювання, механізм реалізації права: особливості взаємодії. *Держава і право*. 2010. Випуск 50. С. 12-18.

151. Адміністративне право України. Академічний курс: підручник: У двох томах: Том 1. Загальна частина / Редакційна колегія: В. Б. Авер'янов (голова). Київ: Видавництво «Юридична думка», 2004. 584 с.

152. Баранов О. Методи інформаційного права. *Правова інформатика*. 2007. № 4 (16). С. 8-12.

153. Про телекомунікації: Закон України від 18.11.2003 р. № 1280-IV. URL. https://zakon.rada.gov.ua/laws/card/1280-15

154. Бурмагін О. О., Онишко Л. В. Судова практика про поширення інформації в Інтернеті: тенденції та проблеми правозастосовної діяльності. Київ: ГО «Платформа прав людини», 2020. 49 с.

155. Волошин О. Як захистити дітей та не заблокувати Інтернет в

Україні? Жовтень 2021. URL. https://dslua.org/wp-content/uploads/2021/10/Taking-Down-Content-Harmful-for Children_final_OCT21-1.pdf

156. Чемодурова А. Правове регулювання та його ефективність у сучасному світі. *Підприємництво, господарство і право*. 2020. № 4. С. 262-267.

157. Ящишен А. Заборонено поширювати інформацію про українських військових: що загрожуватиме порушникам. 25 березня 2022 р. URL. https://ye.ua/cruminal/58327_Zaboroneno_poshiryivati_informaciyi_pro_ukrayinskih_viyskovih__scho_zagrozhuvatime_porushnikam.html

158. Про внесення змін до статті 114^{-2} Кримінального кодексу України щодо удосконалення відповідальності за несанкціоноване розповсюдження інформації про засоби протидії збройній агресії Російської Федерації: Закон України від 01.04.2022 р. № 2178-IX. URL. https://zakon.rada.gov.ua/laws/show/2178-20#Text

159. Про санкції: Закон України від 14.08.2014 р. № 1644-VII. URL. https://zakon.rada.gov.ua/laws/show/1644-18#Text

160. Про рішення Ради національної безпеки і оборони України від 18 червня 2021 року «Про застосування, скасування і внесення змін до персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»: Указ Президента України від 24.06.2021 року № 265/2021. URL. https://www.president.gov.ua/documents/2652021-39265

161. Про рішення Ради національної безпеки і оборони України від 18 червня 2021 року «Про застосування, скасування і внесення змін до персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»:Указ Президента України від 24.06.2021 р. № 266/2021. URL. https://www.president.gov.ua/documents/2662022-42225

162. Судові рішення і судова практика щодо блокування Інтернет-ресурсів, Укрінформ. 02.08.2022. URL. https://www.ukrinform.ua/rubric-presshall/3256058-sudovi-risenna-i-sudova-praktika-sodo-blokuvanna-internetresursiv.html

163. Дворовий М. Санкції та блокування веб-сайтів в Україні: як непомітно відкрити скриньку Пандори. Аналітичний звіт. Київ: ГО «Лабораторія цифрової безпеки», 2021. 43 с.

164. За допомогою Телеграм-ботів кіберполіції вдалося заблокувати понад 3 тисячі ворожих Інтернет-ресурсів, – Ігор Клименко. Національна поліція України, 02 червня 2022 року. URL. https://www.kmu.gov.ua/news/za-dopomogoyu-telegram-botiv-kiberpoliciyi-vdalosya-zablokuvati-ponad-3-tisyachi-vorozhih-internet-resursiv-igor-klimenko

165. Невельська-Гордєєва О. П., Нечитайло В. О. Феномен «fakenews» у контексті забезпечення інформаційної безпеки держави. *Вісник Національного юридичного університету імені Ярослава Мудрого.* 2022. № 1 (52). С. 123-135.

166. Володовська В. Регулювання онлайн-медіа: роз'яснення ключових положень доопрацьованого законопроекту «Про медіа». 09 липня 2020 року. URL. https://detector.media/rinok/article/178630/2020-07-09-regulyuvannya-onlayn-media-rozyasnennya-klyuchovykh-polozhen-doopratsovanogo-zakonoproektu-pro-media/

167. Проєкт Закону України «Про медіа» від 27.12.2019 р. № 2693. URL. http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67812

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

169. Як у сучасних умовах вибудувати систему інформаційної протидії. 02.08.2022. URL. https://defence-ua.com/army_and_war/jak_u_suchasnih_umovah_vibuduvati_sistemu_informatsijnoji_protidiji-404.html

170. Директива Європейського Парламенту і Ради (ЄС) 2016/1148 від 06 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу. URL. https://zakon.rada.gov.ua/laws/show/984_013-16

171. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on

information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance). URL. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0881

172. Баран М. Проблеми забезпечення інформаційної безпеки особи в адміністративному процесі. *Проблеми розвитку адміністративного, фінансового та інформаційного права в контексті євроінтеграційних процесів*: збірник. тез міжнародної науково-практичної конференції (м. Львів, 3 червня 2022 р.). Київ: Комп'ютерний дизайн, 2022. С. 27-30.

173. Баран М. Захист прав людини в умовах розвитку цифрових технологій і формування інформаційної безпеки. *Теоретико-прикладні проблеми правового регулювання в Україні:* матеріали V Всеукраїнської науково-практичної конференції (м. Львів, 10 грудня 2021 р.) / за заг. ред. І. В. Красницького. Львів : Львівський державний університет внутрішніх справ, 2021. С. 11-16.

174. Баран М. В. Інформаційно-правова специфіка соціалізації військовослужбовців в аспекті інформаційної безпеки. *Проблеми розвитку адміністративного, фінансового та інформаційного права в контексті євроінтеграційних процесів:* збірник тез міжнародної науково-практичної конференції (м. Львів,15 квітня 2021 р.). Київ ПП «Комп'ютерний дизайн», 2021. С. 18-20.

175. Баран М. Аналіз комунікативної діяльності людини в інформаційному просторі в контексті інформаційної безпеки. *Теоретико-прикладні проблеми правового регулювання в Україні:* матеріали Всеукраїнської науково-практичної конференції (м. Львів, 11 грудня 2020 р.) / за заг. ред. І. В. Красницького. Львів: ЛьвДУВС, 2020. С. 20-24.

176. Проєкт Концепції та плану заходів з розвитку цифрових прав дітей. URL. https://thedigital.gov.ua/storage/uploads/files/%D0%9F%D1%80%D0%BE%D1%94%D0%BA%D1%82%20%D0%B0%D0%BA%D1%82%D0%B0.pdf

177. Топчий О. В. Адміністративно-правове забезпечення інформаційної безпеки неповнолітніх в Україні: автореф. дис. … д-ра юрид. наук: спец.:

12.00.07. Ужгород, 2019. 40 с.

178. Про внесення змін до деяких законодавчих актів України щодо імплементації Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства (Ланцаротської конвенції): Закон України від 18.02.2022 р. № 1256-IX. URL. https://zakon.rada.gov.ua/laws/show/1256-20#n38

179. Про затвердження критеріїв віднесення продукції до такої, що має порнографічний характер: Наказ Міністерства культури України від 16.03.2018 р. № 212. URL. https://zakon.rada.gov.ua/laws/show/z0393-18#n13

180. Нестеренко А. О. Адміністративно-правове забезпечення прав дітей в інформаційному середовищі: дис. … д-ра філософії: спец.: 081. Львів, 2021. 213 с.

181. Лесько Н. В. Правові засади попередження медіа насильства щодо дітей. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького.* 2022. № 13 (25). С. 98-105.

182. Про внесення змін до Закону України «Про захист суспільної моралі» щодо захисту прав та найкращих інтересів дитини»: Закон України від 15.02.2022 р. № 2047-IX. URL.https://zakon.rada.gov.ua/laws/show/2047-20#Text

183. Робота із соціальними мережами. Посібник з питань використання соціальних мереж, розроблений Департаментом преси і публічної інформації Консультативної місії ЄС в Україні. Київ: EUAM, 2020. 47 с.

184. Про схвалення Рекомендацій щодо вікової класифікації інформаційної продукції: Рішення Національної експертної комісії України з питань захисту суспільної моралі від 05.09.2013 р. № 60. URL. https://zakon.rada.gov.ua/rada/show/vr060623-13#Text

185. Про судову експертизу: Закон України від 25.02.1994 р. № 4038-XII. URL. https://zakon.rada.gov.ua/laws/card/4038-12

186. Про затвердження Положення про Департамент кіберполіції Національної поліції України: Наказ Національної поліції України від 10.11.2015 р. № 85. URL. http://tranzit.ltd.ua/nakaz

187. Про електронні довірчі послуги: Закон України від 05.10.2017 р. № 2155-VIII. URL. https://zakon.rada.gov.ua/laws/card/2155-19

188. Про затвердження Положення про інтегровану систему електронної ідентифікації: Постанова Кабінету Міністрів України від 19.06.2019 р. № 546. URL. https://zakon.rada.gov.ua/laws/show/546-2019-%D0%BF#Text

189. Проєкт Концепції виховання дітей та молоді в цифровому просторі. Київ: Національна академія педагогічних наук України, 2021. 52 с.

190. Деякі питання цифрової трансформації: Розпорядження Кабінету Міністрів України від 17.02.2021 р. № 365-р. URL. https://zakon.rada.gov.ua/laws/show/365-2021-%D1%80#Text

191. Захарченко В. К. інституційний вимір інформаційної безпеки України: трансформаційні виклики, глобальні контексти, стратегічні орієнтири: дис. … д-ра політичних наук: спец. 23.00.02. Київ, 2021. 423 с.

192. Вінник О. Цифровізація в ракурсі державної економіко-правової політики. *Підприємництво, господарство і право*. 2020. № 8. С. 61-70.

193. Чорна В. Г. Відносини адміністративно-правових обмежень. *Науковий вісник Ужгородського національного університету*. *Серія: право*. 2018. Випуск. 51. Том 2. С. 55-57.

194. Остапенко О. Про заборони та обмеження в адміністративному праві. *Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки.* 2018. № 894. С. 51-59.

195. Адміністративне право України (загальна частина): навчальний посібник / Остапенко О. І. Ковалів М. В., Єсімов С. С. та ін.; Вид. 2-е, доповнене. Львів: СПОЛОМ, 2021. 616 с.

196. Ткаля О. Розуміння адміністративно-правового впливу. *Підприємництво, господарство і право*. 2016. № 12. С. 157-163.

197. Семенюк О. Г., Леонов Б. Д. Правовий режим доступу до інформації. *Інформація і право*. 2019. № 3 (30). С. 44-49.

198. Ткачук Н. І. Інформаційні права і свободи людини і громадянина в Україні: визначення термінів, співвідношення понять. *Інформація і право*. 2018.

№ 2. (25). С. 17-30.

199. Межі та доповнення. Втручання. Конституційний Суд України. URL. https://ccu.gov.ua/storinka-knygy/412-mezhi-ta-obmezhennya-vtruchannya

200. Солодка О. М. Інформаційний простір держави як сфера реалізації інформаційного суверенітету. *Інформація і право.* 2020. № 4 (35). С. 39-46.

201. Довідник з українського медіа-ландшафту / Березень 2022 року. URL. https://static1.squarespace.com/static/60996b757eb6521a42f3839d/t/624e021032c19857144a7ec7/1649279506406/Ukraine-Media-Landscape-Guide_UK-CDAC.pdf

202. Мак-Квейл Д. Теорія масової комунікації / пер. з англ. Львів: Вид-во «Літопис», 2010. 538 с.

203. Пахнін М. Л. Засоби масової комунікації та засоби масової інформації: співвідношення понять. *Юридичний бюлетень*. 2018. Випуск 8. С. 65-71.

204. Центр О. Разумкова. URL. https://razumkov.org.ua/napriamky/sotsiologichni-doslidzhennia?start=40

205. Центр соціального моніторингу. URL. https://smc.org.ua/pro-kompaniyu/

206. Про заборону пропаганди російського нацистського тоталітарного режиму, збройної агресії Російської Федерації як держави-терориста проти України, символіки воєнного вторгнення російського нацистського тоталітарного режиму в Україну: Закон України від 22.05.2022 р.№ 2265-IX. URL. https://zakon.rada.gov.ua/laws/show/2265-20#Text

207. Квіт С. Масові комунікації. Київ: Видавництво Києво-Могилянська академія, 2018. 352 с.

208. Баран М. В. Адміністративні форми та методи забезпечення інформаційної безпеки у Збройних Силах в умовах воєнного стану. *Конституційні права і свободи людини та громадянина в умовах воєнного стану:*матеріали наукового семінару (м. Львів, 23 червня 2022 р.). Львів: ЛьвДУВС, 2022. С. 24-27.

209. Баран М. В. Конституційне право особи на свободу отримання і поширення інформації у контексті забезпечення інформаційної безпеки. *Сучасний конституціоналізм: проблеми теорії та практики:* матеріали наукового семінару (м. Львів, 25 червня 2021 р.). Львів: ЛьвДУВС, 2021. С. 11-15.

210. Інтернет. Словник іноземних слів. URL. https://www.jnsm.com.ua/cgi-bin/u/book/sis.pl?Qry=%B2%ED%F2%E5%F0%ED%E5%F2

211. RFC is also an abbreviation for Remote Function Call. URL. https://www.techtarget.com/whatis/definition/Request-for-Comments-RFC

212. Глуха Т. До питання особливостей правового регулювання відносин в мережі Інтернет. *Правова система України в умовах європейської інтеграції : погляд студентської молоді*: Збірник тез IV Міжнародної наукової конференції (м. Тернопіль, 15 травня 2020 р.). Тернопіль: ТНЕУ, 2020. С. 161-163.

213. Бортник Н., Єсімов С. Відносини в мережі Інтернет як об’єкт правового регулювання. *Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки*. 2019. Випуск 22. С. 147-153.

214. Тонкощі мережевого етикету – секрети грамотної дискусії. 01.08.2021. URL. https://vcf.vn.ua/tonkoshhi-merezhevogo-etiketu-sekreti-gramotno%D1%97-diskusi%D1%97/

215. Правила безпечної поведінки в Інтернеті. URL. http://gplyceum.org.ua/%D0%BF%D1%80%D0%B0%D0%B2%D0%B8%D0%BB%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%BD%D0%BE%D1%97

216. Інтернет Асоціація України. URL. https://inau.ua/pro-asotsiatsiyu/basedoc/statut-internet-asotsiatsiyi-ukrayiny

217. Василина Н. В. Перспективи впровадження онлайн-урегулювання спорів в Україні. *Науковий вісник Ужгородського національного університету, Серія Прав*о. 2019. Випуск 55. Том 1. С. 114-117.

218. Разумов Д. Мережевий етикет – що це? Особливості інтернет етикету. 20 листопада 2019 р.. URL. https://aboutmarketing.info/internet-marketynh/netiquette/

219. Саморегулювання у мережі Інтернет на прикладі віртуальних організацій Grid. URL https://ndipzir.org.ua/wp-content/uploads/2017/07/Yefremova/4_4.pdf

220. Данильян О.Г., Дзьобань О. П. Віртуальна реальність і кіберпростір як атрибути сучасного суспільства. *Інформація і право*. 2020. № 4 (35). С. 9-20.

221. Основи медіа бізнесу: підручник / З. В. Григорова, О. А. Сухорукова, А. В. Кваско, Л. П. Шендерівська. Київ: КПІ ім. Ігоря Сікорського, 2021. 323 с.

222. Key Internet Statistics to Know in 2022 (Including Mobile). URL. https://www.broadbandsearch.net/blog/internet-statistics

223. Про авторське право і суміжні права: Закон України від 23.12.1993 р. № 3792-XII. URL. https://zakon.rada.gov.ua/laws/card/3792-12

224. З яких соцмереж українці отримують інформацію? Опитування. 15.02.2022. URL. https://life.pravda.com.ua/society/2022/02/15/247467/

225. Половинчак Ю. Особливості інтерактивного простору соціальних медіа в контексті реалізації маніпулятивних технологій. 2018. URL. https://ipiend.gov.ua/wp-content/uploads/2018/07/polovynchak_osoblyvosti.pdf

226. Бакуменко О. Які пошукові системи популярні в світі та Україні? Рейтинг 2021 року. 01.07.2021. URL.https://web-promo.ua/ua/blog/kakie-poiskovye-sistemy-populyarny-v-mire-i-ukraine-rejting-2021-goda/#rejting-poiskovyh-sistem-v-ukraine

227. Авдєєва Т. Відповідність блокування соціальних мереж європейським стандартам свободи вираження поглядів. 29.11.2021. URL. https://cedem.org.ua/analytics/social-media-blocking/

228. Нагорна А. Кращі безкоштовні анонімайзери: VPN, онлайн, браузери. Для тих, кому важлива приватність. 25.01.2022. URL.https://dev.ua/news/best-free-anonymizers-vpn

229. Що таке розумний натовп? 21.09.2020. URL. https://uaeu.top/tsikave/shcho-take-rozumnij-natovp.html

230 Stop Russia Channel | MRIYA. 08.08.2022. URL. https://t.me/+pBBz4EnKJVs5OWI6

231. Радутний О. Е. Ілюзія та реальність інформаційного суверенітету. *Інформація і право.* 2020. № 4 (35). С. 22-38.

232. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології: монографія / І. В. Арістова, О. А. Баранов, О. П. Дзьобань і ін.; за заг. ред. К. І. Бєлякова. Київ: КВІЦ, 2019. 344 с.

233. Заярний О. А. Адміністративна деліктологія в інформаційній сфері: проблеми теорії та практики: дис. … д-ра юрид. наук: спец.: 12.00.07. Київ, 2018. 561 с.

234. Юридична відповідальність за правопорушення в інформаційній сфері: теорія і практика. Монографія / Кол. авторів; За заг. ред. К. І. Бєлякова. Київ: 2016. 293 с.

235. Тихомиров О. О., Тугарова О. К. Юридична відповідальність за правопорушення в інформаційній сфері: навчальний посібник. Київ: Національна академія СБУ, 2015. 172 с.

236. Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України: монографія. Луганськ: РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. 528 с.

237. Сопільник Р. Л., Єсімов С. С., Ковалів М. В., Скриньковський Р. М. Юридична відповідальність у механізмі забезпечення режиму інформації з обмеженим доступом в Україні: адміністративно-правовий вимір. *Право. ua.* 2019. № 2. С. 19-26.

238. Копійка М. В. Стратегічні ризики інформаційної безпеки європейських країн. *Міжнародні та політичні дослідження*. 2019. Випуск 32. С.85-102.

239. Доктрина з інформаційної безпеки. 14 липня 2021 року. URL. https://www.promoteukraine.org/uk/doktryna-z-informaczijnoyi-bezpeky/

240. Остапенко О. І., Баїк О. В. Адміністративно-правова природа інформаційної безпеки. *Вісник Національного університету «Львівська політехніка». Серія: Юридичні науки*. 2021. № 3 (31). С. 167-179.

241. Пєтков С. В. До питання про види юридичної відповідальності в контексті зміни державотворчих парадигм. *Вісник університету імені Альфреда Нобеля. Серія «право»*. 2021. № 1 (2). С. 119-124.

242. Бакумов О. С. Інституціоналізація відповідальності держави: теоретичні та конституційно-правові аспекти: автореф. дис. … д-ра юрид. наук: спец:12.00.01; 12.00.02. Київ, 2021. 42 с.

243. Водовський В. Кіберзлочинність в України: найпоширеніші злочини та як громадянам подбати про власну інформаційну безпеку. 09.01.2021. URL. https://equity.law/press-center/publications/1169.html

244. Собко Г. М. Психічне насильство: кримінологічні та кримінально-правові засади протидії. Київ: Видавництво: Гельветика, 2020. 484 с.

245. Войтюк Т. Що таке «треш-стріми» та як з ними боротися. Розповідає експерт. ·9 червня 2021 року. URL. https://suspilne.media/137786-so-take-tres-strimi-ta-ak-z-nimi-borotisa-rozpovidae-ekspert/

246. Глибокі фейки є більш небезпечною технологією, ніж маніпуляція – німецький експерт. 23 січня 2020 року. URL. https://www.ukrinform.ua/rubric-world/2861208-gliboki-fejki-e-bils-nebezpecnou-tehnologiu-niz-manipulacia-nimeckij-ekspert.html

247. Що таке фішинг і як від нього захиститись? URL. https://www.fg.gov.ua/articles/50140-shcho-take-fishing-i-yak-vid-nogo-zahistitis.html

248. Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану»: Закон України від 24.03.2022 р. № 2160-IX. URL. https://zakon.rada.gov.ua/laws/show/2160-20#Text

249. Про внесення змін до статті 114-2 Кримінального кодексу України

щодо удосконалення відповідальності за несанкціоноване розповсюдження інформації про засоби протидії збройній агресії Російської Федерації: Закон України від 01.04.2022 р. № 2178-IX. URL. https://zakon.rada.gov.ua/laws/show/2178-20#Text

250. Батиргареєва В. С. Правова платформа для забезпечення в Україні ефективного захисту цифрових трансформацій суспільства. *Інформація і право.* 2022. № 1 (40). С. 21-34.

251. Петков С. В., Армаш Н. О., Соболь Є. Ю. Адміністративна деліктологія: сучасна модель відповідальності посадових осіб органів публічної влади. Київ: ЦУЛ, 2020. 153 с.

252. Сторожук І. П. Інформаційне правопорушення як підстава адміністративної відповідальності. *Прикарпатський юридичний вісник*. 2020. Випуск 3 (32). С. 65-69.

253. Давидова І., Гарган Є. Відшкодування шкоди, завданої за порушення інформаційної безпеки. *Дніпровський науковий часопис публічного управління, психології, права*. 2022. № 1. С. 93-97.

254. Про критичну інфраструктуру: Закон України від 16.11.2021 р. №1882-IX. URL. https://zakon.rada.gov.ua/laws/show/1882-20/conv#n410

255. Деякі питання об’єктів критичної інформаційної інфраструктури: Постанова Кабінету Міністрів України від 09.10.2020 р. № 943. URL. https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text

256. Про основні засади державного нагляду (контролю) у сфері господарської діяльності: Закон України від 05.04.2007 р. № 877-V. URL. https://zakon.rada.gov.ua/laws/card/877-16

257. Адміністративна відповідальність посадових осіб контролюючих органів. 14.01.2021. URL. https://ecoindustry.pro/analityka/administratyvna-vidpovidalnist-posadovyh-osib-kontrolyuyuchyh-organiv

258. Про затвердження Регламенту Національної комісії, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв’язку: Рішення Національної комісії,

що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку від 18.02.2022 р. № 1. URL. https://zakon.rada.gov.ua/rada/show/v0001864-22#Text

259. Директива Європейського Парламенту і Ради (ЄС) 2018/1972 від 11 грудня 2018 року про запровадження Європейського кодексу електронних комунікацій. URL. https://zakon.rada.gov.ua/laws/show/984_013-18#Text

260. Спецоперація під назвою «стаття Путіна». Радіо Свобода. 13 липня 2021 року. URL. https://www.radiosvoboda.org/a/putin-stattia-odyn-narod/31354996.html

261. Сопільник Л., Ковалів М., Єсімов С. і інші. Розвиток цифрової економіки в контексті забезпечення інформаційної безпеки в Україні. *Traektoriâ Nauki = Path of Science.* 2020. Vol. 6. № 5. S. 2023-2032.

262. Жураковський Б. Ю., Зенів І. О. Технології Інтернету речей. Навчальний посібник. Київ: КПІ ім. Ігоря Сікорського, 2021. 271 с.

263. Угода користувача. URL. https://mind.ua/agreement https://kneu.edu.ua/userfiles/zb_mise/97/17.pdf

264. Краковська А. Є., Бабик М. К. Цифровізація адміністративних послуг в Україні: проблеми та перспективи розвитку. *Науковий вісник Ужгородського Національного Університету. Серія право*. 2022. Випуск 70. С. 329-334.

265. Про адміністративні послуги: Закон України від 06.09.2012 р. № 5203-IV. URL. https://zakon.rada.gov.ua/laws/show/5203-17/conv#n43

266. Про публічні електронні реєстри: Закон України від 18.11.2021 р. № 1907-IX. URL. https://zakon.rada.gov.ua/laws/show/1907-20/conv#n472

267. Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану: Постанова Кабінету Міністрів України від 12.03.2022 р. № 263. URL. https://zakon.rada.gov.ua/laws/show/263-2022-%D0%BF#Text

268. Про хмарні послуги: Закон України від 17.02.2022 р. № 2075-IX. URL. https://zakon.rada.gov.ua/laws/show/2075-20#Text

269. В Україні запустили єдину платформу цифрової взаємодії для допомоги в релокації бізнесу. 12 квітня 2022. URL. https://zt.dsp.gov.ua/news/v-ukraini-zapustyly-iedynu-platformu-tsyfrovoi-vzaiemodii-dlia-dopomohy-v-relokatsii-biznesu/

270. Ведмедев М. М. Феномен кліпового мислення в дискусійному просторі сучасної науки. *Sciences of Europe*. 2021. № 70. С. 41-49.

271. Геворкян А. Ю. Формування основ культури інформаційної безпеки суспільства як фактор зміцнення національної безпеки. *Вісник Національного університету цивільного захисту України. Серія «Державне управління».* 2021. № 1 (14). С. 168-177.

272. Про здійснення превентивних заходів серед дітей та молоді в умовах воєнного стану в Україні: Лист МОН від 13.05.2022 р. № 1/5119-22.

273. Элементы для создания глобальной культуры кибербезопасности. Утвержденные резолюцией 57/239 Генеральной Ассамблеи ООН от 20 декабря 2002 года. URL. https://zakon.rada.gov.ua/laws/show/995_b42#Text

274. Слабкий Г. О., Жданова О. В. Європейські підходи до подолання *у* населення Інтернет-залежності. *Здоров'я нації.* 2019. № 2 (55). С. 198-201.

275. Медіаграмотність. URL. http://media-iq.tilda.ws/medialiteracy

276. Тілікіна Н. В. Медіа, інформаційна і комп'ютерна грамотність як компоненти цифрової грамотності. *Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична*. 2021. Випуск 29. С. 46-56.

277. Цифрова гігієна: яких правил варто дотримуватися в Інтернеті? 24 березня 2020. URL. https://thedigital.gov.ua/news/tsifrova-gigiena-yakikh-pravil-varto-dotrimuvatisya-v-interneti

278. Ронжес О. Є. Визначення рівня цифрової компетентності як необхідної навички в умовах переходу до цифрової держави. *Проблеми політичної психології*. 2021. Випуск 10 (24). С. 331-348.

279. Про схвалення Концепції розвитку цифрових компетентностей та затвердження плану заходів з її реалізації: Розпорядження Кабінету Міністрів України від 03.03.2021 р. № 167-р. URL. https://zakon.rada.gov.ua/laws/show/167-

2021-%D1%80

280. Опис рамки цифрової компетентності для громадян України. Київ: Цифрова освіта Дія, 2021. 56 с.

281. Цифрова компетентність. Які навички слід розвивати під час пандемії? 10.06.2021. URL. https://eufordigital.eu/uk/digital-competence-what-skills-do-you-need-to-develop-during-the-pandemic/

282. Іонан В. Цифрограм 2.0. Цифрова грамотність українців у режимі реального часу. 26.05.2021. URL. https://ua.interfax.com.ua/news/blog/746434.html

283. Ухвалено типову програму підвищення кваліфікації педагогічних працівників із розвитку цифрової компетентності. 13 грудня 2021 року. URL. ttps://mon.gov.ua/ua/news/uhvaleno-tipovu-programu-pidvishennya-kvalifikaciyi-pedagogichnih-pracivnikiv-iz-rozvitku-cifrovoyi-kompetentnosti

284. Smart-інфраструктура у сталому розвитку міст: світовий досвід та перспективи України. Центр Разумкова. Київ:. Видавництво «Заповіт», 2021. 400 с.

ДОДАТКИ

Додаток А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА

в яких опубліковані основні наукові результати дисертації відповідно до постанови Кабінету Міністрів Україні від 12 січня 2022 року № 44:

1. Баран М. В. Інформаційна безпека як предмет адміністративно-правового регулювання. *Соціально-правові студії.* 2021. Випуск 3 (13). С. 50-56.

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

3. Баран М. В. Захист інформації у контексті забезпечення інформаційної безпеки. *Аналітично-порівняльне правознавство.* 2022. № 3. С. 150-155.

4. Баран М. В. Суб'єкти забезпечення інформаційної безпеки в Україні. *Юридичний науковий електронний журнал*. 2022. № 6. С. 220-223.

інші:

1. Баран М. В. Механізм адміністративно-правового регулювання інформаційної безпеки. *Visegrad journal on human rights*. 2021. № 4. С. 25-30.

які засвідчують апробацію матеріалів дисертації:

1. Баран М. В. Аналіз комунікативної діяльності людини в інформаційному просторі в контексті інформаційної безпеки. *Теоретико-прикладні проблеми правового регулювання в Україні:* матеріали Всеукраїнської науково-практичної конференції (м. Львів, 11 грудня 2020 р.) / за заг. ред. І. В. Красницького. Львів: ЛьвДУВС, 2020. С. 20-24.

2. Баран М. В. Електронні торги в аспекті інформаційної безпеки. *Інформаційні технології в освіті та практиці*: матеріали Всеукраїнської

науково-практичної конференції (м. Львів, 18 грудня 2020 р.) / упорядник: Т. В. Магеровська. Львів : ЛьвДУВС, 2020. С. 89-90.

3. Баран М. В. Інформаційно-правова специфіка соціалізації військовослужбовців в аспекті інформаційної безпеки. *Проблеми розвитку адміністративного, фінансового та інформаційного права в контексті євроінтеграційних процесів»:* збірник тез *міжнародної науково-практичної конференції* (м. Львів, 15 квітня 2021 р.). Київ: ПП «Комп'ютерний дизайн», 2021. С. 18-19.

4. Баран М. В. Конституційне право особи на свободу отримання і поширення інформації у контексті забезпечення інформаційної безпеки. *Сучасний конституціоналізм: проблеми теорії та практики:* матеріали наукового семінару (м. Львів, 25 червня 2021 р.). Львів: ЛьвДУВС, 2021. С. 11-15.

5. Баран М. В. Захист прав людини в умовах розвитку цифрових технологій і формування інформаційної безпеки. *Теоретико-прикладні проблеми правового регулювання в Україні:* матеріали V Всеукраїнської науково-практичної конференції (м. Львів, 10 грудня 2021 р.) / за заг. ред. І. В. Красницького. Львів: ЛьвДУВС, 2021. С. 13-16.

6. Баран М. В. Проблеми забезпечення інформаційної безпеки особи в адміністративному процесі. *Проблеми розвитку адміністративного, фінансового та інформаційного права в контексті євроінтеграційних процесів*: збірник. тез міжнародної науково-практичної конференції (м. Львів, 3 червня 2022 р.). Київ: Комп'ютерний дизайн, 2022. С. 27-30.

7. Баран М. В. Адміністративні форми та методи забезпечення інформаційної безпеки у Збройних Силах в умовах воєнного стану. *Конституційні права і свободи людини та громадянина в умовах воєнного стану:* матеріали наукового семінару (м. Львів, 23 червня 2022 р.). Львів: ЛьвДУВС, 2022. С. 24-27.

Додаток Б

Пропозиції
щодо внесення змін і доповнень до Закону України
«Про інформацію» від 02.10.1992 р. № 2657-XII
(Відомості Верховної Ради України. 1992. № 48. Ст. 650)

Доповнити статтю 9 «Основні види інформаційної діяльності» Закону України «Про інформацію» частиною 2 та викласти у редакції:

2. Захист інформації охоплює захист від неправомірного доступу, знищення, блокування, копіювання, надання, розповсюдження від інших неправомірних дій, від деструктивного інформаційного впливу, що завдає шкоди здоров'ю.

Додаток В

Пропозиції
щодо внесення змін і доповнень до Закону України
«Про адміністративні послуги» від 06.09.2012 р. № 5203-VI
(Відомості Верховної Ради. 2013. № 32. Ст. 409)

Доповнити частину 4 статті 13 «Адміністратор» Закону України «Про адміністративні послуги» пунктом 9 та викласти у редакції:

9) забезпечує захист інформації відповідно до чинного законодавства.

Додаток Д

Пропозиції
щодо внесення змін і доповнень до Закону України
«Про публічні електронні реєстри» від 18.11.2021 р. № 1907-IX
https://zakon.rada.gov.ua/laws/show/1907-20#Text

Доповнити статтю 4 «Регулювання відносин, що виникають під час провадження діяльності у сфері реєстрів» Закону України «Про публічні електронні реєстри» частиною 5 та викласти у редакції:

5. Вимоги про захист інформації, які містяться в реєстрах, встановлюються центральним органом виконавчої влади зі спеціальним статусом у сферах електронних комунікацій, радіочастотного спектру та надання послуг поштового зв'язку.

Додаток Е

Пропозиції
щодо внесення змін і доповнень до Закону України
від 17.02.2022 р. № 2075-X «Про хмарні послуги»
(https://zakon.rada.gov.ua/laws/show/2075-20#Text)

Доповнити статтю 14 «Захист інформації при наданні хмарних послуг та/або послуг центру обробки даних» Закону України «Про хмарні послуги» частиною 3 та викласти у редакції:

3. Державний нагляд за дотриманням вимог з інформаційної безпеки хмарних послуг здійснюється центральним органом виконавчої влади зі спеціальним статусом у сферах електронних комунікацій, радіочастотного спектру та надання послуг поштового зв'язку. Предметом державного нагляду за дотриманням вимог з інформаційної безпеки є дотримання фізичними особами-підприємцями та юридичними особами обов'язкових вимог, встановлених цим законом, іншими законами та ухваленими відповідно до нормативно-правових актів у сфері інформаційної безпеки.

Додаток Ж

Підсумки
соціологічного дослідження

Відповіді працівників юридичних факультетів Львівського національного університету імені Івана Франка, Національного університету «Львівська політехніка», Львівського державного університету внутрішніх справ (науково-педагогічний склад)

№ з/п	Питання	Так	Ні	%
1	Чи доцільно, на Вашу думку, стверджувати, що система правового захисту прав, свобод і законних інтересів громадян у контексті забезпечення інформаційної безпеки донині не досягла стійкої структурно-функціональної системної рівноваги ?	48	8	85,7
2	Чи впливає дисбаланс взаємодій між органами виконавчої влади та інституціями громадянського суспільства на стан інформаційної безпеки ?	33	23	58,9
3	У наявних проектах закону України щодо інформаційної безпеки існує статусна невизначеність спеціалізованих органів забезпечення захисту особи та суспільства від деструктивного інформаційного впливу. Чи погоджуєтесь із зазначеним твердженням?	28	28	50
4	Чи доцільно на законодавчому рівні врегулювати засади захисту особи від деструктивного інформаційного впливу ?	56	0	100
5	Чи вважаєте Ви, що прояви позаправових інституційних практик (лобізм, корупція, захист відомчих, корпоративних, групових інтересів) в межах регіональних владних структур впливають на стан забезпечення інформаційної безпеки ?	56	0	100
6	В юридичних наукових виданнях з питань забезпечення інформаційної безпеки висловлюються думки, що вплив інформаційної культури на забезпечення інформаційної безпеки є більш ефективний, ніж виявлення та блокування деструктивного інформаційного впливу органами спеціальної компетенції. Чи погоджуєтеся Ви із вказаним?	35	21	62,5
7	Чи потребує нині уточнення правового статусу підрозділів Державної служби спеціального зв’язку та захисту інформації України?	22	34	39,2

8	Чи доцільне створення додаткових правових гарантій органам місцевого самоврядування у сфері інформаційної безпеки, що дозволить сконструювати збалансовану систему взаємних обов'язків, прав і відповідальності на основі принципів централізації та взаємоконтролю?	24	32	48,2
9	Чи вважаєте Ви, що узгодженість повноважень Служби безпеки України з процедурно-правовими формами блокування та видалення інформації можливо реалізувати нормативним закріпленням у положенні про таку службу?	14	42	25,0
10	Чи існує нині організаційно-структурна раціональність державної системи забезпечення інформаційної безпеки, тобто система органів державної влади, які відповідають за реалізацію державної інформаційної політики?	44	12	78,5

Опитано: працівників – 56.
Львівський національний університет імені Івана Франка – 14.
Національний університет «Львівська політехніка» – 18.
Львівський державний університет внутрішніх справ – 24.
% визначено за позитивними відповідями.

Опитування проводилось у травня 2021 року.

У зв'язку з істотною зміною вимог забезпечення інформаційної безпеки в умовах воєнного стану щодо агресії Росії проти України, що, на нашу думку, суттєво впливає на наукові погляди вчених, результати соціологічного опитування використані винятково в інформативному плані.

Додаток И

Акт

Додаток К

Довідка